24-Port Intelligent Workgroup Switch

Management Guide

Management Guide

24-Port Intelligent Workgroup Switch

with 24 10BASE-T / 100BASE-TX (RJ-45) Ports,
and 2 Slots for 100BASE-FX or Gigabit Uplink Modules

SF-0204F
E122003-R01
F2.0.3.9
150XXXXXXXXXX

Contents

Chapter 1: Switch Management

Connecting to the Switch

Configuration Options

This 24-port Layer 2 switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a Web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is assigned via DHCP by default. To change this address, see “Setting an IP Address” on page 1-4.

The switch’s HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics graphically using a standard Web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch’s Web management interface can be accessed from any computer attached to the network.

The switch’s management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using management software.

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

- Set user names and passwords
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by rate limiting
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download system firmware/switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to four static or LACP trunks
- Enable port mirroring
- Enable broadcast storm control
- Display system information and statistics

Required Connections

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

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in “Console Port Pin Assignments” on page B-1 of the Installation Guide.

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

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable’s to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set the data rate to 9600 baud.
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.

Notes: **1.** When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal’s VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

2. Refer to “Line Commands” on page 3-57 for a complete description of console configuration options.

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

For a description of how to use the CLI, see “Using the Command Line Interface” on page 3-1. For a list of all the CLI commands and detailed information on using the CLI, refer to “Command Groups” on page 3-8.

Remote Connections

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

The IP address for this switch is assigned via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see “Setting an IP Address” on page 1-4.

Note: This switch supports four concurrent Telnet sessions.

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

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

Basic Configuration

Console Connection

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

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

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

Setting Passwords

Note: 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:

1. Open the console interface with the default user name and password "admin" to access the Privileged Exec level.
2. Type "configure" and press <Enter>.

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

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

```
Username: admin
Password:
CLI session with the SF-2024F is opened.
To end the CLI session, enter [Exit].
Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

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

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment.

Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: The IP address for this switch is assigned via DHCP by default.

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

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

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

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

2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.

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

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

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

Dynamic Configuration

If you select the “bootp” or “dhcp” option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the “ip dhcp restart” command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

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

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

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

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

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

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

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

4. Type “ip dhcp restart” to begin broadcasting service requests. Press <Enter>.

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

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

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

Console#
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

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

Community Strings

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

The default strings are:

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

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

To prevent unauthorized access to the switch via SNMP, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

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

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

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

Trap Receivers

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

To configure a trap receiver, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server host *host-address community-string*,” where “host-address” is the IP address for the trap receiver and “community-string” is the string associated with that host. Press <Enter>.

2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type “snmp-server enable traps *type*,” where “type” is either **authentication** or **link-up-down**. Press <Enter>.

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

Saving Configuration Settings

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

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

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

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

```
Console#copy running-config startup-config
Startup configuration file name []: startup

Console#
```

Managing System Files

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

The three types of files are:

- **Configuration** — These files store system configuration information and are created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. See "Saving or Restoring Configuration Settings" on page 2-15 for more information.
- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI, Web and SNMP management interfaces. See "Managing Firmware" on page 2-14 for more information.
- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files, and two diagnostic code files. However, you can have as many configuration files as available flash memory space allows.

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

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

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file.
(See "Setting the Startup Configuration File" on page 2-16.)

The following table lists some of the basic system defaults.

Function	Parameter	Default
IP Settings	Management VLAN	1
	DHCP	Enabled
	BOOTP	Disabled
	User Specified	Disabled
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
SNMP	Community Strings	"public" (read only) "private" (read/write)
	Authentication Failure Traps	Enabled
	Link-up-Down Traps	Enabled
Security	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	Authentication	Local
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)

Function	Parameter	Default
Port Status	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
	Capabilities	10BASE-T – 10 Mbps half duplex 10 Mbps full duplex Full-duplex flow control disabled 100BASE-TX/FX – 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex Full-duplex flow control disabled 1000BASE-T – 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled 1000BASE-X – 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
Link Aggregation	Static Trunks	None
	LACP (all ports)	Disabled
Spanning Tree Protocol	Status	Enabled (Defaults: All parameters based on IEEE 802.1w)
	Fast Forwarding	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
	Private VLAN	No Private VLAN
Class of Service	Ingress Port Priority	0
	Weighted Round Robin	1:2:4:6
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled

Function	Parameter	Default
Multicast Filtering	IGMP Snooping	Enabled
	Act as Querier	Enabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	32000 octets/second
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
Rate Limit	Status	Disabled
802.1x	Re-authentication	Disabled
	Status	Disabled
	Mode	Force-Authorized (all ports)

Chapter 2: Configuring the Switch

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, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 3: "Command Line Interface."

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

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting the IP Address" on page 2-11.)

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 "Configuring the Logon Password" on page 2-25.)

Note: If you log into the Web interface as guest (Normal Exec level), you can view page information but only change the guest password. If you log in as admin (Privileged Exec level), you can apply changes on all pages.

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

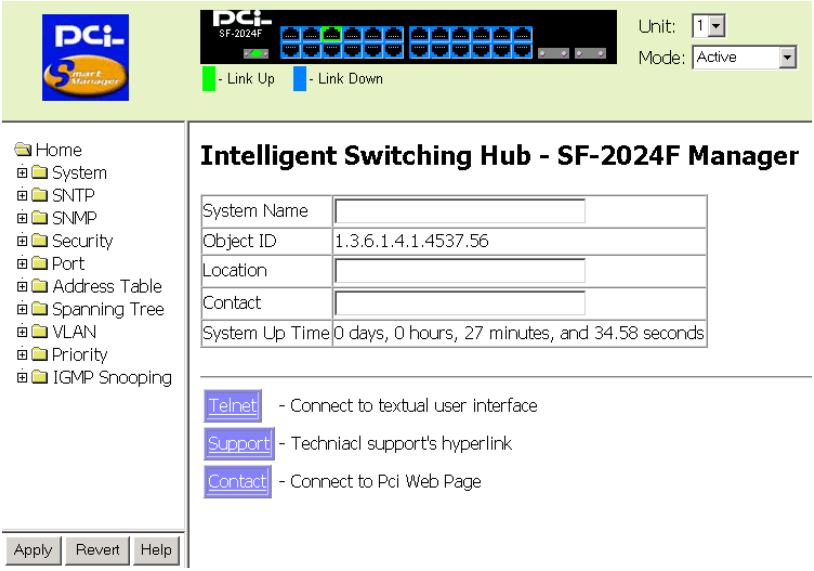
Note: If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding to improve the switch's response time to management commands issued through the Web interface. (See "Displaying Interface Settings" on page 2-72.)

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.



Unit: 1

Mode: Active

Intelligent Switching Hub - SF-2024F Manager

System Name	
Object ID	1.3.6.1.4.1.4537.56
Location	
Contact	
System Up Time	0 days, 0 hours, 27 minutes, and 34.58 seconds

Telnet - Connect to textual user interface

Support - Techniacl support's hyperlink

Contact - Connect to Pci Web Page

If this is your first time to access the management agent, you should define a new Administrator user name and password, record them and put them in a safe place. Select Security from the Main Menu, and then enter a new user name and password for the Administrator. Note that user names and passwords can consist of up to 8 alphanumeric characters and are case sensitive.

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

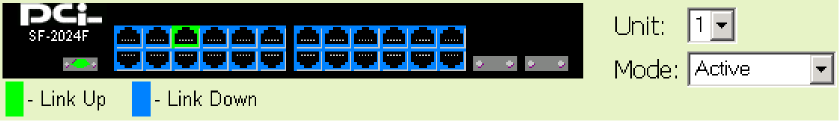
Configuration Options

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.

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

Panel Display

The Web agent displays an image of the switch's ports, indicating whether each link is up or down. Clicking on the image of a port opens the Port Configuration page as described on page 2-49.



Unit: 1

Mode: Active

🟩 - Link Up 🟦 - Link Down

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.

Menu	Description	Page
System		2-7
System Information	Provides basic system description, including contact information	2-7
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	2-8
Bridge Extension Configuration	Shows the configuration for bridge extension commands; enables GVRP multicast protocol	2-10
IP Configuration	Sets the IP address for management access	2-11
File		2-14
Firmware	Manages code image files	2-14
Configuration	Manages switch configuration files	2-15
Log		2-18
System Logs	Sends error messages to a logging process	2-18
Logs	Stores and displays error messages	2-19
Remote Logs	Configures the logging of messages to a remote logging process	2-19
Reset	Restarts the switch	2-21
SNTP		2-21
Configuration	Configures SNTP client settings, including broadcast mode or a specified list of servers	2-21
Clock Time Zone	Sets the local time zone for the clock	2-22
SNMP		2-23
SNMP	Configures community strings and related trap functions	2-23
Security		2-25
Passwords	Assigns a new password for the logon user name	2-25
Authentication Settings	Configures RADIUS/TACACS+ authentication parameters	2-26
HTTPS Settings	Configures secure HTTP settings	2-29
SSH Settings	Configures Secure Shell settings	2-31
Port Security	Configures port security	2-32
802.1X		2-34
Information	Displays general port authentication status information	2-35
Configuration	Enables the changing of general port authentication features	2-36
Port Configuration	Enables the changing of port authentication features	2-37
Statistics	Displays a per-port statistical readout	2-39

Menu	Description	Page
ACL		2-40
Configuration	Configures packet filtering based on IP or MAC addresses	2-40
Port Binding	Binds a port to the specified ACL	2-47
Port		2-48
Port Information	Displays port connection status	2-48
Trunk Information	Displays trunk connection status	2-48
Port Configuration	Configures port connection settings	2-49
Trunk Configuration	Configures trunk connection settings	2-51
Trunk Membership	Specifies ports to group into static trunks	2-52
LACP		2-53
Configuration	Allows ports to dynamically join trunks	2-53
Port Broadcast Control	Sets the broadcast storm threshold	2-54
Mirror Port Configuration	Sets the source and target ports for mirroring	2-55
Rate Limit		2-56
Granularity	Enables or disables the rate limit feature	2-57
Rate Limit Configuration	Sets the rate limit for each port	2-57
Port Statistics	Lists Ethernet and RMON port statistics	2-58
Address Table		2-63
Static Addresses	Displays entries for interface, address or VLAN	2-63
Dynamic Addresses	Displays or edits static entries in the Address Table	2-64
Address Aging	Sets timeout for dynamically learned entries	2-65
Spanning Tree		2-66
STA		2-66
Information	Displays STA values used for the bridge	2-66
Configuration	Configures global bridge settings for STA	2-66
Port Information	Displays individual port settings for STA	2-72
Trunk Information	Displays individual trunk settings for STA	2-72
Port Configuration	Configures individual port settings for STA	2-76
Trunk Configuration	Configures individual trunk settings for STA	2-76
VLAN		2-78
802.1Q VLAN		2-78
Basic Information	Displays basic information on the VLAN type supported by this switch	2-81
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	2-81
Static List	Used to create or remove VLAN groups	2-83
Static Table	Modifies the settings for an existing VLAN	2-84

Menu	Description	Page
Static Membership by Port	Configures membership type for interfaces, including tagged, untagged or forbidden	2-86
Port Configuration	Specifies default PVID and VLAN attributes	2-87
Trunk Configuration	Specifies default trunk VID and VLAN attributes	2-87
Private VLAN		
Information	Displays Private VLAN feature information	2-89
Configuration	This page is used to create/remove primary or community VLANs	2-90
Association	Each community VLAN must be associated with a primary VLAN	2-91
Port/Trunk Information	Displays the interfaces associated with private VLANs	2-92
Port/Trunk Configuration	Sets the private VLAN interface type, and associates the interfaces with a private VLAN	2-93
Priority		2-95
Default Port Priority	Sets the default priority for each port	2-95
Default Trunk Priority	Sets the default priority for each trunk	2-95
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	2-97
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	2-99
Queue Scheduling	Configures Weighted Round Robin queueing	2-100
IP Precedence/DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both	2-101
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	2-102
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	2-104
IP Port Priority Status	Globally enables or disables IP Port Priority	2-106
IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value	2-106
ACL CoS Mapping	Sets the CoS value and corresponding output queue for packets matching an ACL rule	2-107
IGMP Snooping		
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	2-109
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router/switch for each VLAN ID	2-110
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router/switch	2-111
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	2-112
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	2-113

Basic Configuration

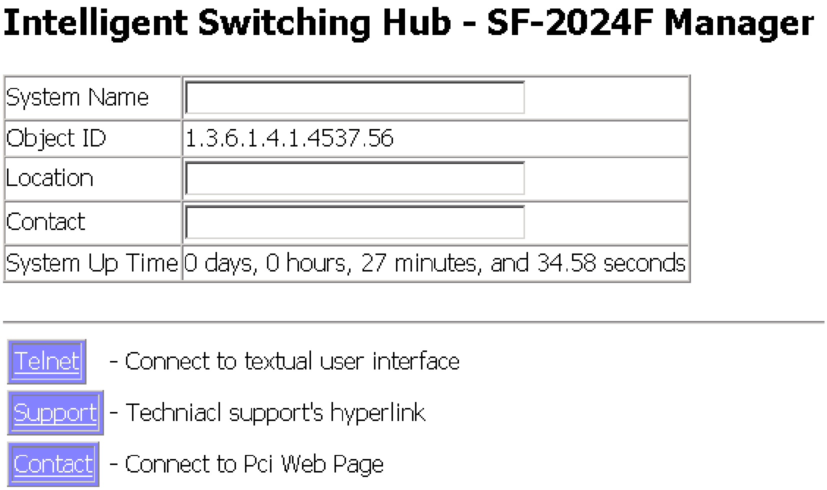
Displaying System Information

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

Command Attributes

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

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows you to access the Command Line Interface via Telnet.)



Intelligent Switching Hub - SF-2024F Manager

System Name	
Object ID	1.3.6.1.4.1.4537.56
Location	
Contact	
System Up Time	0 days, 0 hours, 27 minutes, and 34.58 seconds

Telnet - Connect to textual user interface

Support - Techniacl support's hyperlink

Contact - Connect to Pci Web Page

CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname SF-2024F                                         3-20
Console(config)#snmp-server location [NONE]                               3-49
Console(config)#snmp-server contact [NONE]                                3-48
Console#show system                                                       3-31
System description: Intelligent Switching Hub - SF-2024F
System OID string: 1.3.6.1.4.1.4537.56
System information
 System Up time: 0 days, 0 hours, 55 minutes, and 10.30 seconds
 System Name            : SF-2024F
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 5A-A5-AA-55-4C-45
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result
UART Loopback Test......................PASS
Timer Test..............................PASS
DRAM Test ..............................PASS
I2C Initialization......................PASS
Runtime Image Check ....................PASS
PCI Device Check .......................PASS
Switch Driver Initialization............PASS
Switch Internal Loopback Test...........PASS
------------------- DONE --------------------
Console#
```

Displaying Switch Hardware/Software Versions

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

Command Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in RJ-45 ports and expansion ports.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power supply.
- **Redundant Power Status*** – Displays the status of the redundant power supply.

* CLI only.

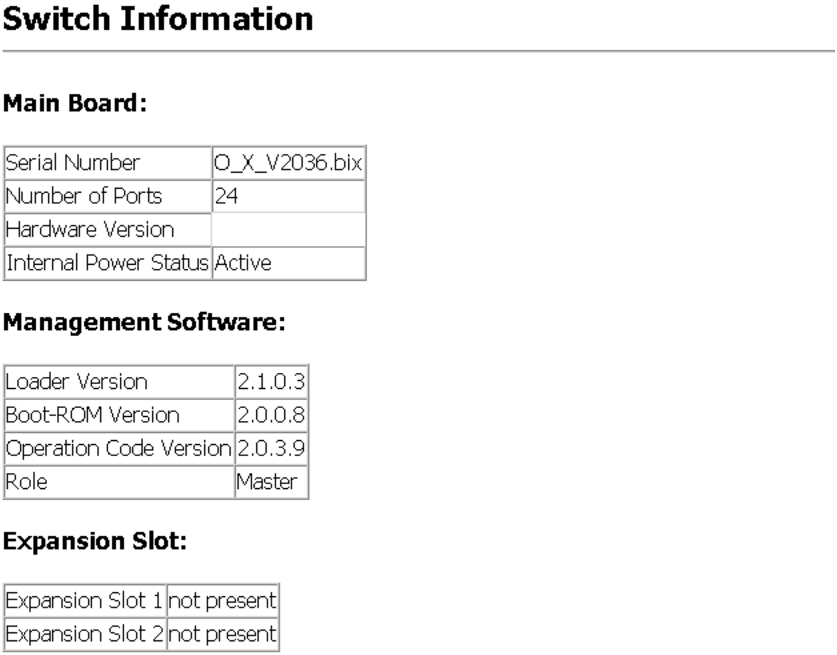
Management Software

- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version number of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows if the switch is stacked or operating stand-alone.

Expansion Slot

- **Expansion Slot 1/2** – Slots for expansion modules.

Web – Click System, Switch Information.



Switch Information

Main Board:

Serial Number	O_X_V2036.bix
Number of Ports	24
Hardware Version	
Internal Power Status	Active

Management Software:

Loader Version	2.1.0.3
Boot-ROM Version	2.0.0.8
Operation Code Version	2.0.3.9
Role	Master

Expansion Slot:

Expansion Slot 1	not present
Expansion Slot 2	not present

CLI – Use the following command to display version information.

```
Console#show version                                                   3-33
Unit1
 Serial number           :ag1005
 Service tag             :
 Hardware version        :
 Module A type           :not present
 Module B type           :not present
 Number of ports         :24
 Main power status       :up
 Redundant power status  :not present
Agent(master)
 Unit id                 :1
 Loader version          :2.1.0.0
 Boot rom version        :2.0.0.7
 Operation code version  :2.0.3.1
Console#
```

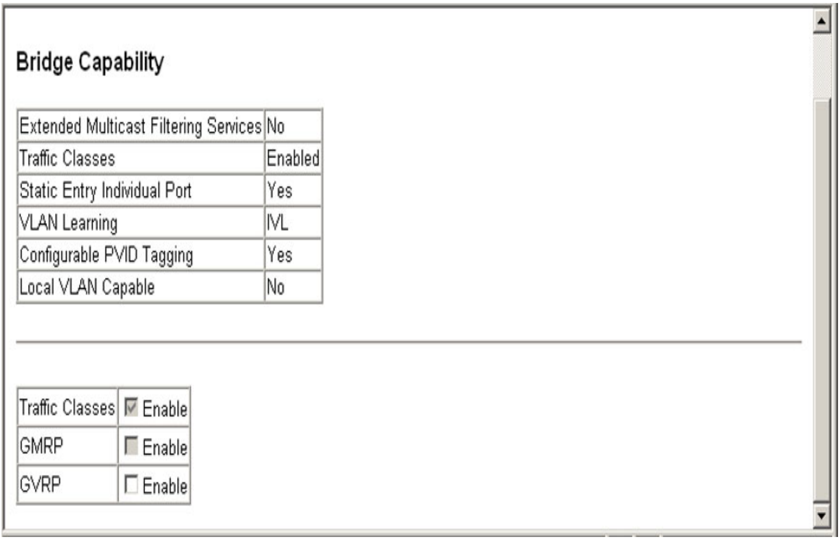
Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables, or to configure the global setting for GARP VLAN Registration Protocol (GVRP).

Command Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Class of Service Configuration” on page 2-95.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to “Setting Static Addresses” on page 2-63.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to “VLAN Configuration” on page 2-78.)
- **Local VLAN Capable** – This switch does not support multiple local bridges (i.e., multiple Spanning Trees).
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.
- **GVRP** – GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLAN groups which extend beyond the local switch.

Web – Click System, Bridge Extension Configuration.



Bridge Capability

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

Traffic Classes	☑ Enable
GMRP	□ Enable
GVRP	□ Enable

CLI – Enter the following command.

```
Console#show bridge-ext                                         3-108
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

Setting the IP Address

An IP address may be used for management access to the switch over your network. By default, the switch uses DHCP to assign IP settings to VLAN 1 on the switch.

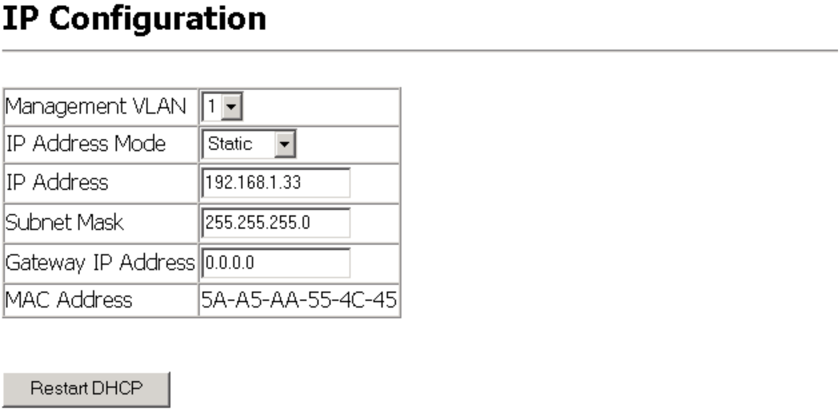
You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server when it is powered on. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Command Attributes

- **Management VLAN** – This is the only VLAN through which you can gain management access to the switch. By default, all ports on the switch are members of VLAN 1, so a management station can be connected to any port on the switch. However, if other VLANs are configured and you change the Management VLAN, you may lose management access to the switch. In this case, you should reconnect the management station to a port that is a member of the Management VLAN.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
- **IP Address** – Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.
- **Gateway IP Address** – IP address of the gateway router between this device and management stations that exist on other network segments.
- **MAC Address** – The MAC address of this switch.

Manual Configuration

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



IP Configuration

Management VLAN	1
IP Address Mode	Static
IP Address	192.168.1.33
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	5A-A5-AA-55-4C-45

CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address 10.2.13.30 255.255.255.0              3-53
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254                    3-54
Console(config)#
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click System, IP Configuration. Specify the Management VLAN, set the IP Address Mode to DHCP or BOOTP. Then click Apply to save your changes. The switch will broadcast a request for IP configuration settings on the next power reset. Otherwise, you can click Restart DHCP to immediately request a new address.

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

CLI – Specify the management interface, and set the IP Address Mode to DHCP or BOOTP.

```
Console#config
Console(config)#interface vlan 1                                    3-66
Console(config-if)#ip address dhcp                                  3-53
Console(config-if)#end
Console#ip dhcp restart                                             3-54
Console#show ip interface                                           3-55
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

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

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

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart                                             3-54
```

Managing Firmware

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

Command Attributes

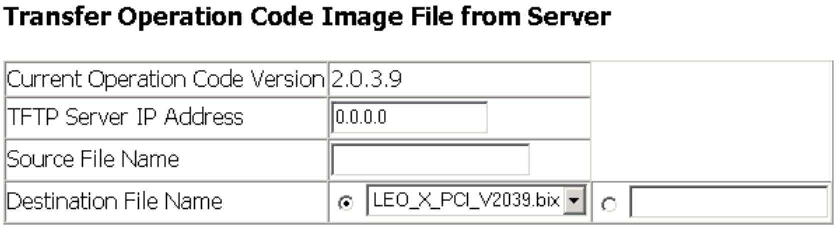
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **Destination File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

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

Downloading System Software from a Server

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

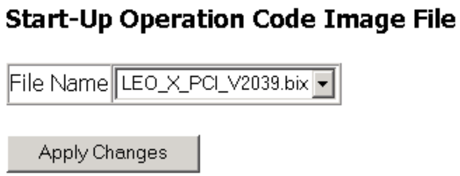
Web – Click System, File, Firmware. Enter the IP address of the TFTP server, enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Transfer from Server. To start the new firmware, reboot the system via the System, Reset menu.



Transfer Operation Code Image File from Server

Current Operation Code Version	2.0.3.9	
TFTP Server IP Address	0.0.0.0	
Source File Name		
Destination File Name	● LEO_X_PCI_V2039.bix ▾	○

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



Start-Up Operation Code Image File

File Name: LEO_X_PCI_V2039.bix

CLI – Enter the IP address of the TFTP server, select “config” or “opcode” file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

```
Console#copy tftp file                                                   3-14
TFTP server ip address: 10.1.0.99
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: LEO_X_PCI_V2039.bix
Destination file name: LEO_X_PCI_V2039.bix
/
Console#config
Console(config)#boot system opcode: LEO_X_PCI_V2039.bix                  3-18
Console(config)#exit
Console#reload                                                           3-12
```

To start the new firmware, enter the “reload” command or reboot the system.

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. The configuration file can be later downloaded to restore the switch’s settings.

Command Attributes

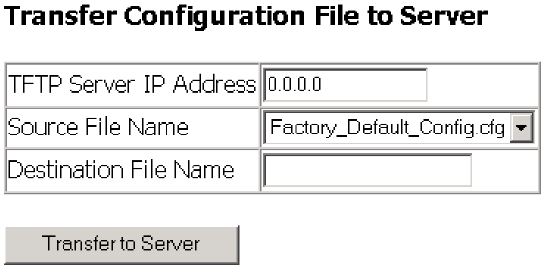
- **TFTP Server IP Address** — The IP address of a TFTP server.
- **Destination File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

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

Downloading Configuration Settings from a Server

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

Web – Click System, File, Configuration. Enter the IP address of the TFTP server, enter the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Transfer from Server.

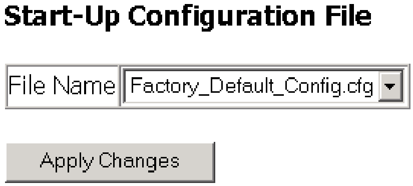


Transfer Configuration File to Server

TFTP Server IP Address	0.0.0.0
Source File Name	Factory_Default_Config.cfg
Destination File Name	

Setting the Startup Configuration File

If you download to a new file name, then select the new file from the drop-down box for Startup Configuration File, and press Apply Changes. To use the new settings, reboot the system via the System, Reset menu.



Start-Up Configuration File

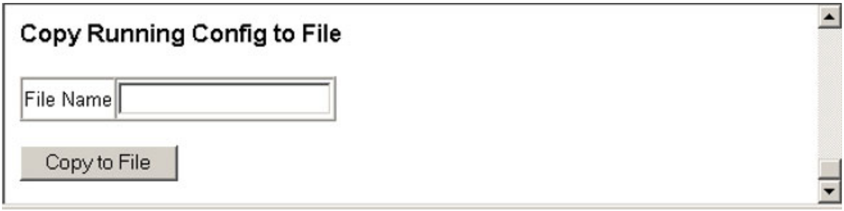
File Name	Factory_Default_Config.cfg

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                    3-14
TFTP server ip address: 192.168.1.19
Source configuration file name: startup2.0
Startup configuration file name [startup] : startup2.0
/
Console#
Console#config
Console(config)#boot system config: startup2.0                      3-18
Console(config)#exit
Console#reload
```

Copying the Running Configuration to a File

You can copy the running configuration to a file.



Copy Running Config to File

File Name

CLI – If you copy the running configuration to a file, you can set this file as the startup file at a later time, and then restart the switch.

```
Console#copy running-config file                                  3-14
destination file name : 051902.cfg
/
Console#
Console#config
Console(config)#boot system config: 051902.cfg                    3-18
Console(config)#exit
Console#reload                                                    3-12
```

System Logs Configuration

The system can be configured to send debug and error messages to a logging process. This logging process controls the type of error messages that are stored in switch memory or sent to a remote syslog server.

The system allows you to 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.

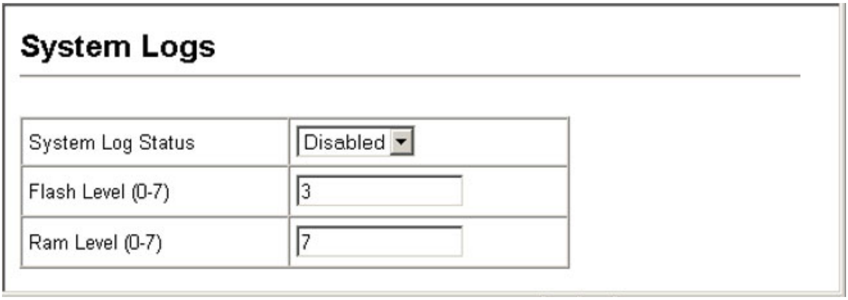
The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

Command Attributes

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

Note: The Flash Level must be equal to or less than the Ram Level.

Web – Click System, Log, System Logs. Specify System Log Status, then change the level of messages, and click Apply.



System Logs

System Log Status	Disabled
Flash Level (0-7)	3
Ram Level (0-7)	7

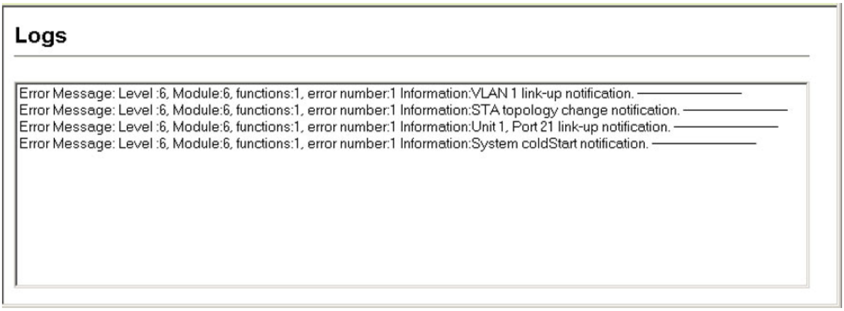
CLI – Specify the hostname, location and contact information.

```
Console(config)#logging on                                            3-23
Console(config)#logging history ram 0                                 3-23
Console(config)#
Console#show logging flash                                            3-27
Syslog logging: Disable
History logging in FLASH: level errors
Console#
```

Logs

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

Web – Click System, Log, Logs.



Logs

```
Error Message: Level :6, Module:6, functions:1, error number:1 Information:VLAN 1 link-up notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:STA topology change notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, Port 21 link-up notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:System coldStart notification.
```

Remote Logs Configuration

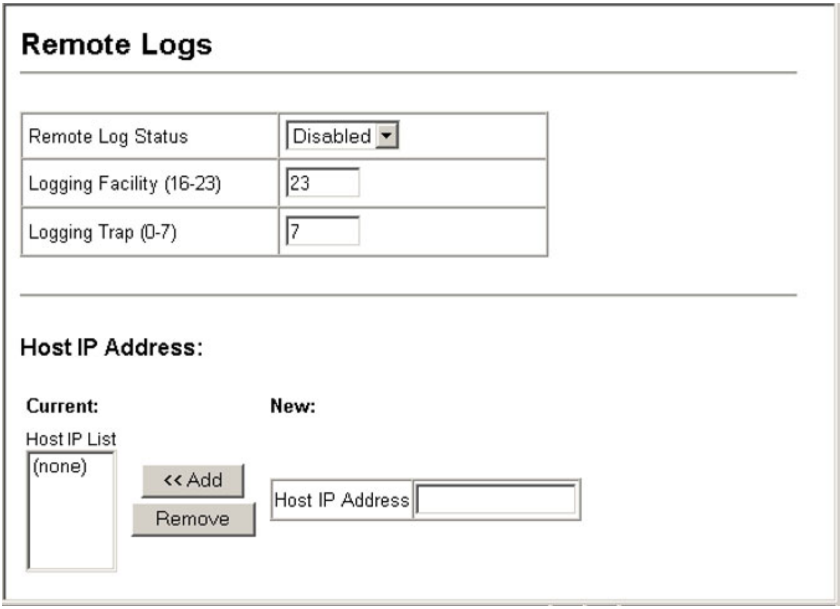
The Remote Logs page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the error messages sent to only those messages of a specified level.

Command Attributes

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process.
  (Default: enabled)
- **Logging Facility (16-23)** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service. (Default: 23)
- **Logging Trap (0-7)** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server.
  (Default: 3)

- **Host IP List** – Displays the list of remote server IP addresses that receive the syslog messages. The maximum number of host IP addresses allowed is five.
- **Host IP Address** – Specifies a new server IP address to add to the Host IP List.

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



Remote Logs

Remote Log Status	Disabled
Logging Facility (16-23)	23
Logging Trap (0-7)	7

Host IP Address:

Current:

Host IP List

(none)

New:

Host IP Address

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

```
Console(config)#logging host 10.1.0.9
Console(config)#logging facility 23
Console(config)#logging trap 4
Console(config)#
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: enable
REMOTELOG facility type: local use 7
REMOTELOG level type: Warning conditions
REMOTELOG server ip address: 10.1.0.9
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#
```

Reset

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

Reset the switch by selecting 'Reset'.

CLI – Use the reload command to reboot the system.

```
Console#reload                                                         3-12
System will be restarted, continue <y/n>? y
Console#
```

Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. (See “calendar set” on page 45.) If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

This switch acts as an SNTP client in two modes:

Unicast – 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.

Broadcast – The switch sets its clock from an time server in the same subnet that broadcasts time updates. If there is more than one SNTP server, the switch accepts the first broadcast it detects and ignores broadcasts from other servers.

Configuring SNTP

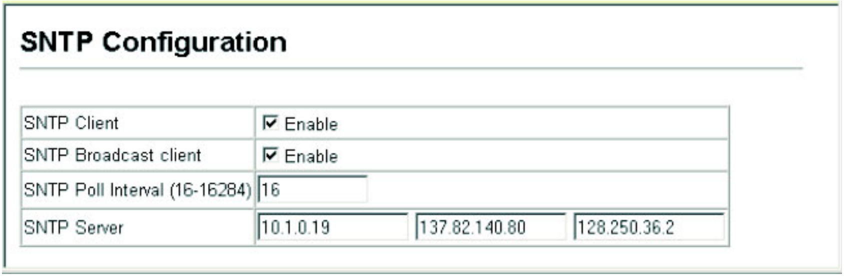
You can configure the switch to send time synchronization requests to specific time servers (i.e., client mode), update its clock based on broadcasts from time servers, or use both methods. When both methods are enabled, the switch will update its clock using information broadcast from time servers, but will query the specified server(s) if a broadcast is not received within the polling interval.

Command Attributes

- **SNTP Client** – Configures the switch to operate as an SNTP unicast client. This mode requires at least one time server to be specified in the SNTP Server field.
- **SNTP Broadcast Client** – Configures the switch to operate as an SNTP broadcast client. This mode requires no other configuration settings; the switch will obtain time updates from time server broadcasts (using the multicast address 224.0.1.1).

- **SNTP Poll Interval (16-16284)** – Sets the interval between sending requests for a time update from a time server when set to SNTP Client mode.
  (Range: 16-16284 seconds; Default: 16 seconds)
- **SNTP Server** – In unicast mode, sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

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



SNTP Configuration

SNTP Client	☑ Enable		
SNTP Broadcast client	☑ Enable		
SNTP Poll Interval (16-16284)	16		
SNTP Server	10.1.0.19	137.82.140.80	128.250.36.2

CLI – This example configures the switch to operate as an SNTP multicast client.

```
Console(config)#sntp client                                       3-42
Console(config)#sntp poll 16                                      3-43
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.2  3-43
Console(config)#sntp broadcast client                             3-44
Console(config)#
```

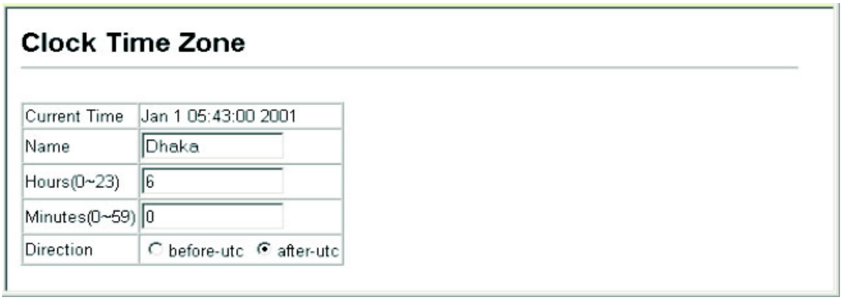
Setting the Time Zone

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

Command Attributes

- **Current Time** – Displays the current time.
- **Name** – Assigns a name to the time zone.
- **Hours (0-23)** – The number of hours before/after UTC.
- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

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



Clock Time Zone

Current Time	Jan 1 05:43:00 2001
Name	Dhaka
Hours(0~23)	6
Minutes(0~59)	0
Direction	○ before-utc ● after-utc

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

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC      3-45
Console#
```

Configuring SNMP

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.

The switch includes an onboard agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports, based on the Simple Network Management Protocol (SNMP). A network management station can access this information using software such as HP OpenView. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

Setting Community Access Strings

You may configure up to five community strings authorized for management access. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

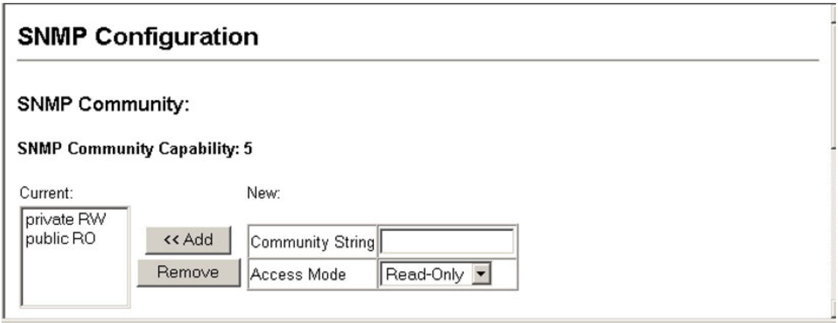
Command Attributes

- **SNMP Community Capability** – Indicates that the switch supports up to five community strings.
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

  Default strings: “public” (read-only access), “private” (read/write access)
  Range: 1-32 characters, case sensitive

- **Access Mode**
  - **Read-Only** – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

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



SNMP Configuration

SNMP Community:

SNMP Community Capability: 5

Current:

private RW
public RO

New:

Community String	
Access Mode	Read-Only

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

```
Console(config)#snmp-server community spiderman rw                    3-47
Console(config)#
```

Specifying Trap Managers

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

Command Usage

- You can enable or disable authentication messages via the Web interface.
- You can enable or disable authentication messages, link-up-down messages, or all notification types via the CLI.

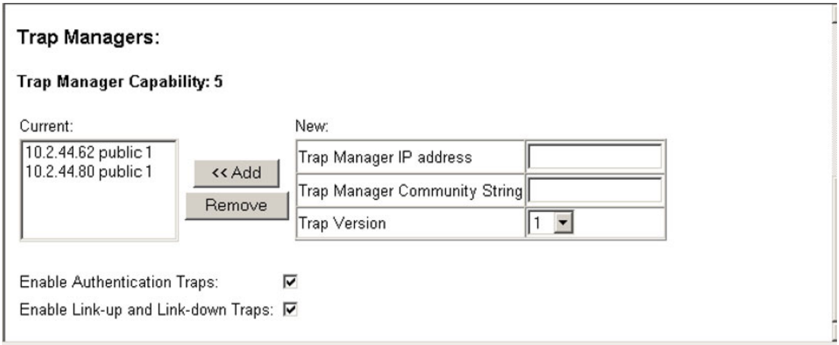
Command Attributes

- **Trap Manager Capability** – Indicates that the switch supports up to five trap managers.
- **Current** – Displays a list of the trap managers currently configured.
- **Trap Manager IP Address** – IP address of a new management station to receive trap messages.
- **Trap Manager Community String** – Specifies a valid community string for the new trap manager entry. Though you can set this string in the Trap Managers table,

we recommend that you define this string in the SNMP Protocol table as well. Range: 1-32 characters, case sensitive

- **Trap Version** – Indicates if the user is running version 1 or version 2c.
- **Enable Authentication Traps** – Issues a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is enabled.)
- **Enable Link-up and Link-down Traps** – Issues a trap message whenever a port link is established or broken.

Web – Click SNMP, Configuration. Fill in the Trap Manager IP Address box and the Trap Manager Community String box, mark Enable Authentication Traps if required, and then click Add.



Trap Managers:

Trap Manager Capability: 5

Current:

10.2.44.62 public 1
10.2.44.80 public 1

New:

Trap Manager IP address	
Trap Manager Community String	
Trap Version	1

Enable Authentication Traps: ☑

Enable Link-up and Link-down Traps: ☑

CLI – This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 batman                      3-49
Console(config)#snmp-server enable traps authentication                 3-50
```

Security

Use the Passwords or RADIUS/TACACS+ menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch (using the Passwords menu), or you can use a remote access authentication server based on the RADIUS/TACACS+ protocol. You can also use IEEE 802.1x port authentication to control access to specific ports (dot1X menu).

Configuring the Logon Password

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. (If for some reason your password is lost, you can delete all the user-defined configuration files to restore the factory defaults and the default password as described in “Upgrading Firmware via the Serial Port” on A-1.)

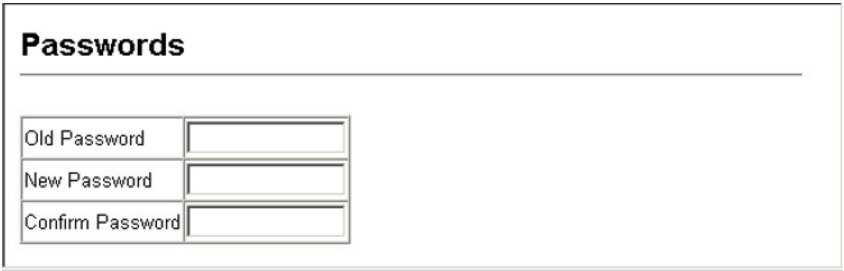
The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.” Note that user names can only be assigned via the CLI.

Command Attributes

- **User Name*** – The name of the user.
  (Maximum length: 8 characters; maximum number of users: 5)
- **Access Level*** – Specifies the user level.
  (Options: Normal and Privileged)
- **Password** – Specifies the user password.
  (Range: 0-8 characters plain text, case sensitive)

* CLI only.

Web – Click Security, Passwords. Enter the old password, enter the new password, confirm it by entering it again, then click Apply.



Passwords

Old Password	
New Password	
Confirm Password	

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

```
Console(config)#username bob access-level 15                        3-21
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring RADIUS/TACACS Logon Authentication

You can configure this switch to authenticate users logging into the system for management access using local, RADIUS, or TACACS+ authentication methods.

RADIUS and 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 a switch.

Like RADIUS, Terminal Access Controller Access Control System Plus (TACACS+) is a system that uses a central server to control authentication for access to switches on the network.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol.
- 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 control management access via the console port, Web browser, or Telnet. These access options must be configured on the authentication server.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS+ and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
  - **RADIUS** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - **Local** – User authentication is performed only locally by the switch.
  - **[authentication sequence]** – User authentication is performed by up to three authentication methods in the indicated sequence.

RADIUS Settings

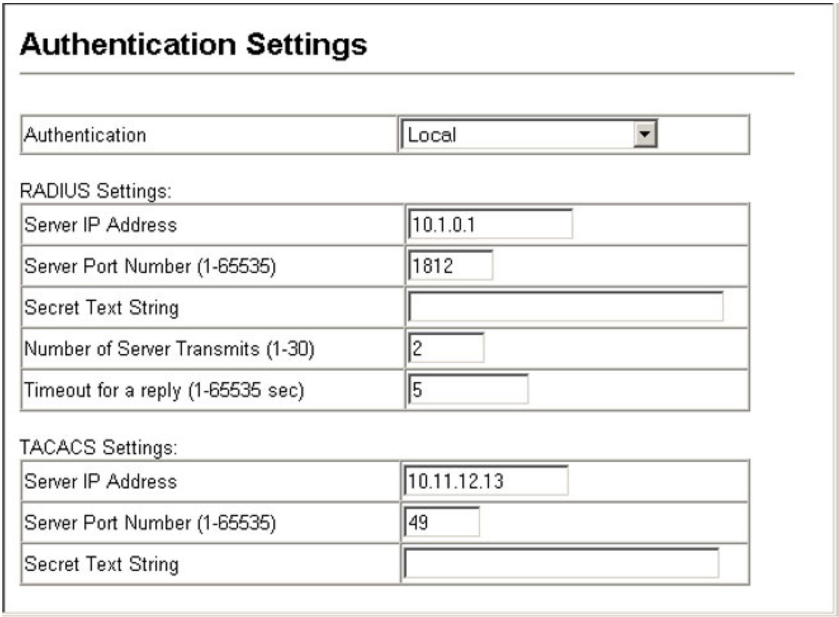
- **Server IP Address** – Address of the RADIUS server.
  (Default: 10.1.0.1)
- **Server Port Number** – Network (UDP) port of the RADIUS server used for authentication messages.
  (Range: 1-65535; Default: 1812)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
  (Maximum length: 48 characters)
- **Number of Server Transmits (1-30)** – Number of times the switch will try to authenticate logon access via the RADIUS server.
  (Range: 1-30; Default: 2)
- **Timeout for a reply (1-65535 sec)** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request.
  (Range: 1-65535; Default: 5)

TACACS Settings

- **Server IP Address** – Address of the TACACS+ server.
  (Default: 10.11.12.13)
- **Server Port Number (1-65535)** – Network (TCP) port of TACACS+ server used for authentication messages.
  (Range: 1-65535; Default: 49)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
  (Maximum length: 32 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI.

Web – Click Security, Authentication Settings. Specify the authentication sequence, server address, port number and other parameters, then click Apply.



Authentication Settings

Authentication	Local ▾

RADIUS Settings:

Server IP Address	10.1.0.1
Server Port Number (1-65535)	1812
Secret Text String	
Number of Server Transmits (1-30)	2
Timeout for a reply (1-65535 sec)	5

TACACS Settings:

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

CLI – Specify all the required parameters to enable login authentication.

```
Console(config)#authentication login radius                         3-118
Console(config)#radius-server host 192.168.1.25                     3-119
Console(config)#radius-server port 181                              3-119
Console(config)#radius-server key green                             3-120
Console(config)#radius-server retransmit 5                          3-120
Console(config)#radius-server timeout 10                            3-121
Console#show radius-server                                          3-121
Server IP address: 192.168.1.25
 Communication key with radius server: green
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Console(config)#
Console(config)#authentication login tacacs                         3-118
Console(config)#tacacs-server host 10.20.30.40                      3-121
Console(config)#tacacs-server port 200                              3-122
Console(config)#tacacs-server key green                             3-122
Console#show tacacs-server                                          3-123
Server IP address: 10.20.30.40
 Communication key with tacacs server: green
 Server port number: 200
 Console(config)#
```

Configuring HTTPS

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

Command Usage

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*].
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server’s digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
  A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x.
- The following Web browsers and operating systems currently support HTTPS:

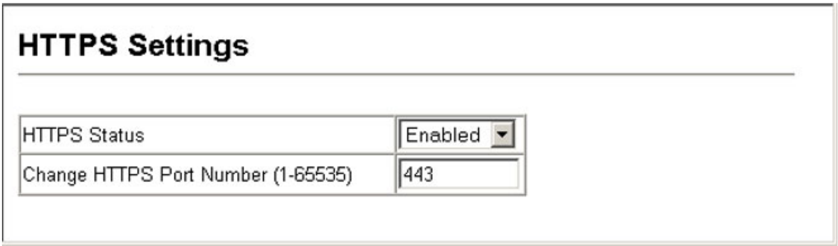
Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” on page 2-30.

Command Attributes

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch.
  (Default: Enabled)
- **Change HTTPS Port Number (1-65535)** – Specifies the UDP port number used for HTTPS/SSL connection to the switch’s Web interface.
  (Default: Port 443)

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



HTTPS Settings

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

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

```
Console(config)#ip http secure-server                                    3-35
Console(config)#ip http secure-port 443                                  3-36
Console(config)#
```

Replacing the Default Secure-site Certificate

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

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

When you have obtained these, place them on your TFTP server, and use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate                                       3-14
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

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

Configuring SSH

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

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

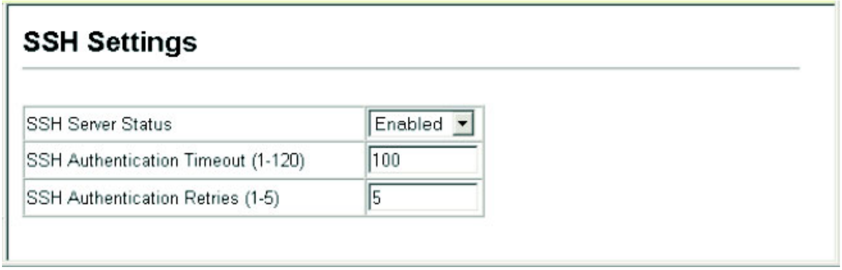
This section describes the commands used to configure the SSH server. However, note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

Note: The switch supports only SSH Version 1.5.

Command Attributes

- **SSH Server Status** – Allows you to enable/disable the SSH server feature on the switch. (Default: Enabled)
- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1 to 120 seconds; Default: 120 seconds)
- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)

Web – Click Security, SSH Settings. Enable SSH and adjust the authentication parameters as required, then click Apply.



SSH Settings

SSH Server Status	Enabled
SSH Authentication Timeout (1-120)	100
SSH Authentication Retries (1-5)	5

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

```
Console(config)#ip ssh server                                            3-37
Console(config)#ip ssh timeout 100                                       3-38
Console(config)#ip ssh authentication-retries 5                          3-38
Console(config)#
Console#show ip ssh                                                      3-39
Information of secure shell
SSH status: enable
SSH authentication timeout: 100
SSH authentication retries: 5
Console#show ssh                                                         3-40
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   1.5      cipher-3des   session-started
Console#disconnect ssh 0                                                 3-39
Console#
```

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port.

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. 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.

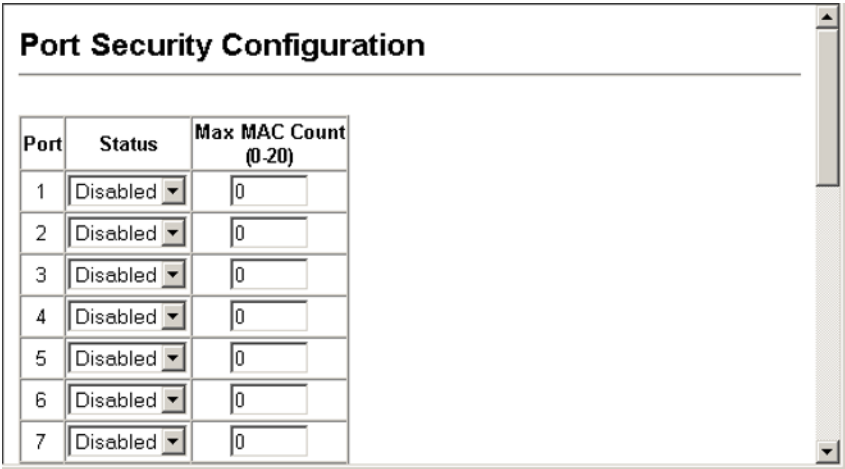
Command Usage

- Note that a secure port has the following restrictions:
  - It should not be connected to a network interconnection device.
  - It cannot be configured as a member of a static trunk.
  - It can be configured as an LACP trunk port, but the switch does not allow the LACP trunk to be enabled.
- A port that is already configured as an LACP or static trunk port cannot be enabled as a secure port.
- The default maximum number of MAC addresses allowed on a secure port is zero. You must configure a maximum address count from 1 - 20 for the port to allow access.

Command Attributes

- **Status** – Enables or disables port security on the port. (Default: disabled)
- **Max MAC Count (0-20)** – Sets the maximum number of MAC addresses that can be learned on a port when port security is enabled. (Range: 0 - 20, Default: 0)

Web – Click Security, Port Security Configuration. In the Status column for a port, select Enabled, then set the required Max MAC Count and click Apply.



Port Security Configuration

Port	Status	Max MAC Count (0-20)
1	Disabled	0
2	Disabled	0
3	Disabled	0
4	Disabled	0
5	Disabled	0
6	Disabled	0
7	Disabled	0

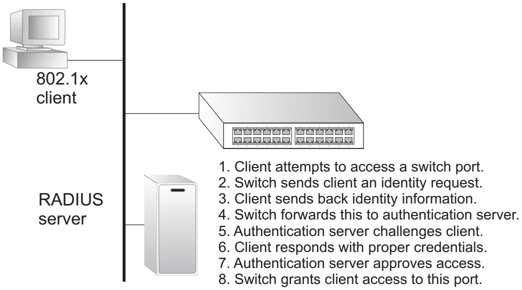
CLI – This example selects the target port, then uses the **port security max-mac-count** command to set the maximum MAC addresses allowed on that port. Use the **port security** command to enable security for the port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security max-mac-count 10
Console(config-if)#port security
Console(config-if)#
```

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.



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

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method can be MD5, TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security), or other. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

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.
- 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, TLS, TTLS, PEAP, etc. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

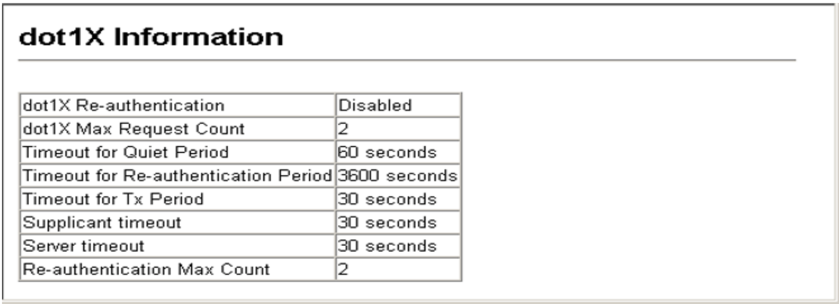
Displaying 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Command Attributes

- **dot1x Re-authentication -** Indicates if switch ports require a client to be re-authenticated after a certain period of time.
- **dot1x Max Request Count -** The maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session.
- **Timeout for Quiet Period -** Indicates the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client.
- **Timeout for Re-authentication Period -** Indicates the time period after which a connected client must be re-authenticated.
- **Timeout for TX Period -** The time period during an authentication session that the switch waits before re-transmitting an EAP packet.
- **Supplicant timeout -** The time the switch waits for a client response to an EAP request.
- **Server timeout -** The time the switch waits for a response from the RADIUS server to an authentication request.
- **Re-authentication Max Count -** The number of times the switch will attempt to re-authenticate a connected client before the port becomes unauthorized.

Web - Click 802.1X, Information.



dot1X Information

dot1X Re-authentication	Disabled
dot1X Max Request Count	2
Timeout for Quiet Period	60 seconds
Timeout for Re-authentication Period	3600 seconds
Timeout for Tx Period	30 seconds
Supplicant timeout	30 seconds
Server timeout	30 seconds
Re-authentication Max Count	2

CLI – This example shows the default protocol settings for dot1x. For a description of the additional entries displayed in the CLI, see “show dot1x” on 3-127.

```
Console#show dot1x                                                       3-127
Global 802.1X Parameters
reauth-enabled: no
reauth-period:  3600
quiet-period:   60
tx-period:      30
supp-timeout:   30
server-timeout: 30
reauth-max:     2
max-req:        2

802.1X Port Summary
 Port Name     Status          Mode          Authorized
         1       disabled    ForceAuthorized           n/a
         2       disabled    ForceAuthorized           yes
         3       disabled    ForceAuthorized           n/a
         4       disabled    ForceAuthorized           n/a
        ................................................
        23       disabled    ForceAuthorized           n/a
        24       disabled    ForceAuthorized           n/a
Console#
```

Configuring Global dot1x Parameters

The dot1x protocol includes global parameters that control the client 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. The configuration options for parameters are described in this section.

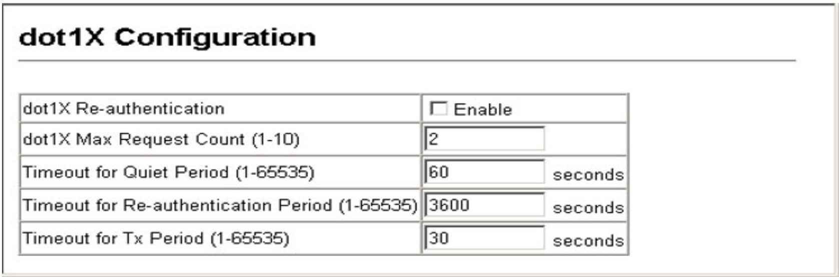
Command Attributes

- **dot1X Re-authentication -** Sets the client to be re-authenticated after the interval specified by the Timeout for Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port.
  (Default: Disabled)
- **dot1X Max Request Count (1-10) -** 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)
- **Timeout for Quiet Period (1-65535) -** Sets the time that a switch port waits after the dot1X Max Request Count has been exceeded before attempting to acquire a new client.
  (Range: 1-65535 seconds; Default: 60 seconds)
- **Timeout for Re-authentication Period (1-65535) -** Sets the time period after which a connected client must be re-authenticated.
  (Range: 1-65535 seconds; Default: 3600 seconds)
- **Timeout for TX Period (1-65535) -** Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet.
  (Range: 1-65535; Default: 30 seconds)

- **authentication dot1x*** – Sets the default authentication server type. Note the specified authentication server type must be enabled and properly configured for dot1x to function properly. (Options: radius)

* CLI only.

Web - Select 802.1X, Configuration. Enable dot1x globally for the switch, modify any of the parameters as required, and then click Apply.



dot1X Configuration

dot1X Re-authentication	□ Enable
dot1X Max Request Count (1-10)	2
Timeout for Quiet Period (1-65535)	60 seconds
Timeout for Re-authentication Period (1-65535)	3600 seconds
Timeout for Tx Period (1-65535)	30 seconds

CLI – This example enables re-authentication and sets all of the global parameters for dot1x.

```
Console(config)#dot1x max-req 5                                    3-124
Console(config)#dot1x re-authentication                            3-125
Console(config)#dot1x timeout quiet-period 40                      3-126
Console(config)#dot1x timeout re-auth 5                            3-126
Console(config)#dot1x timeout tx-period 40                         3-127
Console(config)#authentication dot1x default radius                3-123
Console(config)#
```

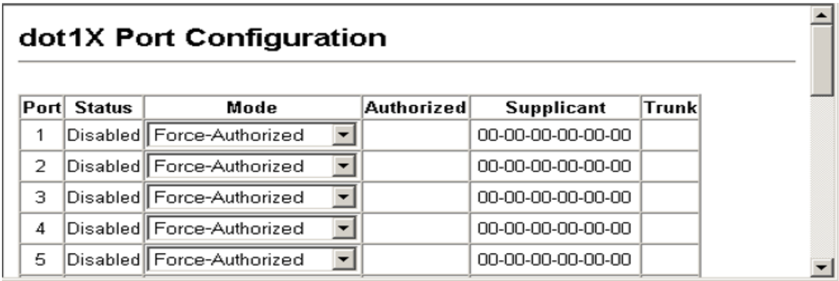
Configuring Port Authorization Mode

When dot1x is enabled, you need to specify the dot1x authentication mode configured for each port.

Command Attributes

- **Status** - Indicates if authentication is enabled or disabled on the port.
- **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.
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Authorized** –
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
  - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web - Select 802.1X, Port Configuration.



dot1X Port Configuration

Port	Status	Mode	Authorized	Supplicant	Trunk
1	Disabled	Force-Authorized		00-00-00-00-00-00	
2	Disabled	Force-Authorized		00-00-00-00-00-00	
3	Disabled	Force-Authorized		00-00-00-00-00-00	
4	Disabled	Force-Authorized		00-00-00-00-00-00	
5	Disabled	Force-Authorized		00-00-00-00-00-00	

CLI - In Interface mode type dot1x port-control auto, or use the no form to disable.

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x port-control auto                              3-124
Console(config-if)#
```

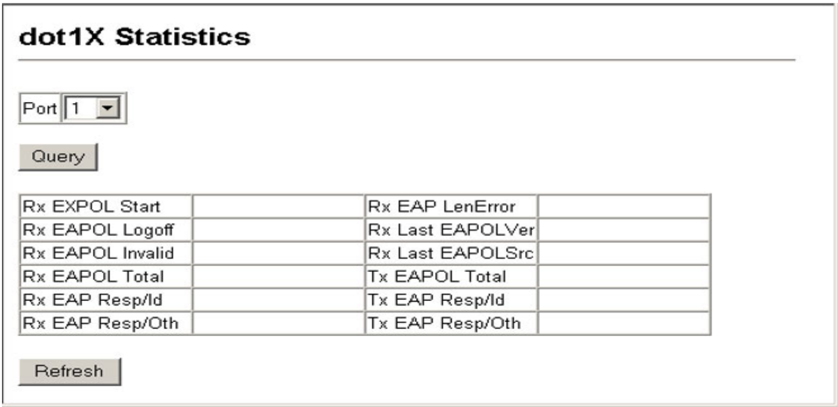
Displaying 802.1x Statistics

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

Statistical Values

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

Web – Select 802.1X, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.



dot1X Statistics

Port 1

Query

Rx EXPOL Start		Rx EAP LenError	
Rx EAPOL Logoff		Rx Last EAPOLVer	
Rx EAPOL Invalid		Rx Last EAPOLSrc	
Rx EAPOL Total		Tx EAPOL Total	
Rx EAP Resp/Id		Tx EAP Resp/Id	
Rx EAP Resp/Oth		Tx EAP Resp/Oth	

Refresh

CLI – This example displays the dot1x statistics for port 2.

```
Console#show dot1x statistics                                          3-127

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

    Last       Last
EAPOLVer     EAPOLSrc
       0     30-30-30-30-30-30

Tx: EAPOL      EAP       EAP
    Total     Req/Id   Req/Oth
       29       21         0
Console#
```

Access Control Lists

Access Control Lists (ACL) 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). 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 incoming packets against the conditions in an ACL one by one. If a list contains all permit rules, a packet will be accepted as soon as it passes any of the rules. If a list contains all deny rules, a packet will be rejected as soon as it fails any one of the rules. In other words, if no rules match for a permit list, the packet is dropped; and if no rules match for a deny list, the packet is accepted.

Note: An ACL can contain up to 32 rules.

Command Attributes

ACL Configuration – Setting the Name and Type

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

ACL Configuration – Configuring a Standard IP ACL

- **Action** – An ACL can contain all permit rules or all deny rules.
  (Default: Permit rules)
- **IP** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields.
  (Options: Any, Host, IP; Default: Any)
- **Address** – Source IP address.
- **SubMask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bit 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.

ACL Configuration – Configuring an Extended IP ACL

- **Action** – An ACL can contain all permit rules or all deny rules.
  (Default: Permit rules)
- **Src/Dst IP** – Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields.
  (Options: Any, Host, IP; Default: Any)
- **Src/Dst Address** – Source or destination IP address.
- **Src/Dst SubMask** – Subnet mask for source or destination address.
  (See SubMask in the preceding section.)
- **Service Type** – Specifies the service type.
  (Options: TOS, Precedence, DSCP; Default: TOS)
- **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)
- **Src/Dst Port (0-65535)** – TCP or UDP source/destination port number.
  (Range: 0-65535)
- **Control Code (0-63)** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header.
  (Range: 0-63)
- **Control Bitmask (0-63)** – Decimal number representing the code bits to match. The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:
  - SYN flag valid, use "control-flag 2 2"
  - Both SYN and ACK valid, use "control-flag 18 18"
  - SYN valid and ACK invalid, use "control-flag 2 18"

ACL Configuration – Configuring a MAC ACL

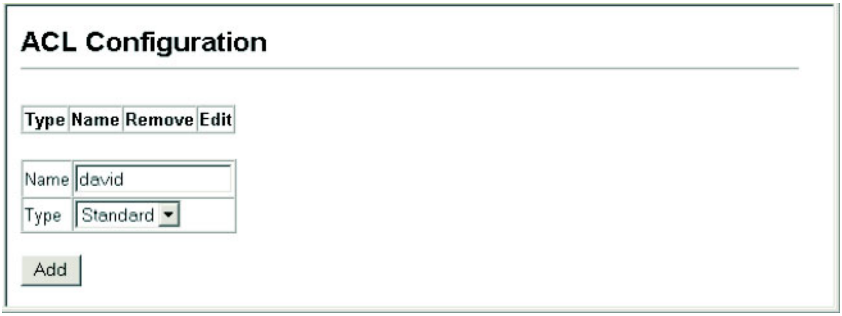
- **Action** – An ACL can contain all permit rules or all deny rules.
  (Default: Permit rules)
- **Source/Destination MAC** – Source or destination MAC.
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination Bitmask** – Binary mask for source or destination MAC address.

- **VID** – ID of VLAN.
- **Ethernet Type** – This 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 0800 (IP), 0806 (ARP), 8137 (IPX).

Examples

Creating a New ACL

Web –
1. Click ACL, Configuration.
2. Enter an ACL List name in the Name field.
3. Select the list type (Standard, Extend, or MAC).
4. Click Add to open the configuration page for the new list.



ACL Configuration

Type	Name	Remove	Edit

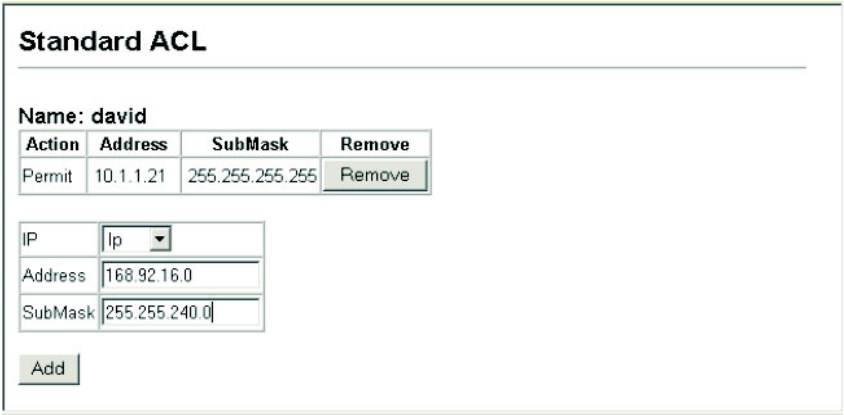
Name	david
Type	Standard ▾

CLI – This example creates a standard IP ACL named david.

```
Console(config)#access-list ip standard david                3-131
Console(config-std-acl)#
```

Standard IP ACL

Web –
1. Specify the action (i.e., Permit or Deny).
2. Select the address type (Any, Host, or IP), where Host means a specific address, and IP means an address range.
3. If you selected “Host” – enter the host address.
   If you selected “IP” – enter the subnet address and mask.
4. Click Add.



Standard ACL

Name: david

Action	Address	SubMask	Remove
Permit	10.1.1.21	255.255.255.255	Remove

IP	Ip
Address	168.92.16.0
SubMask	255.255.240.0

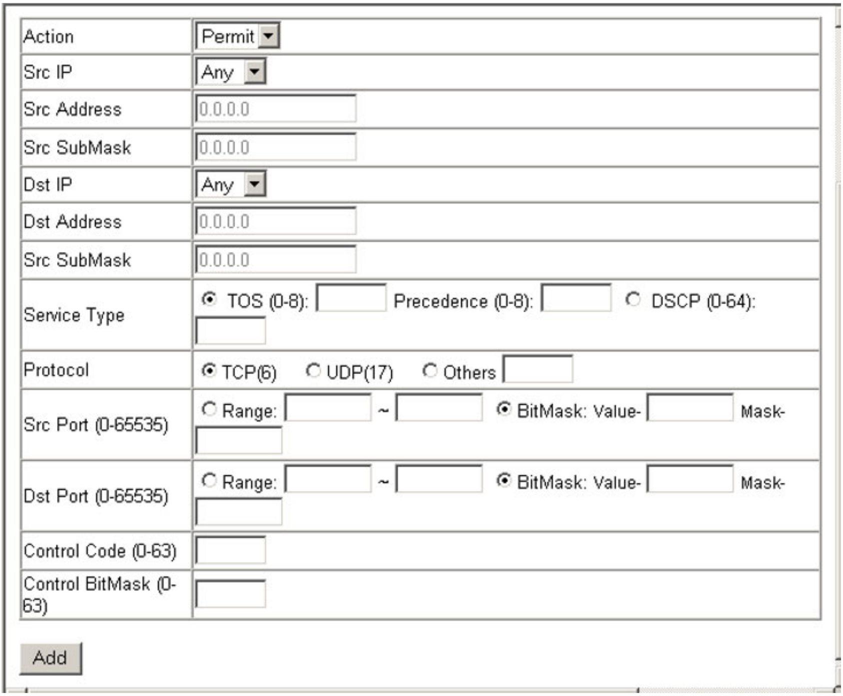
CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21                    3-132
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Extended IP ACL

Web –

1. Specify the action (i.e., Permit or Deny).
2. Select the source IP (Any, Host, or IP), where Host means a specific address, and IP means an address range.
3. If you selected “Host” – enter the host address.
   If you selected “IP” – enter the subnet address and mask.
4. Select the destination IP (Any, Host, or IP).
5. Specify the service type (TOS, Precedence, or DSCP).
6. Select the protocol type (TCP, UDP, or Others), where the range for others includes protocol numbers 0-255.
7. Enter the TCP/UDP source and destination port numbers. (Range: 0-65535)
8. If you selected TCP protocol type, then you can also specify the control code and control bitmask. (Range: 0-63)
9. Click Add.



Action	Permit ▾
Src IP	Any ▾
Src Address	0.0.0.0
Src SubMask	0.0.0.0
Dst IP	Any ▾
Dst Address	0.0.0.0
Src SubMask	0.0.0.0
Service Type	● TOS (0-8): Precedence (0-8): ○ DSCP (0-64):
Protocol	● TCP(6) ○ UDP(17) ○ Others
Src Port (0-65535)	○ Range: ~ ● BitMask: Value- Mask-
Dst Port (0-65535)	○ Range: ~ ● BitMask: Value- Mask-
Control Code (0-63)	
Control BitMask (0-63)	

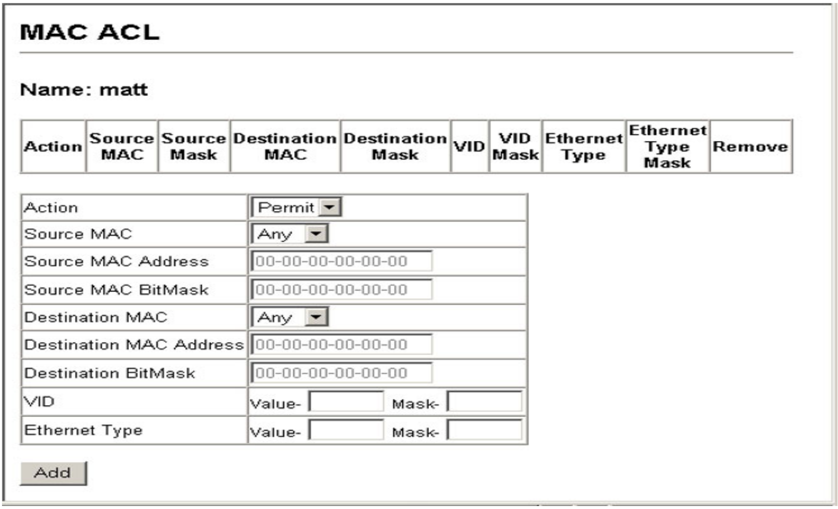
CLI – This example adds three rules:

1. Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.
2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).
3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any              3-133
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
 destination-port 80
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
 control-flag 2 2
Console(config-std-acl)#
```

MAC ACL

Web –
1. Specify the action (i.e., Permit or Deny).
2. Select the Source MAC address using a dash to separate each two digits (e.g., 11-22-33-44-55-66). Leave this field blank to specify any host address.
3. Specify the Source Mask using a binary bitmask to indicate an address range.
4. Specify the Destination MAC, and a Destination Mask if required.
5. Specify the VID and the Ethernet Type as a protocol number. (Range: 1536-65535; Default: all)
6. Click Add.



MAC ACL

Name: matt

Action	Source MAC	Source Mask	Destination MAC	Destination Mask	VID	VID Mask	Ethernet Type	Ethernet Type Mask	Remove

Action	Permit	
Source MAC	Any	
Source MAC Address	00-00-00-00-00-00	
Source MAC BitMask	00-00-00-00-00-00	
Destination MAC	Any	
Destination MAC Address	00-00-00-00-00-00	
Destination BitMask	00-00-00-00-00-00	
VID	Value-	Mask-
Ethernet Type	Value-	Mask-

CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
  ethertype 0800                                                     3-139
Console(config-mac-acl)#
```

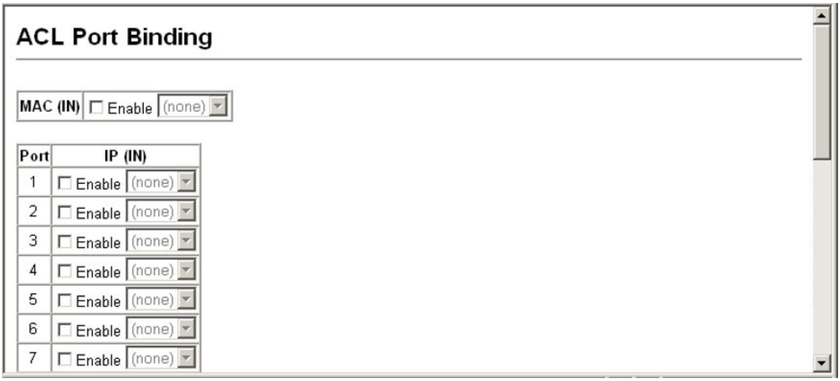
Binding a Port to an Access Control List

After configuring Access Control Lists (ACL), you should bind them to the ports that need to filter traffic. You can only assign one IP access list and/or one MAC access list to any port.

Command Attributes

- **MAC** – Specifies the MAC Access List to enable globally.
- **IP** – Specifies the IP Access List to enable for a port.

Web – Click Security, ACL, Port Binding. Mark the Enable field for the port you want to bind to an ACL, select the required ACL from the drop-down list, then click Apply.



ACL Port Binding

MAC (IN)	□ Enable (none)

Port	IP (IN)
1	□ Enable (none)
2	□ Enable (none)
3	□ Enable (none)
4	□ Enable (none)
5	□ Enable (none)
6	□ Enable (none)
7	□ Enable (none)

CLI – This example assigns an IP and MAC access list to port 1, and an IP access list to port 2.

```
Console(config)#interface ethernet 1/1                               3-66
Console(config-if)#ip access-group david in                          3-135
Console(config-if)#mac access-group jerry in                         3-140
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

Port Configuration

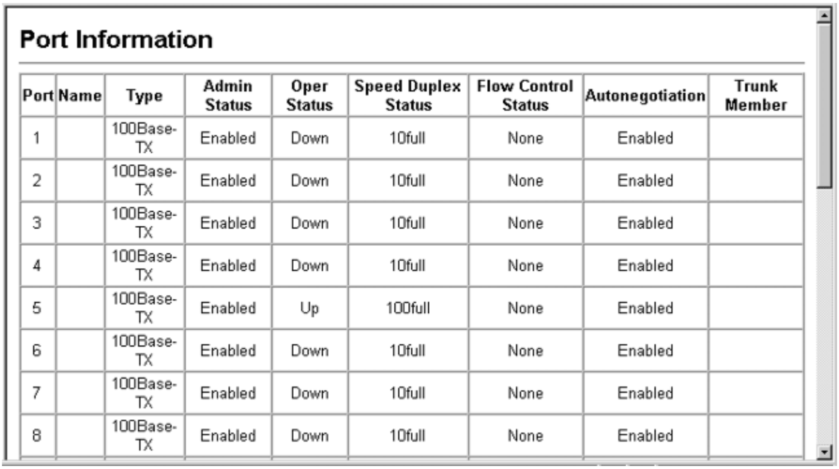
Displaying Connection Status

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

Command Attributes

- **Name** – Interface label.
- **Type** – Indicates the port type (10BASE-T, 100BASE-TX, 100BASE-FX, 1000BASE-SX, 1000BASE-LX, or 1000BASE-GBIC).
- **Admin Status** – Shows if the interface is enabled or disabled.
  Web: Displays Enabled or Disabled.
  CLI: Displays Port Admin (up or down).
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed Duplex Status** – Shows the current speed and duplex mode.
- **Flow Control Status** – Indicates the type of flow control currently in use.
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Trunk Member** – Shows if port is a trunk member. (Port Information only.)
- **Creation** – Shows if a trunk is manually configured. (Trunk Information only.)

Web – Click Port, Port Information or Trunk Information. Modify the required interface settings, and click Apply.



Port Information

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

CLI – This example shows the connection status for Port 13.

```
Console#show interfaces status ethernet 1/13                                3-73
Information of Eth 1/13
 Basic information:
  Port type: 100tx
  Mac address: 00-30-f1-47-58-46
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
 Current status:
  Link status: Down
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Command Attributes

- **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 reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows manual selection of port speed and duplex mode (i.e., with auto-negotiation disabled).
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control.The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **Sym** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames.
    (The current switch chip only supports symmetric pause frames.)
  - **FC** - Supports flow control

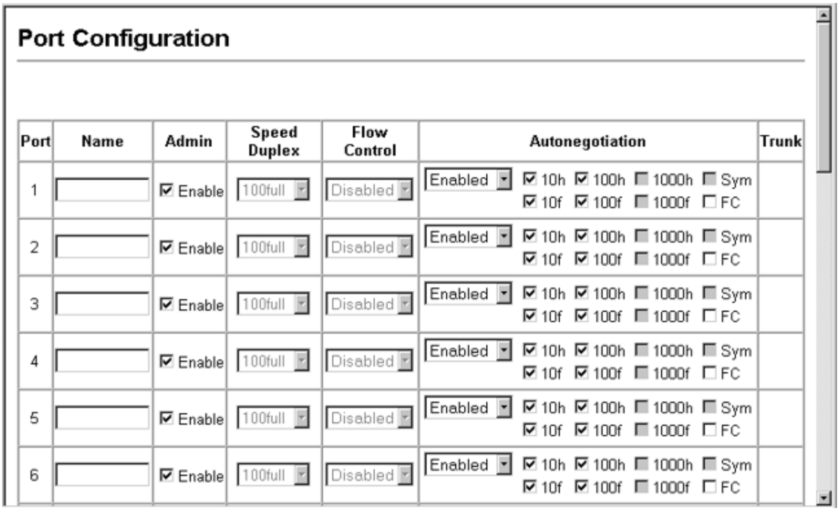
Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

(Default: Autonegotiation enabled; Advertised capabilities for;
100BASE-TX – 10half, 10full, 100half, 100full;
1000BASE-T – 10half, 10full, 100half, 100full, 1000full;
1000BASE-SX/LX/LH – 1000full)

- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see “Trunk Configuration” on page 2-51.

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

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



Port Configuration

Port	Name	Admin	Speed Duplex	Flow Control	Autonegotiation	Trunk
1		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
2		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
3		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
4		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
5		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
6		☑ Enable	100full	Disabled	Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13
Console(config-if)#description RD SW#13                                  3-66
Console(config-if)#shutdown                                              3-71
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                        3-68
Console(config-if)#speed-duplex 100half                                  3-67
Console(config-if)#flowcontrol                                           3-70
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                                  3-69
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
```

Trunk Configuration

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

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

Command Usage

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

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to six trunks on the switch, with up to four 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.
- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation.

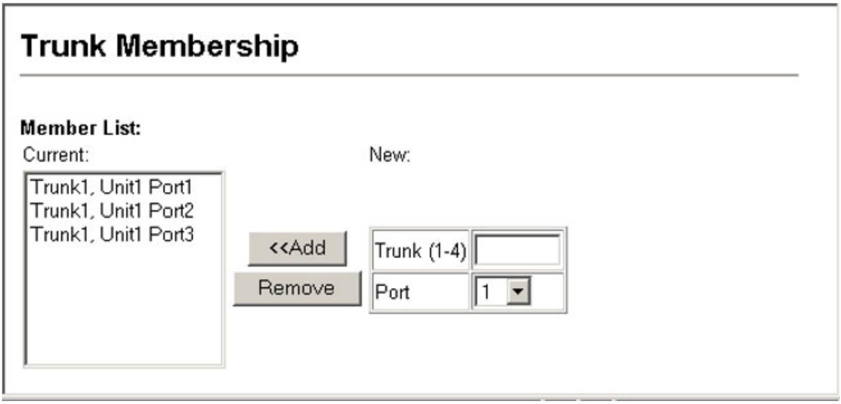
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Statically Configuring a Trunk

Command Usage

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

Web – Click Port, Trunk Membership. Enter a trunk ID of 1-4 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.



Trunk Membership

Member List:

Current:

Trunk1, Unit1 Port1
Trunk1, Unit1 Port2
Trunk1, Unit1 Port3

New:

Trunk (1-4)	
Port	1

CLI – This example creates trunk 1 with ports 11 and 12. Just connect these ports to two static trunk ports on another switch to form a trunk.

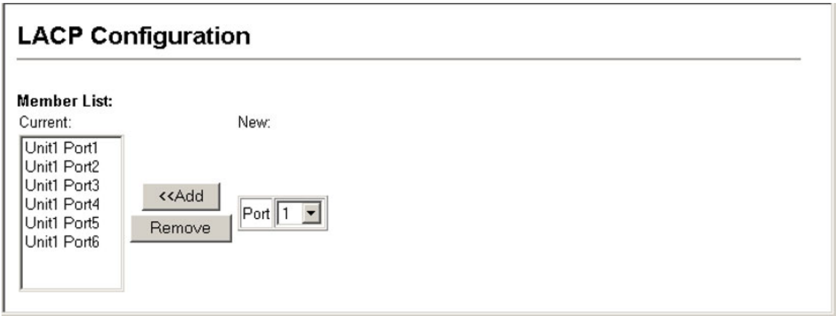
```
Console(config)#interface port-channel 1                                3-66
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1                                      3-112
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1                           3-73
Information of Trunk 1
 Basic information:
  Port type: 100tx
  Mac address: 22-22-22-22-22-2c
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control status: Disabled
 Current status:
  Created by: User
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12,
Console#
```

Dynamically Configuring a Trunk

Command Usage

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

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



CLI – The following example enables LACP for ports 17 and 18. Just connect these ports to two LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/17
Console(config-if)#lacp                                              3-112
Console(config-if)#exit
Console(config)#interface ethernet 1/18
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                       3-73
Information of Trunk 1
 Basic information:
  Port type: 100tx
  Mac address: 22-22-22-22-22-2d
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control status: Disabled
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/17, Eth1/18,
Console#
```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic. Any broadcast octets exceeding the specified threshold will then be dropped.

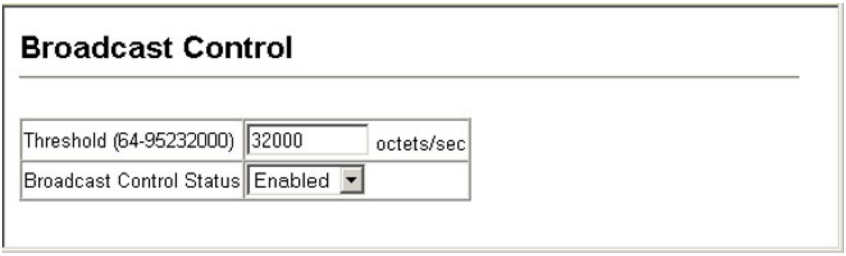
Command Usage

- Broadcast Control is enabled by default.
- The default threshold is 32000 octets per second.
- Broadcast control does not effect IP multicast traffic.
- The specified threshold applies to all ports on the switch.

Command Attributes

- **Threshold (64-95232000)** – Threshold as percentage of port bandwidth. (Options: 64-95232000 octets per second; Default: 32000 octets per second)
- **Broadcast Control Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)

Web – Click Port, Broadcast Control. Set the threshold for all ports, click Apply.



Broadcast Control

Threshold (64-95232000)	32000 octets/sec
Broadcast Control Status	Enabled

CLI – Specify an interface, and then enter the threshold. This threshold will then be set for all ports. The following sets broadcast suppression at 1000 octets per second.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport broadcast octet-rate 1000          3-72
Console(config-if)#
```

Configuring Port Mirroring

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

Command Usage

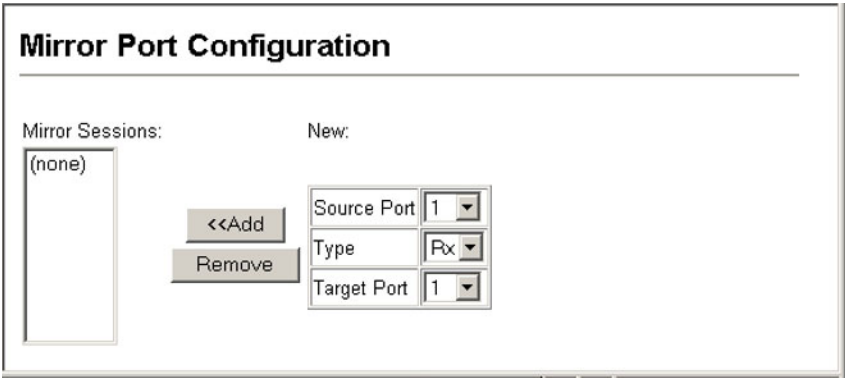
- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Unit** – The unit whose traffic will be monitored.

- **Source Port** – The port whose traffic will be monitored.
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), or Tx (transmit).
- **Target Port** – The port that will “duplicate” or “mirror” the traffic on the source port.

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



Mirror Port Configuration

Mirror Sessions: (none)

New:

Source Port	1
Type	Rx
Target Port	1

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

```
Console(config)#interface ethernet 1/10
Console(config-if)#port monitor ethernet 1/13                    3-109
Console(config-if)#
```

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on a port. Rate limiting is configured on ports at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

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

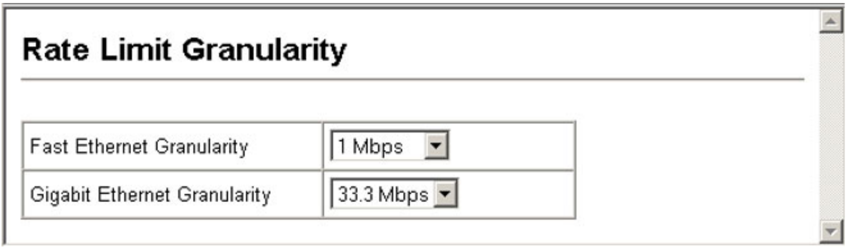
Rate Limit Granularity

Rate limit granularity is an additional feature enabling the network manager greater control over traffic on the network. The "rate limit granularity" is multiplied by the "rate limit level" (page 2-57) to set the actual rate limit for an interface. Granularity is a global setting that applies to Fast Ethernet or Gigabit Ethernet interfaces.

Command Usage

- For Fast Ethernet interfaces, the rate limit granularity is 512 Kbps, 1 Mbps, or 3.3 Mbps.
- For Gigabit Ethernet interfaces, the rate limit granularity is 33.3 Mbps.

Web - Click Port, Rate Limit, Granularity. Choose the required rate limit granularity for Fast Ethernet and Gigabit Ethernet, and click Apply.



Rate Limit Granularity

Fast Ethernet Granularity	1 Mbps
Gigabit Ethernet Granularity	33.3 Mbps

CLI - This example displays Fast Ethernet and Gigabit Ethernet granularity.

```
Console(config)#rate-limit fastethernet granularity 1000              3-115
Console(config)#rate-limit gigabitethernet granularity 33300          3-115
Console(config)#exit
Console#show rate-limit                                               3-115

Fast ethernet granularity:  1000

Gigabit ethernet granularity:  33300
Console#
```

Rate Limit Configuration

Use the rate limit configuration pages to apply rate limiting.

Command Usage

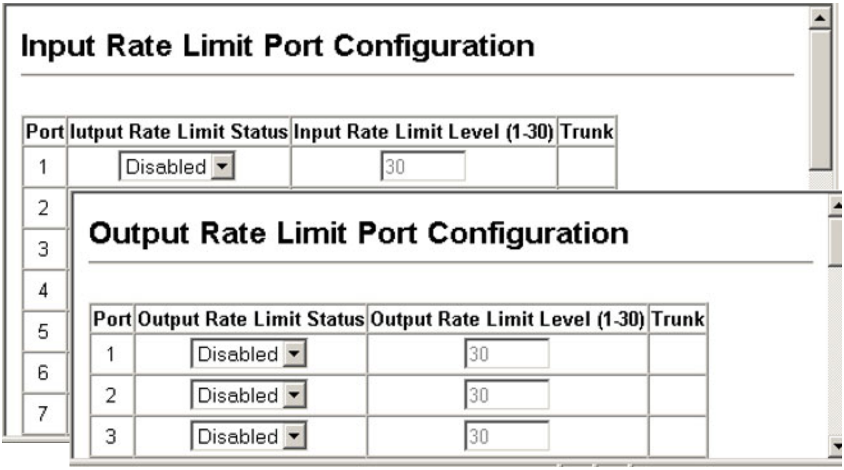
- Input and output rate limit can be enabled or disabled for individual interfaces.

Command Attributes

- **Port/Trunk**– Displays the port number.
- **Rate Limit Status** – Enables or disables the rate limit.
- **Rate Limit Level (1-30)** – Sets the rate limit level. (Range: 1-30; Default: 30)

Note: Actual rate limit = Rate Limit Level * Granularity

Web - Click Port, Rate Limit, Input/Output Port/Trunk Configuration. Enable the Rate Limit Status for the required interfaces, set the Rate Limit Level, and click Apply.



Input Rate Limit Port Configuration

Port	Iutput Rate Limit Status	Input Rate Limit Level (1-30)	Trunk
1	Disabled ▾	30	
2			
3			
4			
5			
6			
7			

Output Rate Limit Port Configuration

Port	Output Rate Limit Status	Output Rate Limit Level (1-30)	Trunk
1	Disabled ▾	30	
2	Disabled ▾	30	
3	Disabled ▾	30	

CLI - This example sets the rate limit level for input and output traffic passing through port 3 and 4.

```
Console(config)#interface ethernet 1/3                                  3-66
Console(config-if)#rate-limit input level 3                             3-114
Console(config-if)#rate-limit output level 3                            3-114
Console(config-if)#exit
Console(config)#interface ethernet 1/4
Console(config-if)#rate-limit input level 6
Console(config-if)#rate-limit output level 6
Console(config-if)#
```

Showing Port Statistics

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

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

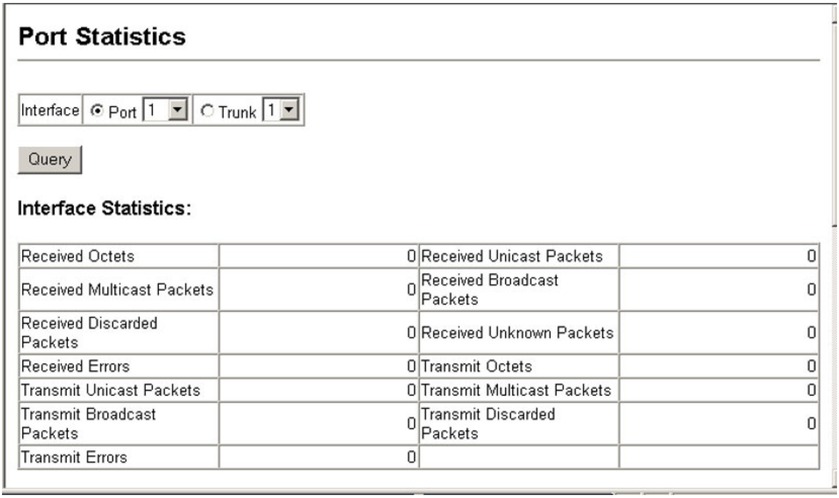
Statistical Values

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.

Parameter	Description
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.

Parameter	Description
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

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

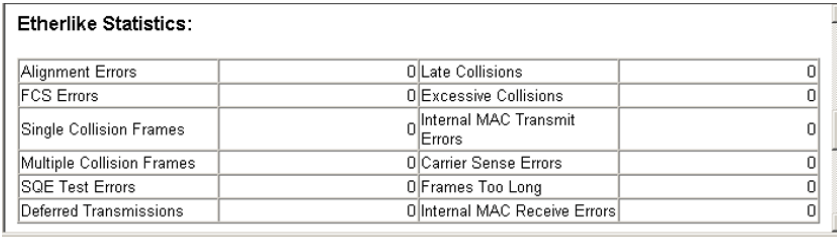


Port Statistics

Interface ● Port 1 ○ Trunk 1

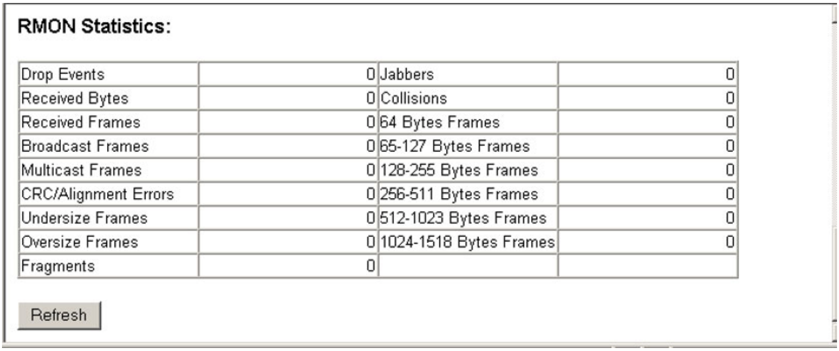
Interface Statistics:

Received Octets	0	Received Unicast Packets	0
Received Multicast Packets	0	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	0
Transmit Unicast Packets	0	Transmit Multicast Packets	0
Transmit Broadcast Packets	0	Transmit Discarded Packets	0
Transmit Errors	0		



Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0



RMON Statistics:

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

CLI – This example shows statistics for port 13.

```
Console#show interfaces counters ethernet 1/13                           3-74
Ethernet 1/13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unicast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets:
   871
Console#
```

Address Table Settings

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

Setting Static Addresses

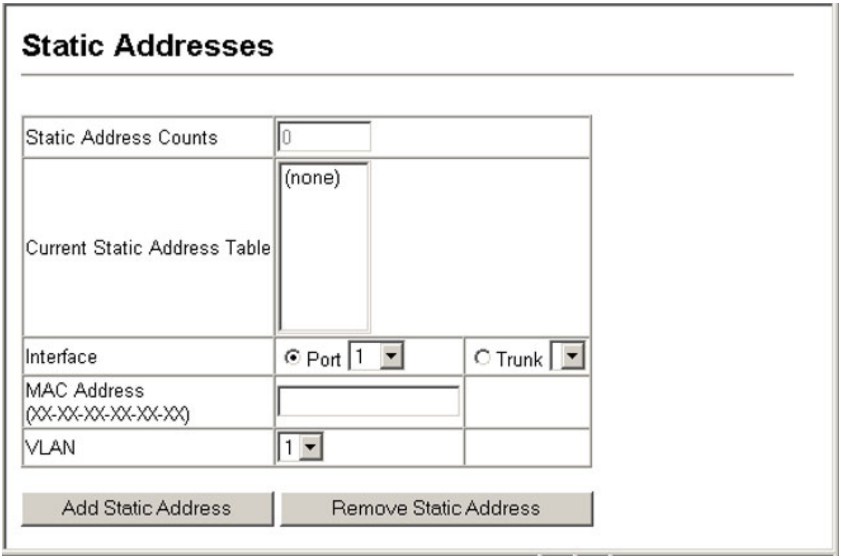
A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

- **Static Address Counts*** – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4094).

* Web Only.

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



Static Addresses

Static Address Counts	0	
Current Static Address Table	(none)	
Interface	● Port 1	○ Trunk
MAC Address (XX-XX-XX-XX-XX-XX)		
VLAN	1	

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

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
 ethernet 1/1 vlan 1 delete-on-reset                                  3-77
Console(config)#
```

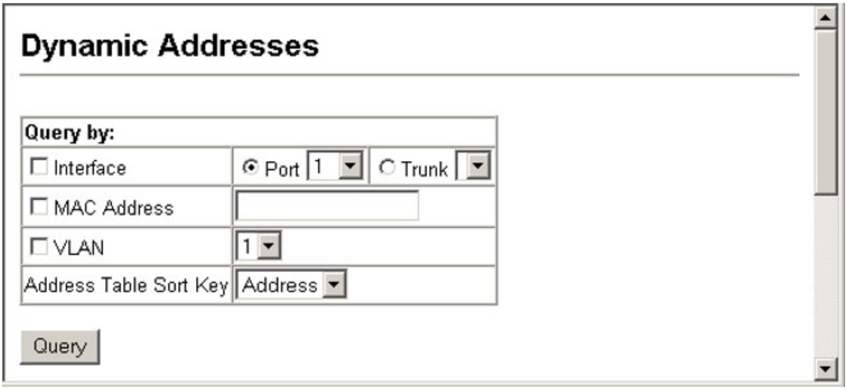
Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

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

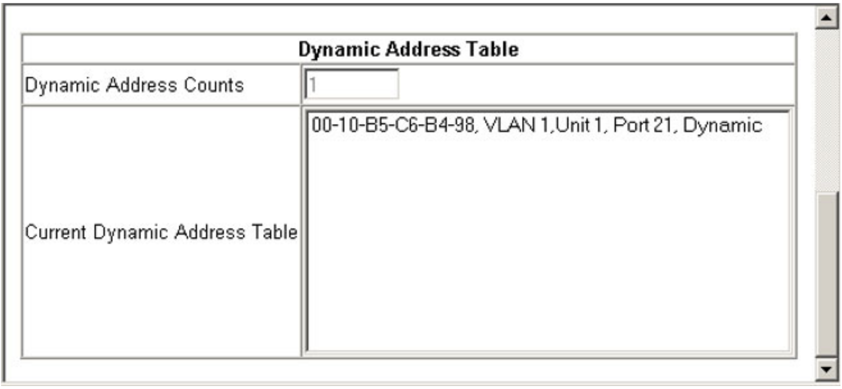
Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., Interface, MAC Address, or VLAN), the method of sorting the displayed addresses, then click Query.



Dynamic Addresses

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

For example, the following screen shows the dynamic addresses for port 7.



Dynamic Address Table

Dynamic Address Counts	1
Current Dynamic Address Table	00-10-B5-C6-B4-98, VLAN 1,Unit 1, Port 21, Dynamic

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

```
Console#show mac-address-table ethernet 1/11                          3-78
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/11 00-10-b5-62-03-74    1 Learned
Console#
```

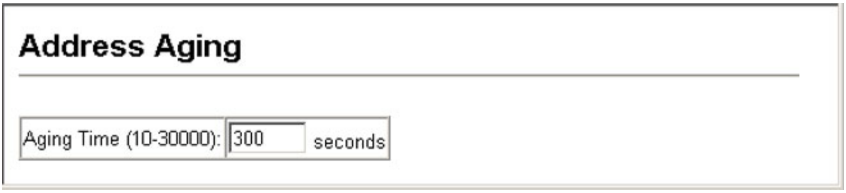
Changing the Aging Time

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

Command Attributes

- **Aging Time (10-30000)** – The time after which a learned entry is discarded. (Range: 10-30000 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, then click Apply.



Address Aging

Aging Time (10-30000): 300 seconds

CLI – This example sets the aging time to 300 seconds.

```
Console(config)#mac-address-table aging-time 300                      3-79
Console(config)#
Console#
Console#show mac-address-table aging-time                             3-78
 Aging time: 300 sec.
Console#
```

Spanning Tree Algorithm Configuration

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

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

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

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device.
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. It then selects a port on the designated bridging device to communicate with each attached LAN or host device as a designated port. 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.

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

RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves must faster reconfiguration (i.e., around one tenth of the time required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Displaying Global Settings

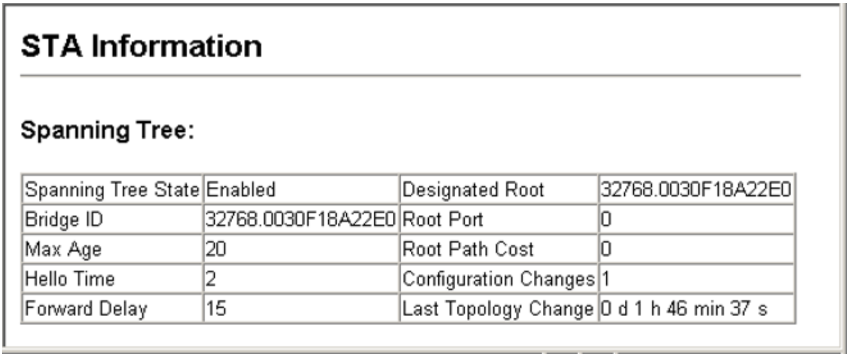
Command Attributes

- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority and MAC address (where the address is taken from the switch system).

- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
- **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Root Hello Time*** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age*** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)
- **Root Forward Delay*** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Root Hold Time*** – The interval (in seconds) during which no more than two bridge configuration protocol data units shall be transmitted by this node.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

* CLI only.

Web – Click Spanning Tree, STA, Information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0030F18A22E0
Bridge ID	32768.0030F18A22E0	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	1
Forward Delay	15	Last Topology Change	0 d 1 h 46 min 37 s

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

```
Console#show spanning-tree                                          3-90
Bridge-group information
--------------------------------------------------------------
Spanning tree protocol :IEEE Std 8021D
Spanning tree enable/disable :enable
Priority :32768
Hello Time (sec.) :2
Max Age (sec.) :20
Forward Delay (sec.) :15
Designated Root :32768.0030f147583a
Current root port :0
Current root cost :0
Number of topology changes :1
Last topology changes time (sec.):26696
Hold times (sec.) :1
---------------------------------------------------------------
Eth 1/ 1 information
--------------------------------------------------------------
Admin status : enable
STA state : broken
Path cost : 18
Priority : 128
Designated cost : 0
Designated port : 128.1
Designated root : 32768.0030f147583a
Designated bridge : 32768.0030f147583a
Fast forwarding : disable
Forward transitions : 0
...
```

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

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

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.

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D; i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode)
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w) RSTP is the default.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

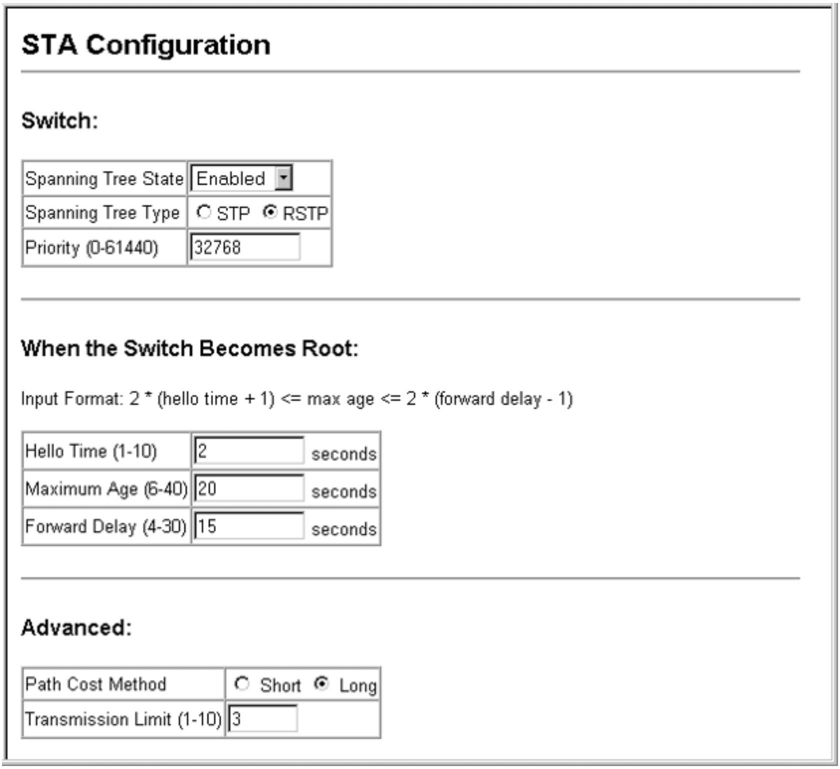
Root Device Configuration

- **Hello Time** – Interval (in seconds) at which this device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (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

Advanced Configuration Settings for RSTP

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
  - Long: Specifies 32-bit based values that range from 1-200,000,000.
  - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Web – Click Spanning Tree, STA, Configuration. Modify the required attributes, click Apply.



STA Configuration

Switch:

Spanning Tree State	Enabled
Spanning Tree Type	○ STP ● RSTP
Priority (0-61440)	32768

When the Switch Becomes Root:

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

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

Advanced:

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

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

```
Console(config)#spanning-tree                                        3-80
Console(config)#spanning-tree mode stp                               3-81
Console(config)#spanning-tree priority 40000                         3-84
Console(config)#spanning-tree hello-time 5                           3-83
Console(config)#spanning-tree max-age 38                             3-83
Console(config)#spanning-tree forward-time 20                        3-82
Console(config)#spanning-tree pathcost method long                   3-84
Console(config)#spanning-tree transmission-limit 5                   3-85
Console(config)#
```

Displaying Interface Settings

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

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA Status** – Displays current state of this port within the Spanning Tree:
  - **Discarding** – Port receives STA configuration messages, but does not forward packets.
  - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** – Port forwards packets, and continues learning addresses.

  The rules defining port status are:

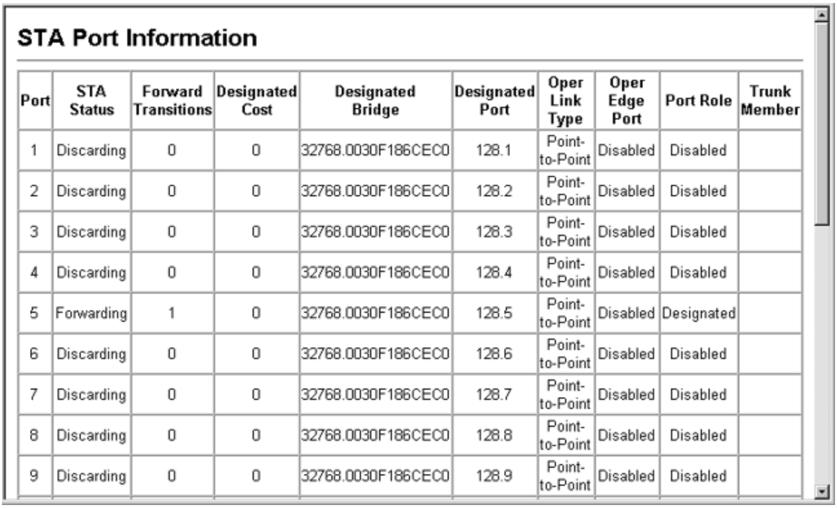
  - A port on a network segment with no other STA compliant bridging device is always forwarding.
  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has changed from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 2-76.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 2-76 (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 spanning tree topology:
  - **Root**: The port is connecting the bridge to the root bridge.
  - **Designated**: The port is connecting a LAN through the bridge to the root bridge.
  - **Alternate** or **Backup**: A port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed.

  - **Disabled**: The role is set to disabled if a port has no role within the spanning tree.
- **Trunk Member** – Indicates if a port is a member of a trunk.
  (STA Port Information only)

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if STA has been enabled on this interface.
- **Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin 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.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

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



STA Port Information

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Discarding	0	0	32768.0030F186CEC0	128.1	Point-to-Point	Disabled	Disabled	
2	Discarding	0	0	32768.0030F186CEC0	128.2	Point-to-Point	Disabled	Disabled	
3	Discarding	0	0	32768.0030F186CEC0	128.3	Point-to-Point	Disabled	Disabled	
4	Discarding	0	0	32768.0030F186CEC0	128.4	Point-to-Point	Disabled	Disabled	
5	Forwarding	1	0	32768.0030F186CEC0	128.5	Point-to-Point	Disabled	Designated	
6	Discarding	0	0	32768.0030F186CEC0	128.6	Point-to-Point	Disabled	Disabled	
7	Discarding	0	0	32768.0030F186CEC0	128.7	Point-to-Point	Disabled	Disabled	
8	Discarding	0	0	32768.0030F186CEC0	128.8	Point-to-Point	Disabled	Disabled	
9	Discarding	0	0	32768.0030F186CEC0	128.9	Point-to-Point	Disabled	Disabled	

CLI – This example shows general STA configuration and attributes for all ports.

```
Console#show spanning-tree ethernet 1/5                              3-90
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode                 :RSTP
 Spanning tree enable/disable       :enable
 Priority                           :32768
 Bridge Hello Time (sec.)           :2
 Bridge Max Age (sec.)              :20
 Bridge Forward Delay (sec.)        :15
 Root Hello Time (sec.)             :2
 Root Max Age (sec.)                :20
 Root Forward Delay (sec.)          :15
 Designated Root                    :32768.00A0CA445566
 Current root port                  :0
 Current root cost                  :0
 Number of topology changes         :2
 Last topology changes time (sec.):2209
 Transmission limit                 :5
 Path Cost Method                   :long
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin status           : enable
 Role                   : disable
 State                  : discarding
 Path cost              : 100000
 Priority               : 128
 Designated cost        : 0
 Designated port        : 128.1
 Designated root        : 32768.00A0CA445566
 Designated bridge      : 32768.00A0CA445566
 Forward transitions    : 0
 Fast forwarding        : disable
 Admin edge port        : disable
 Oper edge port         : disable
 Admin Link type        : auto
 Oper Link type         : point-to-point
---More---
```

Configuring Interface Settings

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

Command Attributes

The following attributes are read-only and cannot be changed:

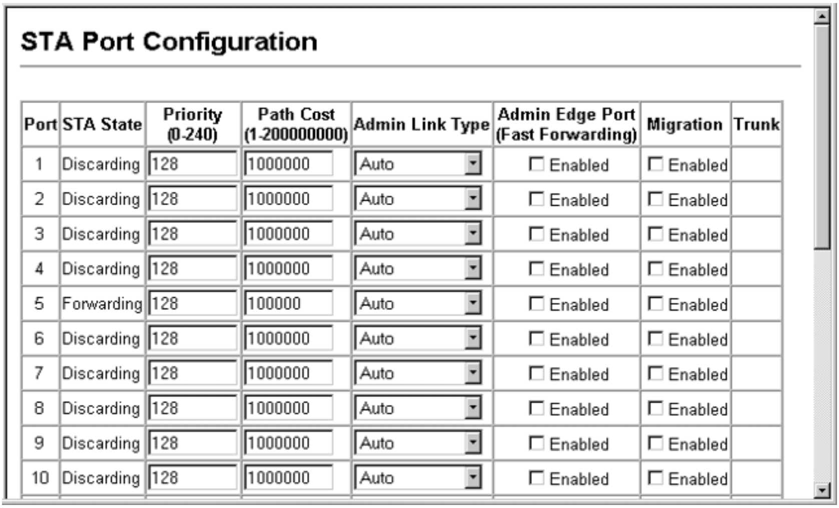
- **Port** – Ports only; i.e., no trunks or trunk port members.
- **STA State** – Displays current state of this port within the spanning tree:
  - **Discarding** – Port receives STA configuration messages, but does not forward packets.
  - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** – Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

The following interface attributes can be configured:

- **Priority (0-240)** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16
- **Path Cost (1-200000000)** – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-84), the maximum path cost is 65,535.
  - Range –
    - Ethernet: 200,000-20,000,000
    - Fast Ethernet: 20,000-2,000,000
    - Gigabit Ethernet: 2,000-200,000
  - Default –
    - Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
    - Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
    - Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

- **Admin Link Type** – The link type attached to this interface.
  - **Point-to-Point** – A connection to exactly one other bridge.
  - **Shared** – A connection to two or more bridges.
  - **Auto** – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.
- **Admin Edge Port (Fast Forwarding)** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

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



STA Port Configuration

Port	STA State	Priority (0-240)	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	
2	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	
3	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	
4	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	
5	Forwarding	128	100000	Auto	□ Enabled	□ Enabled	
6	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	
7	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	
8	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	
9	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	
10	Discarding	128	1000000	Auto	□ Enabled	□ Enabled	

CLI – This example sets STA attributes for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0                    3-86
Console(config-if)#spanning-tree cost 50                            3-86
Console(config-if)#spanning-tree portfast                           3-87
```

VLAN Configuration

Overview

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 videoconferencing).

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

This switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

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

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

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

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

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in “Adding Static Members to VLANs (VLAN Index)” on page 2-84). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

Forwarding Tagged/Untagged Frames

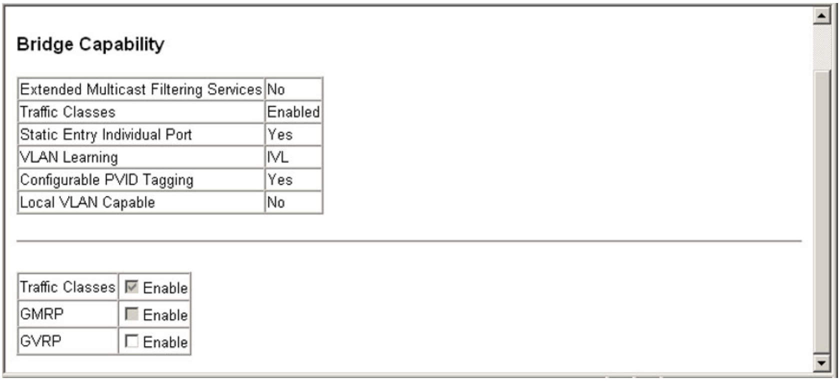
If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

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

Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

Web – Click System, Bridge Extension Configuration. Enable or disable GVRP, click Apply.



Bridge Capability

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

Traffic Classes	☑ Enable
GMRP	□ Enable
GVRP	□ Enable

CLI – This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp                                    3-108
Console(config)#
```

Displaying Basic VLAN Information

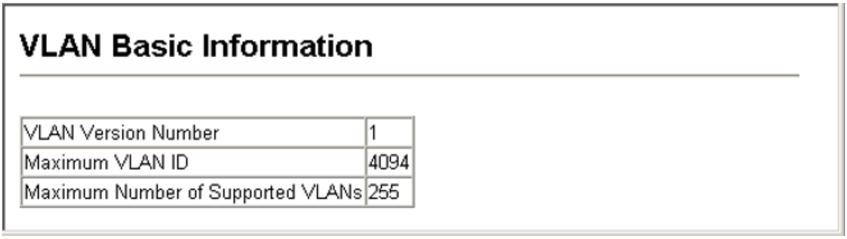
The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Command Attributes

- **VLAN Version Number*** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

* Web only.

Web – Click VLAN, 802.1Q VLAN, Basic Information.



VLAN Basic Information

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

CLI – Enter the following command.

```
Console#show bridge-ext                                           3-108
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

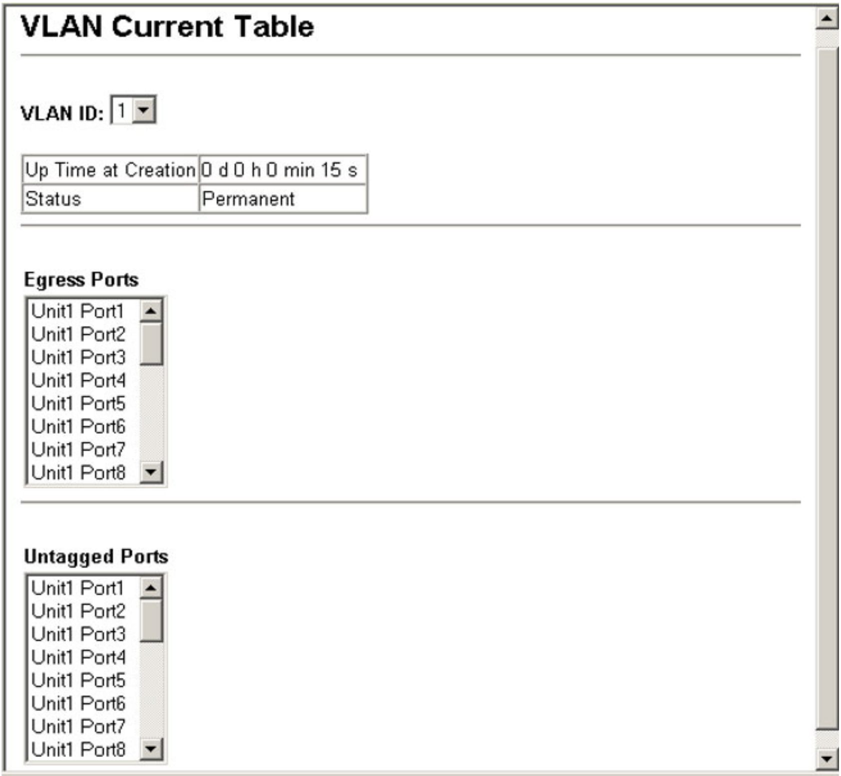
Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).
- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.
  - **Permanent**: Added as a static entry.
- **Egress Ports** – Shows all the VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

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



VLAN Current Table

VLAN ID: 1

Up Time at Creation	0 d 0 h 0 min 15 s
Status	Permanent

Egress Ports

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

Untagged Ports

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

Command Attributes (CLI)

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

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

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                                3-99
VLAN Type    Name                Status    Ports/Channel groups
  1  Static  DefaultVlan         Suspended Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4
                                           Eth1/ 5 Eth1/ 6 Eth1/ 7 Eth1/ 8
                                           Eth1/ 9 Eth1/10 Eth1/11 Eth1/12
                                           Eth1/13 Eth1/14 Eth1/15 Eth1/16
                                           Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                           Eth1/21 Eth1/22 Eth1/23 Eth1/24
 Console#
```

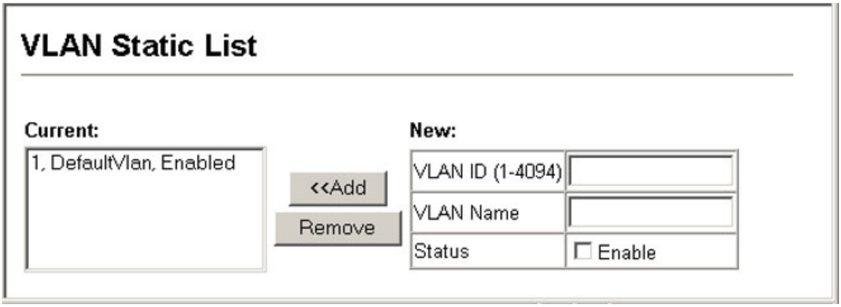
Creating VLANs

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

Command Attributes

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

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



VLAN Static List

Current:

1. DefaultVlan, Enabled

New:

VLAN ID (1-4094)

VLAN Name

Status □ Enable

CLI – This example creates a new VLAN.

```
Console(config)#vlan database                                            3-92
Console(config)#vlan 2 name R&D media ethernet state active              3-93
Console(config)#end
Console#show vlan                                                        3-99
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ---------------------------------------
   1  Static      DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                        Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                        Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                        Eth1/21 Eth1/22 Eth1/23 Eth1/24 Eth1/25
                                        Eth1/26
   2  Static              R&D    Active
Console(config-vlan)
```

Adding Static Members to VLANs (VLAN Index)

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

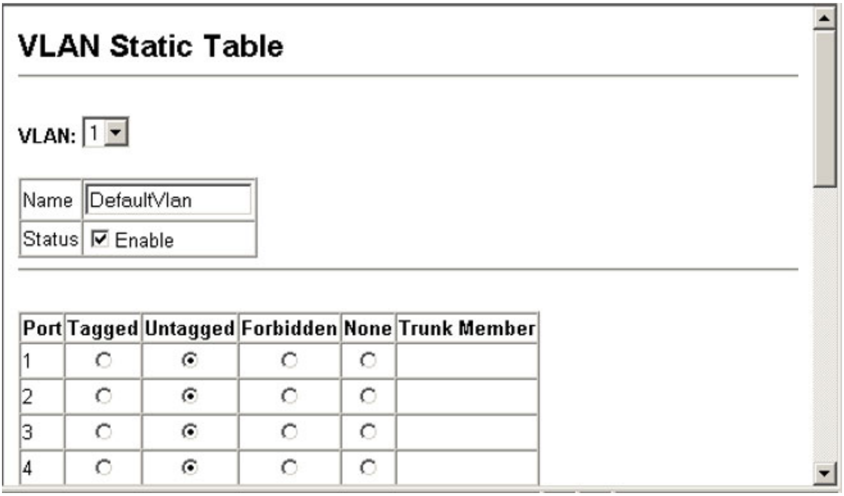
Notes: **1.** You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index. (See “Adding Static Members to VLANs (Port Index)” on page 2-86.) However, note that this configuration page can only add ports to a VLAN as tagged members.

2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under “Configuring VLAN Behavior for Interfaces” on page 2-87.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see “Automatic VLAN Registration” on page 2-79.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.



VLAN Static Table

VLAN: 1

Name	DefaultVlan
Status	☑ Enable

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

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

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 2 tagged              3-97
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

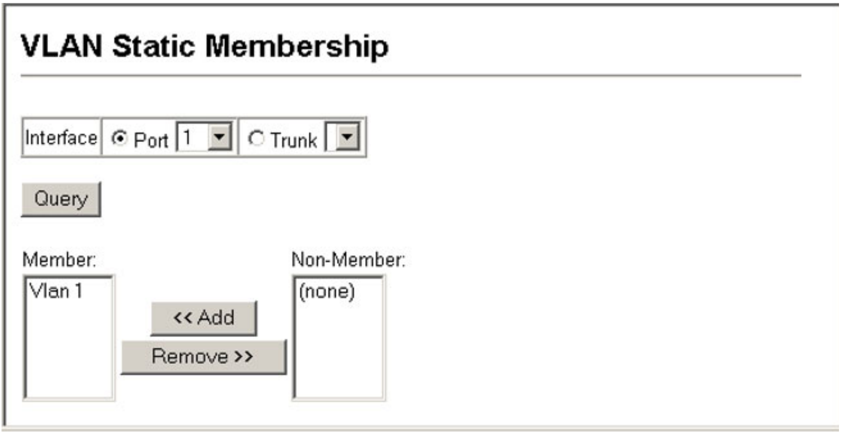
Adding Static Members to VLANs (Port Index)

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

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

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



VLAN Static Membership

Interface: ● Port 1 ○ Trunk

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

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport allowed vlan add 1 tagged              3-97
Console(config-if)#switchport allowed vlan remove 2
```

Configuring VLAN Behavior for Interfaces

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

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

Command Attributes

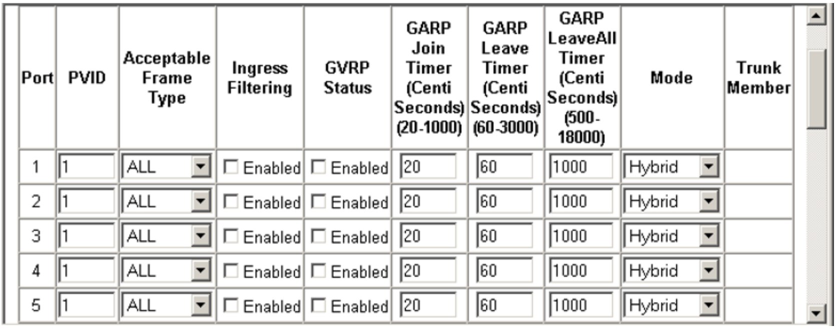
- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)
  - If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)
- **Ingress Filtering** – If ingress filtering is enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port. (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, it does affect VLAN dependent BPDU frames, such as GMRP.
- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See “Displaying Bridge Extension Capabilities” on page 2-10.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)
- **GARP Join Timer*** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)

- **GARP Leave Timer*** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
- **GARP LeaveAll Timer*** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.
  (Range: 500-18000 centiseconds; Default: 1000)

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

- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.
- **Mode** – Indicates VLAN membership mode for an interface. (Default: 1Q Trunk)
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

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



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

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

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged          3-95
Console(config-if)#switchport ingress-filtering                      3-96
Console(config-if)#switchport native vlan 3                          3-97
Console(config-if)#switchport gvrp                                   3-105
Console(config-if)#garp timer join 20                                3-106
Console(config-if)#garp timer leave 90                               3-106
Console(config-if)#garp timer leaveall 2000                          3-106
Console(config-if)#switchport mode hybrid                            3-95
Console(config-if)#
```

Private VLANs

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

Each private VLAN consists of three components: a primary VLAN, an isolated VLAN, and one or more community VLANs. A primary VLAN allows traffic to pass between promiscuous ports, and between promiscuous ports and isolated or community ports subordinate to the primary VLAN. An isolated VLAN allows traffic to pass only between isolated ports and promiscuous ports, all other traffic between ports in the VLAN is blocked. A community VLAN conveys traffic between community ports, and from the community ports to their associated promiscuous ports. Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be configured within each primary VLAN. However, only one isolated VLAN can be associated with each primary VLAN.

To configure private VLANs, follow these steps:

1. Use the Private VLAN Configuration menu (page 2-90) to designate one or more isolated and community VLANs, and the primary VLAN that will channel traffic outside of the VLAN groups.
2. Use the Private VLAN Association menu (page 2-91) to map the secondary (i.e., isolated and community) VLAN(s) to the primary VLAN.
3. Use the Private VLAN Port Configuration menu (page 2-93) to set the port type to promiscuous (i.e., having access to all ports in the primary VLAN), isolated (i.e., having access only to promiscuous ports in its own VLAN), or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through a promiscuous port). Then assign any promiscuous ports to a primary VLAN and any host ports a secondary VLAN (i.e., community VLAN).

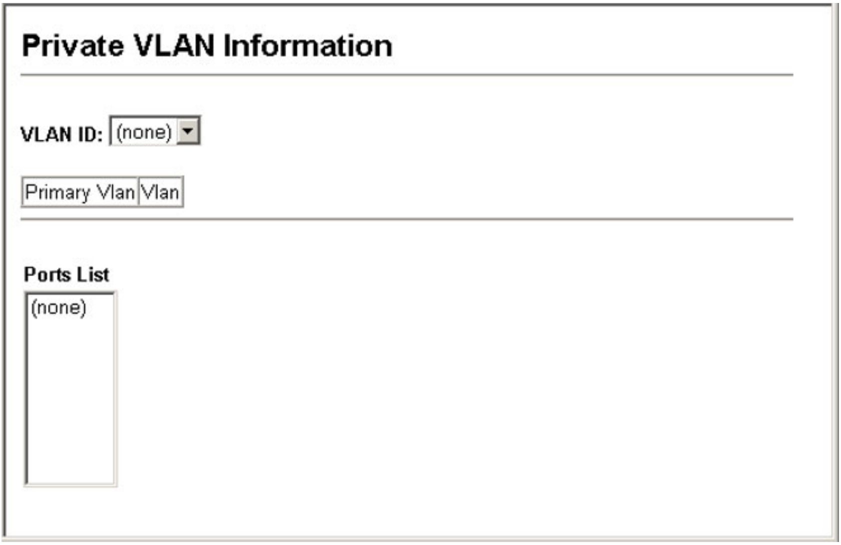
Displaying Current Private VLANs

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

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Primary VLAN** – The primary VLAN with which the selected VLAN is associated. (Note that this displays as VLAN 0 if the selected VLAN is itself a primary VLAN.)
- **Ports List** – The list of ports (and assigned type) in the selected private VLAN.

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



Private VLAN Information

VLAN ID: (none)

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

```
Console#show vlan private-vlan                                          3-104
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  --------------------------------------
     5                 primary     Eth1/ 3
     5         6       community   Eth1/ 4 Eth1/ 5
Console#
```

Configuring Private VLANs

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

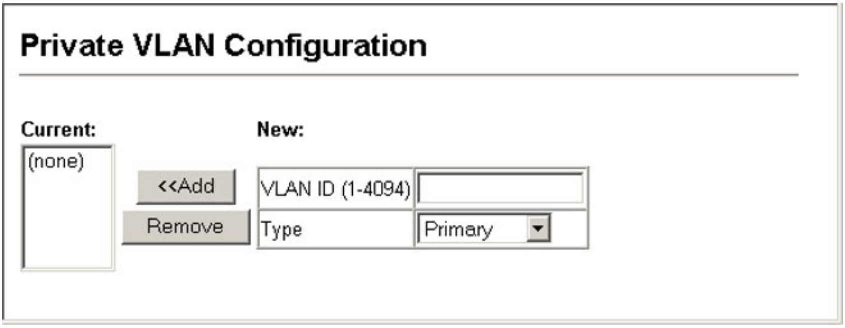
Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **Type** – There are three types of VLANs within a private VLAN:
  - **Primary VLANs** - Conveys traffic between promiscuous ports, and to community ports within secondary VLANs.
  - **Isolated VLANs** - Conveys traffic only between the VLAN’s isolated ports and promiscuous ports. Traffic between isolated ports within the VLAN is blocked.

- **Community VLANs** - Conveys traffic between community ports, and to their associated promiscuous ports.

- **Current** – Displays a list of the currently configured VLANs.

Web – Click VLAN, Private VLAN, Configuration. Enter the VLAN ID number, select Primary, Isolated, or Community type, then click Add. To remove a private VLAN from the switch, highlight an entry in the Current list box and then click Remove. Note that all member ports must be removed from the VLAN before it can be deleted.



Private VLAN Configuration

Current: (none)

New:

VLAN ID (1-4094)	
Type	Primary

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

```
Console(config)#vlan database                                     3-92
Console(config-vlan)#private-vlan 5 primary                       3-101
Console(config-vlan)#private-vlan 6 community
Console(config-vlan)#private-vlan 7 community
Console(config-vlan)#
```

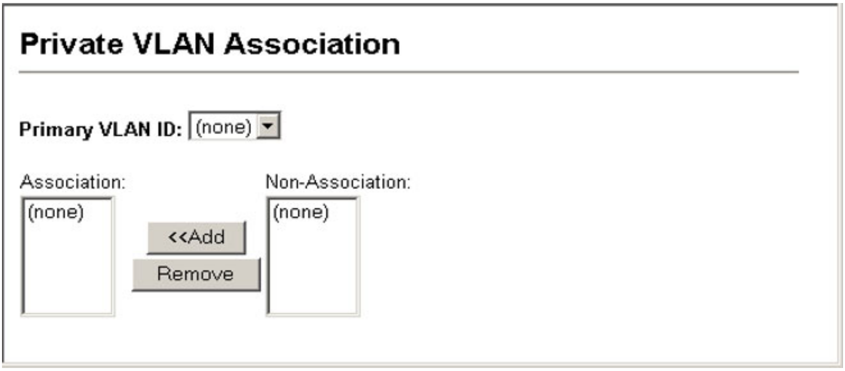
Associating VLANs

Each community or isolated VLAN must be associated with a primary VLAN.

Command Attributes

- **Primary VLAN ID** – ID of primary VLAN (1-4094, no leading zeroes).
- **Association** – Community or isolated VLANs associated with the selected primary VLAN.
- **Non-Association** – Community or isolated VLANs not associated with the selected primary VLAN.

Web – Click VLAN, Private VLAN, Association. Select the required primary VLAN from the scroll-down box, highlight one or more VLANs in the Non-Association list box, and click Add to associate these entries with the selected primary VLAN. (An isolated or community VLAN can only be associated with one primary VLAN.)



Private VLAN Association

Primary VLAN ID: (none)

Association: (none)

Non-Association: (none)

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

```
Console(config)#vlan database                                      3-92
Console(config-vlan)#private-vlan 5 association 6                  3-101
Console(config-vlan)#private-vlan 5 association 7
Console(config)#
```

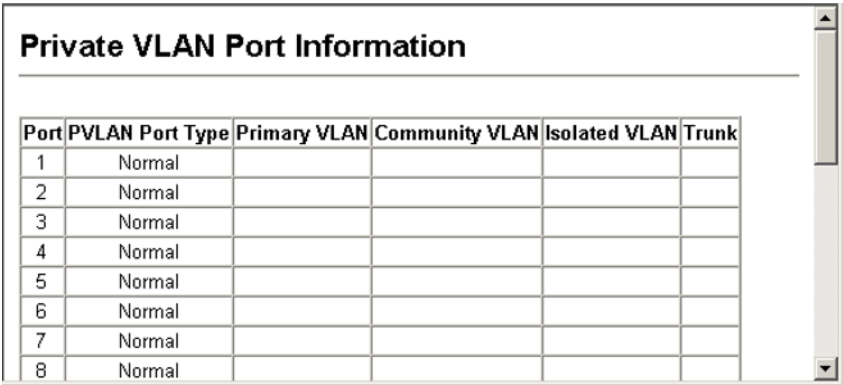
Displaying Private VLAN Interface Information

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

Command Attributes

- **Port/Trunk** – The switch interface.
- **PVLAN Port Type** – Displays private VLAN port types.
  - **Normal** – The port is not configured in a private VLAN.
  - **Host** – The port is a community port and can only communicate with other ports in its own community VLAN, and with the designated promiscuous port(s).
  - **Promiscuous** – A promiscuous port can communicate with all the interfaces within a private VLAN.
- **Primary VLAN** – Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs.
- **Community VLAN** – A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports.
- **Isolated VLAN** – Conveys traffic only between the VLAN’s isolated ports and promiscuous ports. Traffic between isolated ports within the VLAN is blocked.
- **Trunk** – The trunk identifier. (Port Information only)

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



Private VLAN Port Information

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

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

```
Console#show vlan private-vlan                                           3-104
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  --------------------------------------
     5                 primary     Eth1/ 3
     5          6      community   Eth1/ 4 Eth1/ 5
Console#
```

Configuring Private VLAN Interfaces

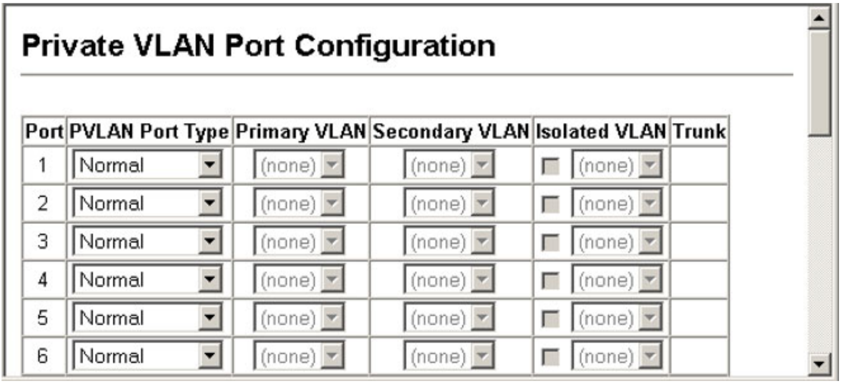
Use the Private VLAN Port Configuration and Private VLAN Trunk Configuration menus to set the private VLAN interface type, and associate the interfaces with a private VLAN.

Command Attributes

- **Port/Trunk** – The switch interface.
- **PVLAN Port Type** – Sets the private VLAN port types.
  - **Normal** – The port is not configured into a private VLAN.
  - **Host** – The port is a community port and can only communicate with other ports in its own community VLAN, and with the designated promiscuous port(s).
  - **Promiscuous** – A promiscuous port can communicate with all interfaces within a private VLAN.
- **Primary VLAN** – Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs. If PVLAN type is “Promiscuous,” then specify the associated primary VLAN. For “Host” type, the Primary VLAN displayed is the one to which the selected secondary VLAN has been associated.

- **Secondary VLAN** – On this switch, all secondary VLANs are community VLANs. A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports. If PVLAN Port Type is “Host,” then specify the associated secondary VLAN.
- **Isolated VLAN** – Conveys traffic only between the VLAN’s isolated ports and promiscuous ports. Traffic between isolated ports within the VLAN is blocked.

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



Private VLAN Port Configuration

Port	PVLAN Port Type	Primary VLAN	Secondary VLAN	Isolated VLAN	Trunk
1	Normal	(none)	(none)	□ (none)	
2	Normal	(none)	(none)	□ (none)	
3	Normal	(none)	(none)	□ (none)	
4	Normal	(none)	(none)	□ (none)	
5	Normal	(none)	(none)	□ (none)	
6	Normal	(none)	(none)	□ (none)	

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

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan promiscuous          3-102
Console(config-if)#switchport private-vlan mapping 5                 3-103
Console(config-if)#exit
Console(config)#interface ethernet 1/4
Console(config-if)#switchport mode private-vlan host                 3-102
Console(config-if)#switchport private-vlan host-association 6        3-103
Console(config-if)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#switchport mode private-vlan host
Console(config-if)#switchport private-vlan host-association 6
Console(config-if)#
```

Class of Service Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four egress (output) queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. The switch forwards packets onto the network based on traffic classes. The switch places packets into outgoing queues by mapping each of the eight incoming priority levels to one of four outgoing traffic classes. (See "Mapping CoS Values to Egress Queues" on page 2-97.) You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's traffic classes.

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate egress queue at the output port.

Command Usage

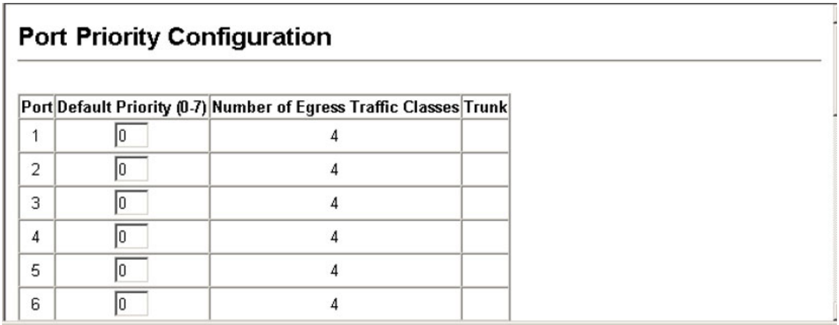
- This switch provides four egress queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- **Default Priority (0-7)*** – The priority that is assigned to untagged frames received on the specified interface.
  (Range: 0 - 7, Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

* CLI displays this information as "Priority for untagged traffic."

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



Port Priority Configuration

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

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

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5                    3-143
Console(config-if)#end
Console#show interfaces switchport ethernet 1/5                     3-75
Information of Eth 1/5
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 5
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

Mapping CoS Values to Egress Queues

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

	Egress Queue			
	0	**1**	**2**	**3**
Priority Level		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

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

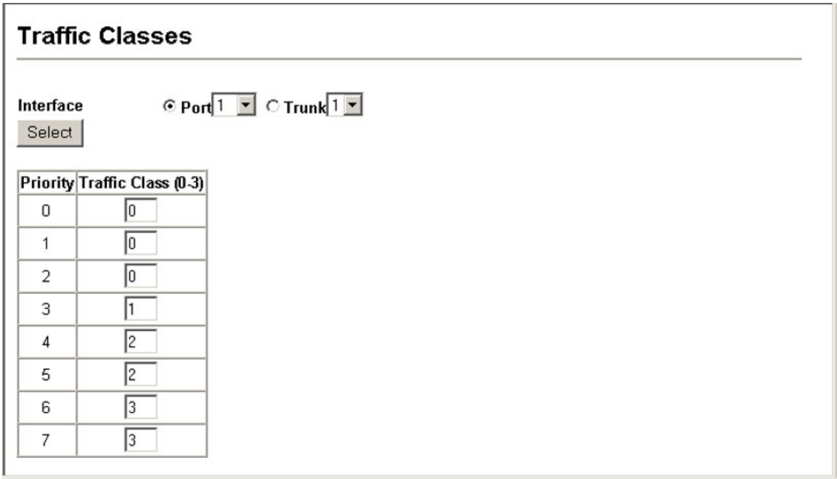
Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

- **Priority** – CoS value.
  (Range: 0-7, where 7 is the highest priority)
- **Traffic Class (0-3)*** – Output queue buffer.
  (Range: 0-3, where 3 is the highest CoS egress queue)

* CLI shows Queue ID.

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



Traffic Classes

Interface ● Port 1 ○ Trunk 1

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

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

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 1 2                               3-145
Console(config-if)#queue cos-map 1 0 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#exit
Console(config)#exit
Console#show queue cos-map ethernet 1/1                              3-147
Information of Eth 1/1
 Priority Queue: 0 1 2 3 4 5 6 7
 Traffic Class : 1 0 0 1 2 2 3 3
Console#
```

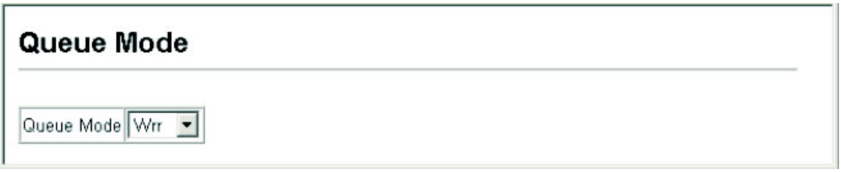
Selecting the Queue Mode

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

Command Attributes

- **WRR** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 1, 4, 16 for egress queues 0 through 3 respectively.
- **Strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

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



Queue Mode

Queue Mode: Wrr

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

```
Console(config)#queue mode strict                                    3-144
Console(config)#exit
Console#show queue mode                                              3-147

Queue mode: strict
Console#
```

Setting the Service Weight for Traffic Classes

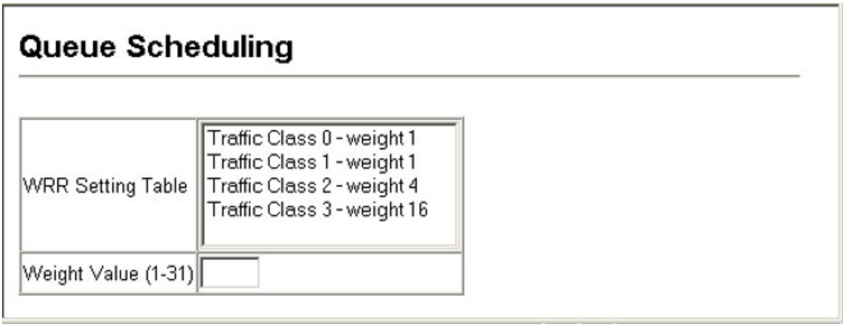
This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each egress queue. As described in “Mapping CoS Values to Egress Queues” on page 2-97, the traffic classes are mapped to one of the four egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **WRR Setting Table*** – Displays a list of weights for each traffic class (i.e., queue).
- **Weight Value (1-31)** – Sets a new weight for the selected traffic class. (Range: 1-31)

* CLI shows Queue ID.

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



Queue Scheduling

WRR Setting Table	Traffic Class 0 - weight 1 Traffic Class 1 - weight 1 Traffic Class 2 - weight 4 Traffic Class 3 - weight 16
Weight Value (1-31)	

CLI – The following example shows how to assign WRR weights of 1, 1, 4 and 16 to the output queues 0, 1, 2 and 3.

```
Console(config)#queue bandwidth 1 1 4 16                                      3-144
Console(config)#exit
Console#show queue bandwidth                                                  3-147
 Queue ID Weight
 -------- ------
        0     1
        1     1
        2     4
        3     16
Console#
```

Mapping Layer 3/4 Priorities to CoS Values

This switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP/UDP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

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

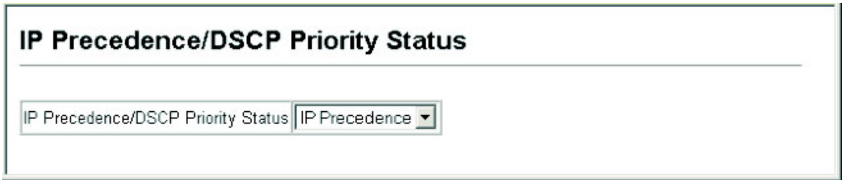
Selecting IP Precedence/DSCP Priority

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

Command Attributes

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

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



IP Precedence/DSCP Priority Status

IP Precedence/DSCP Priority Status: IP Precedence

CLI – The following example enables IP Precedence service on the switch.

```
Console(config)#map ip precedence                          3-149
Console(config)#
```

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

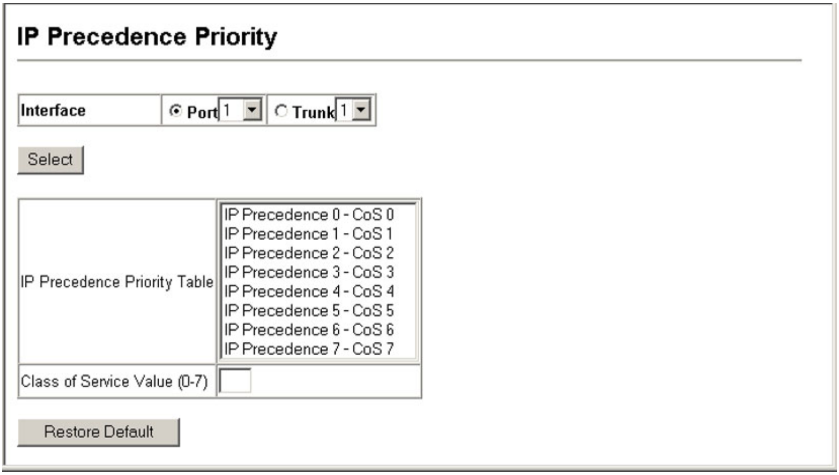
Priority Level	Traffic Type
7	Network Control
6	Internetwork Control
5	Critical
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.
- **Class of Service Value (0-7)** – Maps a CoS value to the selected IP Precedence value. Note that “0” represents low priority and “7” represent high priority.

Note: IP Precedence settings apply to all interfaces.

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



IP Precedence Priority

Interface ● Port 1 ○ Trunk 1

IP Precedence Priority Table:
IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7

Class of Service Value (0-7)

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

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

```
Console(config)#map ip precedence                                         3-149
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0                              3-150
Console(config-if)#end
Console#show map ip precedence ethernet 1/5                               3-153
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   0
  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#
```

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

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, and it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

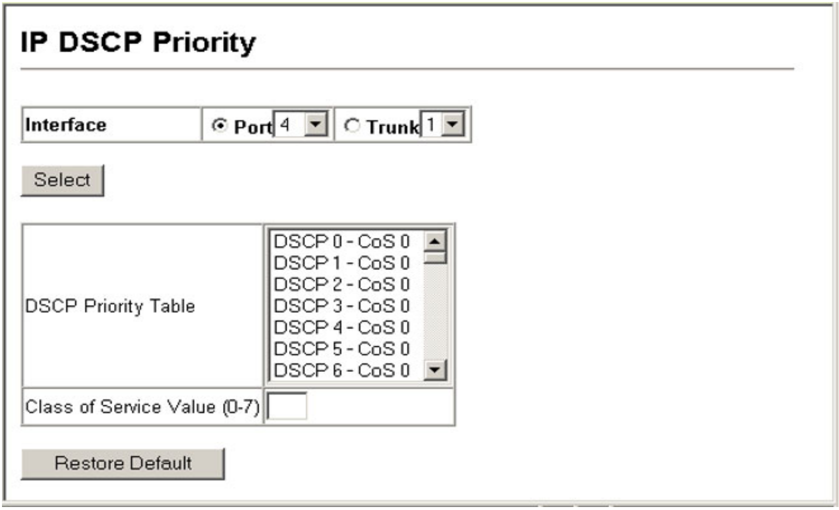
IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

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

Note: IP DSCP settings apply to all interfaces.

Web – Click Priority, IP DSCP Priority. Select a Port or Trunk from the Interface field. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.



IP DSCP Priority

Interface ● Port 4 ○ Trunk 1

Select

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

Class of Service Value (0-7)

Restore Default

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

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

```
Console(config)#map ip dscp                                          3-151
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0                               3-151
Console(config-if)#end
Console#show map ip dscp ethernet 1/5                                3-154
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 5    0   0
  Eth 1/ 5    1   0
  Eth 1/ 5    2   0
  Eth 1/ 5    3   0
.
.
.
  Eth 1/ 5   61   0
  Eth 1/ 5   62   0
  Eth 1/ 5   63   0
Console#
```

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

Mapping IP Port Priority

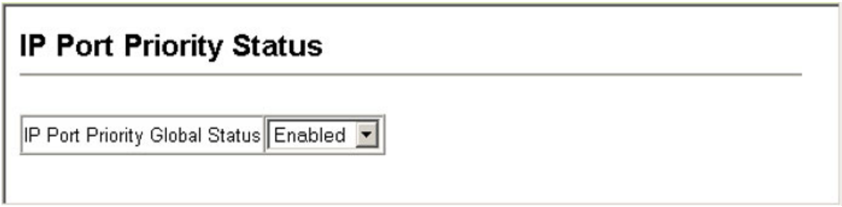
You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Command Attributes

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

Note: IP Port Priority settings apply to all interfaces.

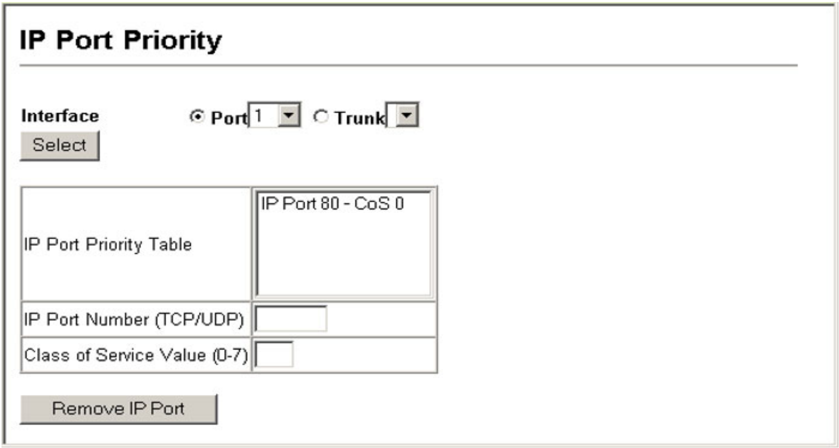
Web – Click Priority, IP Port Priority Status. Set IP Port Priority Global Status to Enabled.



IP Port Priority Status

IP Port Priority Global Status	Enabled

Web – Click Priority, IP Port Priority. Select a Port or Trunk from the Interface field. Highlight the port in the IP Port Priority Table, and then click Remove IP Port.



IP Port Priority

Interface ● Port 1 ○ Trunk

IP Port Priority Table	IP Port 80 - CoS 0
IP Port Number (TCP/UDP)	
Class of Service Value (0-7)	

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

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

```
Console(config)#map ip port                                         3-148
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0                             3-148
Console(config-if)#end
Console#show map ip port ethernet 1/5                               3-152
TCP port mapping status: disabled

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

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

ACL CoS Mapping

Use the ACL CoS Mapping page to set the output queue for packets matching an ACL rule as shown in the following table. Note that the specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. For information on mapping the CoS values to output queues, see 2-97.

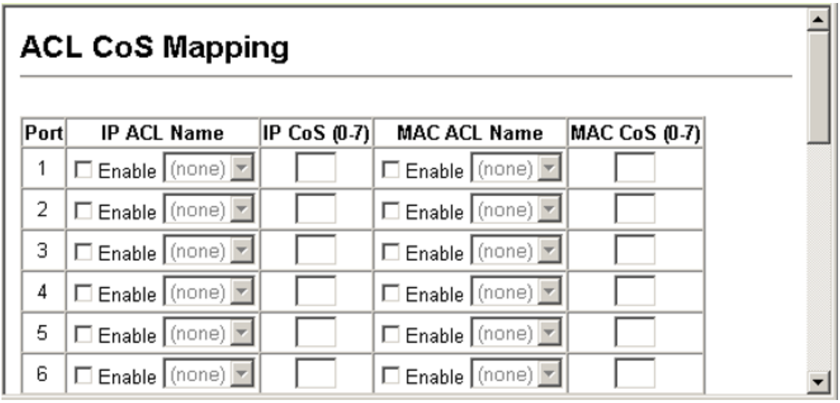
Priority Level	0	1	2	3	4	5	6	7
Output Queue	1	0	0	1	2	2	3	3

Command Attributes

- **IP ACL Name*** – Name of the IP ACL.
- **IP CoS (0-7)** – CoS value used for packets matching an IP ACL rule. (Range: 0-7)
- **MAC ACL Name*** – Name of the MAC ACL.
- **MAC CoS (0-7)** – CoS value used for packets matching a MAC ACL rule. (Range: 0-7)

* For information on configuring ACLs, see 2-40.

Web – Click Priority, ACL CoS Mapping. Enable mapping for any port, select an ACL from the scroll-down list, then click Apply.



ACL CoS Mapping

Port	IP ACL Name	IP CoS (0-7)	MAC ACL Name	MAC CoS (0-7)
1	□ Enable (none)		□ Enable (none)	
2	□ Enable (none)		□ Enable (none)	
3	□ Enable (none)		□ Enable (none)	
4	□ Enable (none)		□ Enable (none)	
5	□ Enable (none)		□ Enable (none)	
6	□ Enable (none)		□ Enable (none)	

CLI – This example assigns a CoS value of zero to packets matching rules within the specified ACL on port 25.

```
Console(config)#interface ethernet 1/25
Console(config-if)#map access-list ip bill cos 0                     3-136
Console(config-if)#
```

Multicast Filtering

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

Configuring IGMP Snooping Parameters

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

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly.
- **IGMP Query** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

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

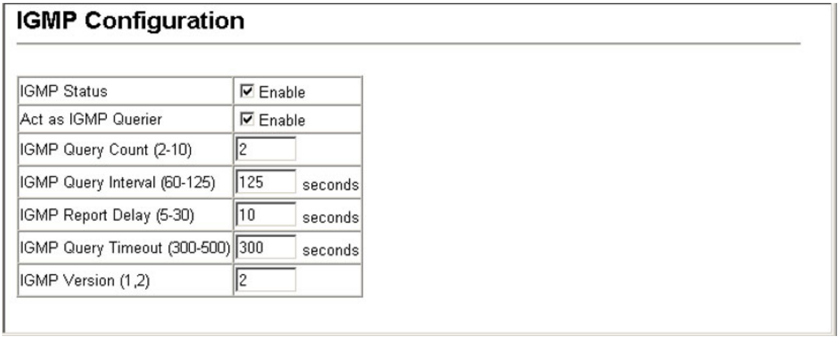
Command Attributes

- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Disabled)
- **Act as IGMP Querier** — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)
- **IGMP Query Count (2-10)** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Default: 2, Range: 2-10)
- **IGMP Query Interval (60-125)** — Sets the frequency (in seconds) at which the switch sends IGMP host-query messages. (Default: 125, Range: 60-125)
- **IGMP Report Delay (5-30)** — Sets the time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Default: 10, Range: 5-30)
- **Query Timeout (300-500)** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Default: 300 seconds, Range: 300-500)
- **IGMP Version (1,2)** — Sets the protocol version for compatibility with other devices on the network. (Default: 2, Range: 1-2)

Notes:

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

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply.



IGMP Configuration

IGMP Status	☑ Enable
Act as IGMP Querier	☑ Enable
IGMP Query Count (2-10)	2
IGMP Query Interval (60-125)	125 seconds
IGMP Report Delay (5-30)	10 seconds
IGMP Query Timeout (300-500)	300 seconds
IGMP Version (1,2)	2

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

```
Console(config)#ip igmp snooping                                   3-155
Console(config)#ip igmp snooping querier                           3-158
Console(config)#ip igmp snooping query-count 10                    3-159
Console(config)#ip igmp snooping query-interval 100                3-160
Console(config)#ip igmp snooping query-max-response-time 20        3-160
Console(config)#ip igmp snooping query-time-out 300                3-161
Console(config)#ip igmp snooping version 2                         3-156
Console(config)#exit
Console#show ip igmp snooping                                      3-157
Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
 Query interval          : 100 sec
 Query max response time : 20 sec
 Query time-out          : 300 sec
 IGMP snooping version   : Version 2
Console#
```

Interfaces Attached to a Multicast Router

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

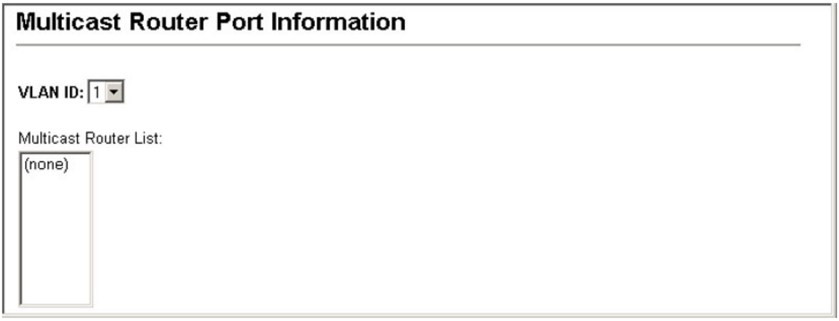
Displaying Interfaces Attached to a Multicast Router

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

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

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



Multicast Router Port Information

VLAN ID: 1

Multicast Router List:

(none)

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

```
Console#show ip igmp snooping mrouter vlan 1                              3-162
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
```

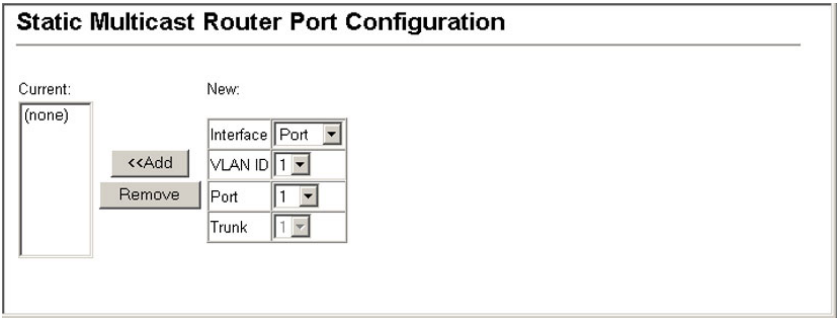
Specifying Interfaces Attached to a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

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

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



Static Multicast Router Port Configuration

Current:
(none)

New:

Interface: Port
VLAN ID: 1
Port: 1
Trunk: 1

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

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11       3-162
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                        3-162
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11  Static
```

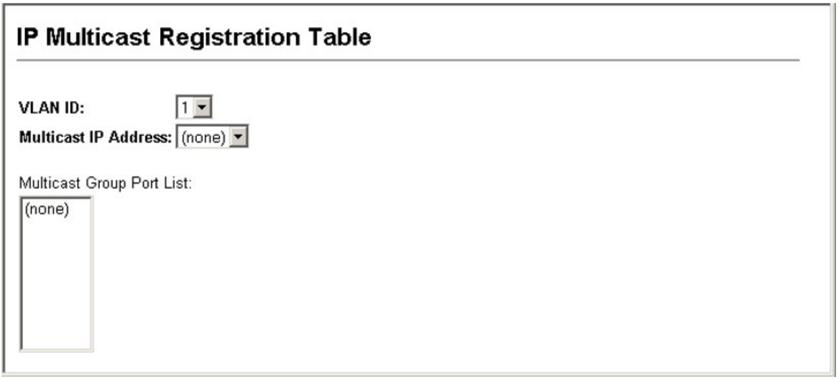
Displaying Port Members of Multicast Services

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

Command Attributes

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

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



IP Multicast Registration Table

VLAN ID: 1

Multicast IP Address: (none)

Multicast Group Port List:

(none)

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

```
Console#show mac-address-table multicast vlan 1                    3-158
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.0.0.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Adding Multicast Addresses to VLANs

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in “Configuring IGMP Snooping Parameters” on page 2-109. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

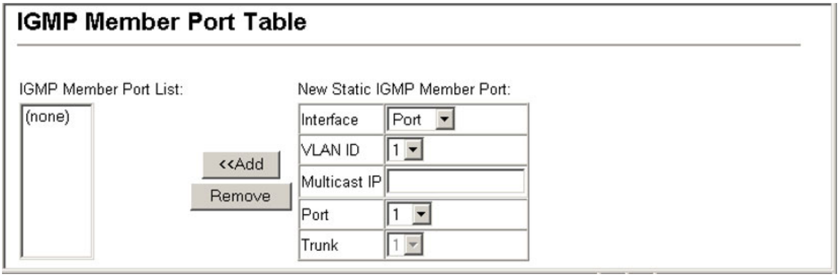
Command Usage

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

Command Attributes

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

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



IGMP Member Port Table

IGMP Member Port List: (none)

New Static IGMP Member Port:

Interface	Port
VLAN ID	1
Multicast IP	
Port	1
Trunk	1

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

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
 ethernet 1/12                                                 3-156
Console(config)#exit
Console#show mac-address-table multicast vlan 1                3-158
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.0.0.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Chapter 3: Command Line Interface

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

Using the Command Line Interface

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 connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

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 SF-2024F is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Caution: The IP address for this switch is unassigned by default.

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Vty-0#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-0>” for the guest to show that you are using normal access mode (i.e., Normal Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

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

Vty-0#
```

Caution: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

  ```
  Console>enable
  Console#show startup-config
  ```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

  ```
  Console(config)#username admin password 0 smith
  ```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab will result in printing the command up to “**logging**.”

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

Showing Commands

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

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

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

```
Console>show interfaces ?
  counters    Information of interfaces counters
  status      Information of interfaces status
  switchport  Information of interfaces switchport
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

```
Console#show s?
snmp            spanning-tree  startup-config  system
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “**?**” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

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

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

Exec Commands

When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.” The system will now display the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password “super” (page 3-9).

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

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

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

Console#
```

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

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

Console#enable
Password: [privileged level password if so configured]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in nonvolatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- DHCP Configuration - These commands are used to configure the DHCP server.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include commands such as **parity** and **databits**.
- Router Configuration - These commands configure global settings for unicast and multicast routing protocols.
- 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.

Mode	Command	Prompt	Page
Line	line {console | vty}	Console(config-line)#	3-57
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)#	3-65
VLAN	vlan database	Console(config-vlan)	3-92

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode.

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-P	Shows the last command.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

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

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	3-9
Flash/File	Manages code image or switch configuration files	3-14
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	3-19
SNTP	Configures SNTP client settings, including broadcast mode or a specified list of servers	3-41
SNMP	Activates authentication failure traps; configures community access strings, and trap managers	3-47
IP Interface	Configures the IP address and gateway for management access, DHCP server and relay service for server blades, displays the default gateway, or pings a specified device	3-52
Line	Sets communication parameters for the serial port, including baud rate and console time-out	3-58
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	3-65
Address Table	Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time	3-77
Spanning Tree	Configures Spanning Tree settings for the switch	3-80
VLANs	Configures VLAN settings, and defines port membership for VLAN groups	3-92
PVLAN	Enables or configures private VLANs	3-100
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB	3-105
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	3-109
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	3-111
Rate Limiting	Controls the maximum rate for traffic transmitted or received on a port	3-114
Authentication	Configures RADIUS and TACACS+ client-server authentication for logon access and commands for IEEE 802.1x port access control.	3-117
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)	3-130
Priority	Sets port priority for untagged frames, relative weight for each priority queue, also sets priority for TCP/UDP traffic types, IP precedence, and DSCP	3-142
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	3-155

The access mode shown in the following tables is indicated by these abbreviations:

NE (Normal Exec)	**IC** (Interface Configuration)
PE (Privileged Exec)	**LC** (Line Configuration)
GC (Global Configuration)	**VC** (VLAN Database Configuration)

General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	3-9
disable	Returns to normal mode from privileged mode	PE	3-10
configure	Activates global configuration mode	PE	3-10
show history	Shows the contents of the command history buffer	NE, PE	3-11
reload	Restarts the system	PE	3-12
prompt	Customizes the CLI prompt	GC	3-12
end	Returns to Privileged Exec mode	any config. mode	3-12
exit	Returns to the previous configuration mode, or exits the CLI	any	3-13
quit	Exits a CLI session	NE, PE	3-13
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See page 3-5.

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 on page 3-22.)

- 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 (3-10)
enable password (3-22)

disable

Use this command to return 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 page 3-5.

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 (3-9)

configure

Use this command to activate 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, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See page 3-5.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end (3-12)

show history

Use this command to show the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

Use this command to restart the system.

Caution: 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
```

prompt

Use this command to customize the CLI prompt. Use the **no** form to revert to the default prompt.

Syntax

prompt *string*
no prompt

string - Any alphanumeric string to use for the command prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt ES3526X-ZZ
ES3526X-ZZ(config)#
```

end

Use this command to return to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

Use this command to return to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

quit

Use this command to exit 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:
```

Flash/File Commands

These commands are used to manage the system code or configuration files.

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	3-14
delete	Deletes a file or code image	PE	3-16
dir	Displays a list of files in flash memory	PE	3-17
whichboot	Displays the files booted	PE	3-18
boot system	Specifies the file or image used to start up the system	GC	3-18

copy

Use this command to move (upload/download) a code image or configuration file between the switch's flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy file {**file** | **running-config** | **startup-config** | **tftp**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file | running-config | startup-config | https-certificate**}

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Copies a HTTPS certificate from a TFTP server to the switch.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM image cannot be uploaded or downloaded from the TFTP server. You must use a direct console connection and access the download menu during a boot up to download the Boot ROM (or diagnostic) image. See "Upgrading Firmware via the Serial Port" on page A-1.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
/
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#
```

delete

Use this command to delete a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

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.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (3-17)

dir

Use this command to display a list of files in flash memory.

Syntax

dir [**boot-rom** | **config** | **opcode** [:*filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file
- **config** - Switch configuration file
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- File information is shown below:

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

```
Console#dir
                       file name      file type startup size (byte)
-------------------------------- -------------- ------- -----------
                       diag_0060 Boot-Rom image       Y      111360
                       run_01642 Operation Code       N     1074304
                        run_0200 Operation Code       Y     1083008
      Factory_Default_Config.cfg    Config File       N        2574
                         startup    Config File       Y        2710
-------------------------------------------------------------------
                                        Total free space:         0
Console#
```

whichboot

Use this command to display which files were booted when the system powered up.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
        file name      file type startup size (byte)
----------------- -------------- ------- -----------
        diag_0060 Boot-Rom image       Y      111360
         run_0200 Operation Code       Y     1083008
          startup    Config File       Y        2710
Console#
```

boot system

Use this command to specify the file or image used to start up the system.

Syntax

boot system {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom** - Boot ROM
- **config** - Configuration file
- **opcode** - Run-time operation code

The colon (:) is required.

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (3-17)
whichboot (3-18)

System Management Commands

These commands are used to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

Command	Function	Mode	Page
Device Designation Command			
hostname	Specifies the host name for the switch	GC	3-20
snmp-server contact	Sets the system contact string	GC	3-48
snmp-server location	Sets the system location string	GC	3-49
User Access Commands			
username	Establishes a user name-based authentication system at login	GC	3-21
enable password	Sets a password to control access to various Privileged Exec levels	GC	3-22
Event Logging Commands			
logging on	Controls logging of error messages	GC	3-23
logging history	Limits syslog messages saved to switch memory based on severity	GC	3-23
logging host	Adds a syslog server host IP address that will receive logging messages	GC	3-24
logging facility	Sets the facility type for remote logging of syslog messages	GC	3-25
logging trap	Limits syslog messages saved to a remote server based on severity	GC	3-26
clear logging	Clears messages from the logging buffer	PE	3-27
show logging	Displays the state of logging	PE	3-27
System Status Commands			
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	3-28
show running-config	Displays the configuration data currently in use	PE	3-29
show system	Displays system information	NE, PE	3-31
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client	NE, PE	3-32

Command	Function	Mode	Page
show version	Displays version information for the system	NE, PE	3-33
Web Server Commands			
ip http port	Specifies the port to be used by the Web browser interface	GC	3-34
ip http server	Allows the switch to be monitored or configured from a browser	GC	3-34
ip http secure-server	Enables HTTPS/SSL for encrypted communications	GC	3-35
ip http secure-port	Specifies the UDP port number for HTTPS/SSL	GC	3-36
Secure Shell Commands			
ip ssh server	Enables the SSH server on the switch	GC	3-37
ip ssh	Specifies the authentication timeout for the SSH server and the number of retries allowed by a client	GC	3-38
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	3-39
disconnect ssh	Terminates an SSH connection	PE	3-39
show ssh	Displays the status of current SSH sessions	PE	3-40

hostname

Use this command to specify or modify 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 ES3526X-ZZ
Console(config)#
```

username

Use this command to add named users, require authentication at login, specify or change a user's password (or specify that no password is required), or specify or change 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, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how to 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)#
```

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. Use this command to control 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.
- This 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 (page 3-9).
- 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 (3-9)

logging on

Use this command to control logging of error messages. This command sends debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

logging on
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. The **logging trap** command controls the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (3-23)
logging trap (3-26)
clear logging (3-27)

logging history

Use this command to limit 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 level arguments listed in the following table. Messages sent include the selected level down to level 0.

Level Argument	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (e.g., return false, unexpected return)
errors	3	Error conditions (e.g., invalid input, default used)
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
alerts	1	Immediate action needed
emergencies	0	System unusable

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

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (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

Use this command to add a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

logging host *host_ip_address*
no logging host *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- By using this command more than once you can build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

Use this command to set 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*

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

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

Use this command to limit syslog messages saved to a remote server based on severity. Use the **no** form to return the remote logging of syslog messages to the default level.

Syntax

logging trap *level*
no logging trap *level*

level - One of the level arguments listed below. Messages sent include the selected level up through level 0.

Level Argument	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (e.g., return false, unexpected return)
errors	3	Error conditions (e.g., invalid input, default used)
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
alerts	1	Immediate action needed
emergencies	0	System unusable

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

Default Setting

Level 3 - 0

Command Mode

Global Configuration

Example

```
Console(config)#logging trap 4
Console(config)#
```

clear logging

Use this command to clear messages from the log buffer.

Syntax

clear logging [**flash** | **ram**]

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear logging
Console#
```

Related Commands

show logging (3-27)

show logging

Use this command to display the logging configuration, along with any system and event messages stored in memory.

Syntax

show logging {**flash** | **ram** | **trap**}

- **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).
- **trap** - Messages sent to remote syslog servers.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command shows the following information:

- Syslog logging – Whether or not system logging has been enabled via the **logging on** command.

- History logging in FLASH/RAM – The message level(s) that are reported based on the **logging history** command.
- Any system and event messages stored in memory.
- Remote logging – Whether logging to remote syslog servers has been enabled via the **logging host** command, the message level(s) that are sent, and a list of configured syslog server IP addresses.

Example

The following example shows that system logging is enabled, the message level for flash memory is “errors” (i.e., default level 3 - 0), the message level for RAM is “debugging” (i.e., default level 7 - 0), and lists one sample error.

```
Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
   "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1
   "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#
```

show startup-config

Use this command to display the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names and access levels)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface

- IP address configured for VLANs
- Spanning tree settings
- Any configured settings for the console port and Telnet

Example

```
Console#show startup-config
building startup-config, please wait.....
!
!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp-server community public ro
snmp-server community private rw
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
.
interface vlan 1
 ip address 0.0.0.0 255.0.0.0
 ip address dhcp
!
line console
!
line vty
!
end

Console#
```

Related Commands

show running-config (3-29)

show running-config

Use this command to display the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - IP address configured for VLANs
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

Example

```
Console#show running-config
building running-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
!
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
!
authentication login local
!
!
line console
!
line vty
!
end
Console#
```

Related Commands

show startup-config (3-28)

show system

Use this command to display 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 2-7.
- The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.

Example

```
Console#show system
System description: ES3526X-ZZ
System OID string: 1.3.6.1.4.1.259.6.10.45
System information
 System Up time: 0 days, 1 hours, 1 minutes, and 1.93 seconds
 System Name            : [NONE]
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 00-30-F1-6E-0D-E0
 Web server             : enable
 Web server port        : 80
 POST result
UART Loopback Test.....................PASS
Timer Test.............................PASS
DRAM Test .............................PASS
I2C Initialization.....................PASS
Runtime Image Check ...................PASS
PCI Device Check ......................PASS
Switch Driver Initialization...........PASS
Switch Internal Loopback Test..........PASS
------------------- DONE --------------------

Console#
```

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
 Username accounts:
  Username Privilege
  -------- ---------
     guest         0
     admin        15

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
  1     vty 0    admin           0:04:37      10.1.0.19

Console#
```

show version

Use this command to display hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See “Displaying Switch Hardware/Software Versions” on page 2-8 for detailed information on software items.

Example

```
Console#show version
Unit1
 Serial number          :ag1005
 Service tag            :
 Hardware version       :
 Module A type          :not present
 Module B type          :not present
 Number of ports        :24
 Main power status      :up
 Redundant power status :not present
Agent(master)
 Unit id                :1
 Loader version         :2.1.0.0
 Boot rom version       :2.0.0.7
 Operation code version :2.0.3.1
Console#
```

Web Server Commands

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the Web browser interface	GC	3-34
ip http server	Allows the switch to be monitored or configured from a browser	GC	3-34
ip http secure-server	Enables HTTPS/SSL for encrypted communications	GC	3-35
ip http secure-port	Specifies the UDP port number for HTTPS/SSL	GC	3-36

ip http port

Use this command to specify 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

logging on (3-23)

ip http server

Use this command to allow 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 (3-34)

ip http secure-server

Use this command 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. Use the **no** form to disable this function.

Syntax

[**no**] **ip http secure-server**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

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

  A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x or later versions.
- The following Web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, page 2-30. Also refer to the **copy** command on page 3-14.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (3-36)
copy tftp https-certificate (3-14)

ip http secure-port

Use this command to specify the UDP port number used for HTTPS/SSL connection to the switch’s Web interface. Use the no form to restore the default port.

Syntax

ip http secure-port *port_number*
no ip http secure-port

port_number – The UDP port used for HTTPS/SSL. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://**_device_**:**_port_number_

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (3-35)

Secure Shell Commands

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

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When 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.

This section describes the commands used to configure the SSH server. However, note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

Caution: The switch supports only SSH Version 1.5.

Command	Function	Mode	Page
ip ssh server	Enables the SSH server on the switch	GC	3-37
ip ssh	Specifies the authentication timeout for the SSH server and the number of retries allowed by a client	GC	3-38
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	3-39
disconnect ssh	Terminates an SSH connection	PE	3-39
show ssh	Displays the status of current SSH sessions	PE	3-40

ip ssh server

Use this command to enable 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 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.

Example

```
Console(config)#ip ssh server
Console(config)#
```

Related Commands

show ssh (3-40)

ip ssh

Use this command to configure authentication control parameters for the Secure Shell (SSH) server on this switch. Use the **no** form to restore the default settings.

Syntax

ip ssh {[**timeout** *seconds*] | [**authentication-retries** *count*]}
no ip ssh {[**timeout**] | [**authentication-retries**]}

- *seconds* – The timeout for client response during SSH negotiation. (Range: 1-120)
- *count* – The number of authentication attempts permitted after which the interface is reset.
(Range: 1-5)

Default Setting

timeout: 120 seconds
retries: 3

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (3-39)

show ip ssh

Use this command to display the connection settings used when authenticating client access to the Secure Shell (SSH) server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
Information of secure shell
SSH status: enable
SSH authentication timeout: 120
SSH authentication retries: 3
Console#
```

Related Commands

ip ssh (3-38)

disconnect ssh

Use this command to terminate a Secure Shell (SSH) client connection.

Syntax

disconnect ssh *connection-id*

connection-id – The session identifier as displayed in the **show ip ssh** command.

Command Mode

Privileged Exec

Example

```
Console#disconnect ssh 0
Console#
```

Related Commands

show ip ssh (3-39)

show ssh

Use this command to display the current Secure Shell (SSH) server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   1.5      cipher-3des   session-started
Console#
```

Field	Description
Session	The session number. (Range: 0-3)
Username	The user name of the client.
Version	The Secure Shell version number.
Encrypt method	The encryption method. (Options: cipher-des, cipher-3des)
Negotiation state	The authentication negotiation state.

Port Security

Use this command to enable and configure port security on a port. Use the no form to disable port security and reset the maximum addresses to the default.

Syntax

port security [**max-mac-count** *address-number*]
no port security [**max-mac-count**]

address-number - Sets the maximum number of MAC addresses that can be learned on a port. (Range: 0 - 20)

Default Setting

Status: Disabled
Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security on a specified port, the switch will dynamically learn MAC addresses until the specified number has been reached and then stop. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- 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. You can also manually add secure addresses to the port with the **mac-address-table static** command.

- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port.
- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.
- A secure port has the following restrictions:
  - Cannot be connected to a network interconnection device.
  - Cannot be a member of a static trunk.
  - It can be configured as an LACP trunk port, but the switch does not allow the LACP trunk to be enabled.
- A port that is already configured as an LACP or static trunk port cannot be enabled as a secure port.

Example

This example sets the maximum MAC addresses and enables port security for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security max-mac-count 10
Console(config-if)#port security
Console(config-if)#
```

Related Commands

mac-address-table static (3-77)

SNTP Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP), or by using information broadcast by local time servers.

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	3-42
sntp server	Specifies one or more time servers	GC	3-43
sntp poll	Sets the interval at which the client polls for time	GC	3-43
sntp broadcast client	Accepts time from any time broadcast server	GC	3-44
show sntp	Shows current SNTP configuration settings	NE, PE	3-44
clock timezone	Sets the time zone for the switch’s internal clock	GC	3-45
calendar set	Sets the system date and time	PE	3-45
show calendar	Displays the current date and time setting	NE, PE	3-46

sntp client

Use this command to enable SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form of this command to disable SNTP client requests.

Syntax

[**no**] **sntp client**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.
- The SNTP time query method is set to client mode when the first **sntp client** command is issued. However, if the **sntp broadcast client** command is issued, then the **no sntp broadcast client** command must be used to return the switch to SNTP client mode.

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
Console#
```

Related Commands

sntp server (3-43)
sntp poll (3-43)
sntp broadcast client (3-44)
show sntp (3-44)

sntp server

Use this command to set the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of an time server (NTP or SNTP).
(Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client (3-42)
sntp poll (3-43)
show sntp (3-44)

sntp poll

Use this command to set 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

Command Usage

This command is only applicable when the switch is set to SNTP client mode.

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (3-42)

sntp broadcast client

Use this command to synchronize the switch's clock based on time broadcast from time servers (using the multicast address 224.0.1.1). Use the **no** form to disable SNTP broadcast client mode.

Syntax

[**no**] **sntp broadcast client**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#sntp broadcast client
Console#
```

show sntp

Use this command to display the current time and configuration settings for the SNTP client, and 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 (when the switch is set to SNTP client mode), and the current SNTP mode (i.e., client or broadcast).

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:  unicast
Console#
```

clock timezone

Use this command to set the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 1-12 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp (3-44)

calendar set

Use this command to set the system clock.

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 - 2101)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2003.

```
Console#calendar set 15 12 34 1 February 2003
Console#
```

show calendar

Use this command to display the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar set
 15:12:34 February 1 2003
Console#
```

SNMP Commands

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	3-47
snmp-server contact	Sets the system contact string	GC	3-48
snmp-server location	Sets the system location string	GC	3-49
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	3-49
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC	3-50
show snmp	Displays the status of SNMP communications	NE, PE	3-51

snmp-server community

Use this command to define the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol.
  (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default 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

Command Usage

The first **snmp-server community** command you enter enables SNMP (SNMP v1 and v2c). The **no snmp-server community** command disables SNMP.

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

Use this command to set 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 (3-49)

snmp-server location

Use this command to set 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 (3-48)

snmp-server host

Use this command to specify the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *{host-addr community-string}* [**version 1** | **2c**]
no snmp-server host *host-addr*

- *host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* - Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP v1 or SNMP v2c traps.

Default Setting

Host Address: None
SNMP Version: 1

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- The switch can send SNMP version 1 or version 2c traps 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 traps.
- However, some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (3-50)

snmp-server enable traps

Use this command to enable this device to send Simple Network Management Protocol traps (SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

snmp-server enable traps [**authentication** | **link-up-down**]
no snmp-server enable traps [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.
  The link-up-down trap can only be enabled/disabled via the CLI.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Example

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

Related Commands

snmp-server host (3-49)

show snmp

Use this command 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 traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
   0 Trap PDUs

SNMP logging: disabled
Console#
```

IP Interface Commands

An IP address may be used for management access to the switch over your network. By default, the switch uses DHCP to assign IP settings to VLAN 1 on the switch.

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

Command	Function	Mode	Page
ip address	Sets the IP address for the current interface	IC	3-53
ip dhcp restart	Submits a BOOTP or DCHP client request	PE	3-54
ip default-gateway	Defines the default gateway through which an in-band management station can reach this device	GC	3-54
show ip interface	Displays the IP settings for this device	PE	3-55
show ip redirects	Displays the default gateway configured for this device	PE	3-55
ping	Sends ICMP echo request packets to another node on the network	NE, PE	3-56

ip address

Use this command to set the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**}
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.

Default Setting

DHCP is enabled by default.

Command Mode

Interface Configuration (VLAN)

Command Usage

- You must assign an IP address to this device to gain management access over the network. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart** command, or by rebooting the switch.

Caution: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart (3-54)

ip dhcp restart

Use this command to submit a BOOTP or DCHP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the **ip address** command.
- DHCP requires the server to reassign the client’s last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
   and address mode: Dhcp.
Console#
```

Related Commands

ip address (3-53)

ip default-gateway

Use this command to a establish a static route between this device and management stations that exist on another network segment. Use the **no** form to remove the static route.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

Related Commands

show ip redirects (3-55)

show ip interface

Use this command to display the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Example

```
Console#show ip interface
 IP address and netmask: 10.1.0.254 255.255.255.0 on VLAN 1,
   and address mode: User specified.
Console#
```

Related Commands

show ip redirects (3-55)

show ip redirects

Use this command to show the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (3-54)

ping

Use this command to send 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, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32) The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the **ping** command to see if another site on the network can be reached.
- Following are some results of the **ping** command:
  - *Normal response* -The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 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#
```

Line Commands

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).

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	3-58
login	Enables password checking at login	LC	3-58
password	Specifies a password on a line	LC	3-59
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	3-60
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	3-61
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	3-61
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	3-62
parity*	Defines the generation of a parity bit	LC	3-63
speed*	Sets the terminal baud rate	LC	3-63
stopbits*	Sets the number of the stop bits transmitted per byte	LC	3-64
show line	Displays a terminal line's parameters	NE, PE	3-64

* These commands only apply to the serial port.

line

Use this command to identify a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as “Vty” in screen displays such as **show users**. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (3-64)
show users (3-32)

login

Use this command to enable password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS/TACACS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (3-21)
password (3-59)

password

Use this command to specify the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.

- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (3-58)
password-thresh (3-61)

exec-timeout

Use this command to set the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout *seconds*
no exec-timeout

seconds - Integer that specifies the number of seconds. (Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: 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.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

Use this command to set the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh *threshold*
no password-thresh

threshold - The number of allowed password attempts.
(Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (3-61)

silent-time

Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time *seconds*
no silent-time

seconds - The number of seconds to disable console response.
(Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (3-61)

databits

Use this command to set 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 (3-63)

parity

Use this command to define 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)#
```

speed

Use this command to set 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, 57600, 38400, 19200, 115200 bps)

Default Setting

9600 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

Use this command to set the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- **1** - One stop bit
- **2** - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

show line

Use this command to display the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access.

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 65535
Console#
```

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	3-66
description	Adds a description to an interface configuration	IC	3-66
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	3-67
negotiation	Enables autonegotiation of a given interface	IC	3-68
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	3-69
flowcontrol	Enables flow control on a given interface	IC	3-70
clear counters	Clears the statistics on a given interface	PE	3-71
shutdown	Disables an interface	IC	3-71
switchport broadcast octet-rate	Configures broadcast storm control	IC	3-72
show interfaces status	Displays status for the specified interface	NE, PE	3-73
show interfaces counters	Displays statistics for the specified interfaces	NE, PE	3-74
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	3-75

interface

Use this command to configure an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify the port 25, enter the following command:

```
Console(config)#interface ethernet 1/25
Console(config-if)#
```

description

Use this command to add a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 25.

```
Console(config)#interface ethernet 1/25
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

Use this command to configure the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 100half for 100BASE-TX ports and 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (3-68)
capabilities (3-69)

negotiation

Use this command to enable autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

negotiation
no negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

negotiation (3-68)
speed-duplex (3-67)

capabilities

Use this command to advertise the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

no capabilities [**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**]

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (*The current switch ASIC only supports symmetric pause frames.*)

Default Setting

- 100BASE-TX: 10half, 10full, 100half, 100full
- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

negotiation (3-68)
speed-duplex (3-67)
flowcontrol (3-70)

flowcontrol

Use this command to enable flow control. Use the **no** form to disable flow control.

Syntax

flowcontrol
no flowcontrol

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port.
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (3-68)
capabilities (flowcontrol, symmetric) (3-69)

clear counters

Use this command to clear statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

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 Ethernet port 1/1.

```
Console#clear counters ethernet 1/1
Console#
```

shutdown

Use this command to disable an interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown
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 reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport broadcast octet-rate

Use this command to configure broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast octet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., octets per second.
(Range: 64-95232000)

Default Setting

Enabled for all ports
Octet-rate limit: 32000 octets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, octets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to all ports on the switch.

Example

The following shows how to configure broadcast storm control at 600 octets per second on port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast octet-rate 600
Console(config-if)#
```

show interfaces status

Use this command to display the status for an interface.

Syntax

show interfaces status [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Displaying Connection Status” on page 2-48.

Example

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type: 100TX
  Mac address: 00-00-AB-CD-00-01
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 octets/second
  Flow control: Disabled
  Lacp: Disabled
 Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC address: 00-00-AB-CD-00-00
Console#
```

show interfaces counters

Use this command to display interface statistics.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

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 page 2-58.

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
 Iftable stats:
  Octets input: 30658, Octets output: 196550
  Unicast input: 6, Unicast output: 5
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 227208, Packets: 3338
  Broadcast pkts: 263, Multi-cast pkts: 3064
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
  Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

show interfaces switchport

Use this command to display the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

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 25.

```
Console#show interfaces switchport ethernet 1/22
Information of Eth 1/22
 Broadcast threshold: Enabled, 32000 octets/second
 Lacp status: Disabled
 Ingress rate limit: disable,100M bits per second
 Egress rate limit: disable,100M 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
Console#
```

Field	Description
Broadcast threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 3-72).
Lacp status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 3-112).
VLAN membership mode	Indicates membership mode as Trunk or Hybrid (page 3-95).

Field	Description
Ingress rule	Shows if ingress filtering is enabled or disabled (page 3-96).
Acceptable frame type	Shows if acceptable VLAN frames include all types or tagged frames only (page 3-95).
Native VLAN	Indicates the default Port VLAN ID (page 3-97).
Priority for untagged traffic	Indicates the default priority for untagged frames (page 3-142).
Gvrp status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 3-105).
Allowed Vlan	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 3-97).
Forbidden Vlan	Shows the VLANs this interface can not dynamically join via GVRP (page 3-98).

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.

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	3-77
show mac-address-table	Displays entries in the bridge-forwarding database	PE	3-78
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	3-79
mac-address-table aging-time	Sets the aging time of the address table	GC	3-79
show mac-address-table aging-time	Shows the aging time for the address table	PE	3-80

mac-address-table static

Use this command to map a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)
- *action* -
  - **delete-on-reset** - Assignment lasts until the switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

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

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

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

show mac-address-table

Use this command to view classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - Dynamic address entries
  - Permanent - Static entry
  - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means “any.”
- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Delete-on-reset
  Console#
```

clear mac-address-table dynamic

Use this command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```

mac-address-table aging-time

Use this command to set 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*

seconds - Time in number of seconds (10-30000).

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 300
Console(config)#
```

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.

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	3-80
spanning-tree mode	Configures STP or RSTP mode	GC	3-81
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	3-82
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	3-83
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	3-83
spanning-tree priority	Configures the spanning tree bridge priority	GC	3-84
spanning-tree pathcost method	Configures the path cost method for RSTP	GC	3-84
spanning-tree transmission-limit	Configures the transmission limit for RSTP	GC	3-85
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	3-86
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC	3-86
spanning-tree portfast	Sets an interface to fast forwarding	IC	3-87
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	3-88
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	3-89
spanning-tree link-type	Configures the link type for RSTP	IC	3-89
show spanning-tree	Shows spanning tree configuration for the overall bridge or a selected interface	PE	3-90

spanning-tree

Use this command to enable the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

spanning-tree
no spanning-tree

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

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

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

Use this command to select the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp**}
no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol
  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.
- Rapid Spanning Tree Protocol
  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
  - STP Mode – If the switch receives an 802.1D BPDU after a port’s migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

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

Example

The following example configures the switch to use the Rapid Spanning Tree Protocol.

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

Use this command to configure 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 a blocking state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

Use this command to configure the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds, (Range: 1 - 10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

spanning-tree max-age

Use this command to configure the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

Use this command to configure the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge.
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 4096
Console(config)#
```

spanning-tree pathcost method

Use this command to configure the path cost method used for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

Default Setting

short 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 3-84) takes precedence over port priority (page 3-86).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

Use this command to configure the minimum interval between the transmission of consecutive RSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count -The transmission limit in seconds. (Range: 1-10)

Default

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree cost

Use this command to configure the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

cost - The path cost for the port. (Range: 1-200,000,000))

The recommended range is:

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the spanning-tree pathcost method (page 3-84) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree port-priority

Use this command to configure the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree cost (3-86)

spanning-tree portfast

Use this command to set an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

spanning-tree portfast
no spanning-tree portfast

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)

- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (3-88)

spanning-tree edge-port

Use this command to specify an interface as an edge port. Use the **no** form to restore the default.

Syntax

spanning-tree edge-port
no spanning-tree edge-port

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast**.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (3-87)

spanning-tree protocol-migration

Use this command to re-check the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

spanning-tree link-type

Use this command to configure the link type for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

show spanning-tree

Use this command to show the spanning tree configuration.

Syntax

show spanning-tree [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface.
- For a description of the items displayed under “Spanning-tree information,” see “Configuring Global Settings” on page 2-69. For a description of the items displayed for specific interfaces, see “Displaying Interface Settings” on page 2-72.

Example

```
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode               :RSTP
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Designated Root                  :32768.0000ABCD0000
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :2
 Last topology changes time (sec.):1718
 Transmission limit               :3
 Path Cost Method                 :long
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 Path cost            : 100000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 128.1
 Designated root      : 32768.0000ABCD0000
 Designated bridge    : 32768.0000ABCD0000
 Forward transitions  : 0
 Fast forwarding      : disable
 Admin edge port      : disable
 Oper edge port       : disable
 Admin Link type      : auto
 Oper Link type       : point-to-point
.
.
.
Console#
```

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.

Command	Function	Mode	Page
Edit VLAN Groups			
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	3-92
vlan	Configures a VLAN, including VID, name and state	VC	3-93
Configure VLAN Interfaces			
interface vlan	Enters interface configuration mode for specified VLAN	IC	3-94
switchport mode	Configures VLAN membership mode for an interface	IC	3-95
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	3-95
switchport ingress-filtering	Enables ingress filtering on an interface	IC	3-96
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	3-97
switchport allowed vlan	Configures the VLANs associated with an interface	IC	3-97
switchport gvrp	Enables GVRP for an interface	IC	3-105
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	3-98
Display VLAN Information			
show vlan	Shows VLAN information	NE, PE	3-99
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	3-73
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	3-75

vlan database

Use this command to enter 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 (3-99)

vlan

Use this command to configure a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.
  - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (3-99)

interface vlan

Use this command to enter interface configuration mode for VLANs, and configure a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (3-71)

switchport mode

Use this command to configure the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**trunk** | **hybrid**}
no switchport mode

- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

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 (3-95)

switchport acceptable-frame-types

Use this command to configure 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 passes 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 passed 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 (3-95)

switchport ingress-filtering

Use this command to enable ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

switchport ingress-filtering
no switchport ingress-filtering

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

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

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

Use this command to configure the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

switchport allowed vlan

Use this command to configure VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}
no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan

Use this command to configure forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport forbidden vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

show vlan

Use this command to show VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
  - *vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.

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 Type    Name         Status    Ports/Channel groups
---- ------- ----------- ------    ------------------------------------
1    Static  DefaultVlan  Active Eth1/1  Eth1/2  Eth1/3  Eth1/4  Eth1/5
                                 Eth1/6  Eth1/7  Eth1/8  Eth1/9  Eth1/10
                                 Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                 Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                 Eth1/21 Eth1/22 Eth1/23 Eth1/24
Console#
```

Private VLAN Commands

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This switch supports three types of private VLAN ports: promiscuous, isolated, and community ports. A promiscuous port can communicate with all interfaces within a private VLAN. An isolated port can only communicate with promiscuous ports within its own VLAN. Community ports can only communicate with other ports in their own community VLAN, and with their designated promiscuous ports. This section describes commands used to configure private VLANs.

Command	Function	Mode	Page
Edit Private VLAN Groups			
private-vlan	Adds or deletes primary and secondary VLANs	VC	3-101
private-vlan association	Associates a secondary with a primary VLAN	VC	3-101
Configure Private VLAN Interfaces			
switchport mode private-vlan	Sets an interface to host, isolated, or promiscuous mode	IC	3-102
switchport private-vlan host-association	Associates an interface with a secondary VLAN	IC	3-103
switchport private-vlan mapping	Maps an interface to a primary VLAN	IC	3-103
Display Private VLAN Information			
show vlan private-vlan	Shows Private VLAN information	NE, PE	3-104

To configure private VLANs, follow these steps:

1. Use the **private-vlan** command to designate one or more isolated or community VLANs and the primary VLAN that will channel traffic outside the community groups.

2. Use the **private-vlan association** command to map the secondary (i.e., isolated or 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), isolated (i.e., having access only to promiscuous ports in its own VLAN), or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through a promiscuous port).

4. Use the **switchport private-vlan host-association** command to assign a port to a secondary VLAN.

5. Use the **switchport private-vlan mapping** command to assign a port to a primary VLAN.

6. Use the **show vlan private-vlan** command to verify your configuration settings.

private-vlan

Use this command to create a primary or secondary (i.e., isolated or community) private VLAN. Use the **no** form to remove the specified private VLAN.

Syntax

private-vlan *vlan-id* {**community** | **isolated** | **primary**}
no private-vlan *vlan-id*

- *vlan-id* – ID of private VLAN. (Range: 1-4094, no leading zeroes).
- **community** – Specifies a community VLAN.
- **isolated** – Specifies an isolated VLAN.
- **primary** – Specifies a primary VLAN.

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

- Private VLANs are used to restrict traffic to ports within the same VLAN “community,” and channel traffic passing outside the community through promiscuous ports that have been mapped to the associated “primary” VLAN.
- Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.
- Private VLAN ports cannot be set to trunked mode. (See “switchport mode” on page 3-95.)

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 private VLAN. (Range: 1-4094, no leading zeroes).
- *secondary-vlan-id* - ID of private (i.e., isolated or community) VLAN. (Range: 1-4094, no leading zeroes).

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

Secondary VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (e.g., servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).

Example

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

switchport mode private-vlan

Use this command to set the private VLAN mode for an interface. Use the **no** form to restore the default setting.

Syntax

switchport mode private-vlan {**host** | **promiscuous**}
no switchport mode private-vlan

- **host** – This port type can communicate with all other host ports assigned to the same secondary VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
- **promiscuous** – This port type can communicate with all other promiscuous ports in the same primary VLAN, as well as with all the ports in the associated secondary VLANs.

Default Setting

Normal VLAN

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with all other promiscuous ports in the same VLAN, as well as with all the ports in the associated secondary VLANs.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config)#
```

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, isolated or 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 a promiscuous port.

Example

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config)#
```

switchport private-vlan mapping

Use this command to map an interface to a primary VLAN. Use the **no** form to remove this mapping.

Syntax

switchport private-vlan mapping *primary-vlan-id*
no switchport private-vlan mapping

primary-vlan-id – ID of primary VLAN.
(Range: 1-4094, no leading zeroes).

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated secondary VLANs.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
```

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 associate primary VLAN and assigned host interfaces.
- **isolated** – Displays all isolated VLANs, along with their associate primary VLAN and assigned host interfaces.
- **primary** – Displays all primary VLANs, along with any assigned promiscuous interfaces.

Default Setting

None

Command Mode

Privileged Executive

Example

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

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Command	Function	Mode	Page
Interface Commands			
switchport gvrp	Enables GVRP for an interface	IC	3-105
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	3-98
show gvrp configuration	Displays GVRP configuration for selected interface	NE, PE	3-106
garp timer	Sets the GARP timer for the selected function	IC	3-106
show garp timer	Shows the GARP timer for the selected function	NE, PE	3-107
Global Commands			
bridge-ext gvrp	Enables GVRP globally for the switch	GC	3-108
show bridge-ext	Shows the global bridge extension configuration	PE	3-108

switchport gvrp

Use this command to enable GVRP for a port. Use the **no** form to disable it.

Syntax

switchport gvrp
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 gvrp configuration

Use this command to show if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

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#
```

garp timer

Use this command to set the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.
  Ranges:
  join: 20-1000 centiseconds
  leave: 60-3000 centiseconds
  leavall: 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

Caution: 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 (3-107)

show garp timer

Use this command to show the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 centiseconds
 Leave timer: 60 centiseconds
 Leaveall timer: 1000 centiseconds

Console#
```

Related Commands

garp timer (3-106)

bridge-ext gvrp

Use this command to enable GVRP globally for the switch. Use the **no** form to disable it.

Syntax

bridge-ext gvrp
no bridge-ext gvrp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

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

show bridge-ext

Use this command to show the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Displaying Basic VLAN Information” on page 2-81 and “Displaying Bridge Extension Capabilities” on page 2-10 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```

Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	3-109
show port monitor	Shows the configuration for a mirror port	PE	3-110

port monitor

Use this command to configure 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)
  - *unit* - Switch (unit 1).
  - *port* - Port number.
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the 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.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

Use this command to display mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit*/*port* (source port)

- *unit* - Switch (unit 1).
- *port* - Port number.

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#
```

Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	3-66
channel-group	Adds a port to a trunk	IC	3-112
Dynamic Configuration Command			
lacp	Configures LACP for the current interface	IC	3-112
Trunk Status Display Command			
show interfaces status port-channel	Shows trunk information	NE, PE	3-73

Guidelines for Creating Trunks

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to four 10/100 Mbps ports or up to two 1000 Mbps ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must consist of the same media type (i.e., twisted-pair or fiber).

- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

channel-group

Use this command to add 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: 1-6)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

Use this command to enable 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

lacp
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 four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 11 - 13. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 100tx
  Mac address: 00-00-e8-00-00-0b
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control status: Disabled
 Current status:
  Created by: lacp
  Link status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```

Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

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

Rate limit granularity is an additional feature enabling the network manager greater control over traffic on the network. The "rate limit granularity" is multiplied by the "rate limit level" (page 3-114) to set the actual rate limit for an interface. Granularity is a global setting that applies to Fast Ethernet or Gigabit Ethernet interfaces.

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for a port	IC	3-114
rate-limit granularity	Sets the Fast Ethernet and Gigabit Ethernet granularity	IC	3-115
show rate-limit	Shows the rate limit granularity	PE	3-115

rate-limit

Use this command to define the rate limit level for a specific interface. Use this command without specifying a rate to restore the default rate limit level. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {**input** | **output**} [*level*]
no rate-limit {**input** | **output**}

- **input** – Input rate.
- **output** – Output rate.
- *level* – Rate limit level. (Range: 1 - 30)

Default Setting

30

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Actual rate limit = Rate limit level * Granularity

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input level 10
Console(config-if)#
```

rate-limit granularity

Use this command to define the rate limit granularity for the Fast Ethernet ports, and the Gigabit Ethernet ports. Use the no form of this command to restore the default setting.

Syntax

rate-limit {**fastethernet** | **gigabitethernet**} **granularity** [*granularity*]
no rate-limit {**fastethernet** | **gigabitethernet**} **granularity**

- **fastethernet** – Gigabit Ethernet granularity.
- **gigabitethernet** – Fast Ethernet granularity.
- *granularity* – Sets rate limit granularity for the system. For Fast Ethernet, choose 512 Kbps,1000 Kbps, or 3300 Kbps. For Gigabit Ethernet, only one granularity option is supported, 33300 Kbps.

Default Setting

Fast Ethernet interface – 3.3 Mbps
Gigabit Ethernet interface – 33.3 Mbps

Command Mode

Global Configuration (Ethernet, Port Channel)

Command Usage

Actual rate limit = Rate limit level * Granularity

Example

The following sets Fast Ethernet granularity to 1 Mbps, and Gigabit Ethernet granularity to 33.3 Mbps.

```
Console(config)#rate-limit fastethernet granularity 1000
Console(config)#rate-limit gigabitethernet granularity 33300
Console(config)#
```

show rate-limit

Use this command to display the rate limit granularity.

Default Setting

Fast Ethernet interface – 3.3 Mbps
Gigabit Ethernet interface – 33.3 Mbps

Command Mode

Privileged Exec

Command Usage

- For Fast Ethernet interfaces, the rate limit granularity is 512 Kbps, 1 Mbps, or 3.3 Mbps.
- For Gigabit Ethernet interfaces, the rate limit granularity is 33.3 Mbps.

Example

```
Console#show rate-limit

Fast ethernet granularity:  1000

Gigabit ethernet granularity:  33300
Console#
```

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local, RADIUS, or TACACS authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1x.

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 or group that require management access to a switch.

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 an authentication server using EAP (Extensible Authentication Protocol).

Command	Function	Mode	Page
Authentication Method			
authentication login	Defines logon authentication method and precedence	GC	3-118
RADIUS Client			
radius-server host	Specifies the RADIUS server	GC	3-119
radius-server port	Sets the RADIUS server network port	GC	3-119
radius-server key	Sets the RADIUS encryption key	GC	3-120
radius-server retransmit	Sets the number of retries	GC	3-120
radius-server timeout	Sets the interval between sending authentication requests	GC	3-121
show radius-server	Shows the current RADIUS settings	PE	3-121
TACACS+ Client			
tacacs-server host	Specifies the TACACS+ server	GC	3-121
tacacs-server port	Specifies the TACACS+ server network port	GC	3-122
tacacs-server key	Sets the TACACS+ encryption key	GC	3-122
show tacacs-server	Shows the current TACACS+ settings	GC	3-123
Port Authentication			
authentication dot1x default	Sets the default authentication server type	GC	3-123
dot1x default	Resets all dot1x parameters to their default values.	GC	3-123
dot1x max-req	Sets the maximum number of times the switch will attempt to send a request to the client before authentication fails	GC	3-124
dot1x port-control	Sets dot1x mode for a port interface	IC	3-124
dot1x re-authenticate	Forces a re-authentication on specific ports	PE	3-125
dot1x re-authentication	Enables re-authentication for all ports	GC	3-125

Command	Function	Mode	Page
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	GC	3-126
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	GC	3-126
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	GC	3-127
show dot1x	Shows all dot1x related information	PE	3-127

authentication login

Use this command to define 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 only.
- **radius** - Use RADIUS server password only.
- **tacacs** - Use TACACS server password only.

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.
- RADIUS and TACACS+ logon authentication can control management access via the console port, a Web browser, or Telnet. These access options must be configured on the authentication server.
- 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 (3-21)

radius-server host

Use this command to specify the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server host *host_ip_address*
no radius-server host

host_ip_address - IP address of server.

Default Setting

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

radius-server port

Use this command to set the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

Use this command to set 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

Use this command to set 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

Use this command to set 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

Use this command to display the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server
Remote radius server configuration:
 Server IP address: 10.1.0.1
 Communication key with radius server:
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

tacacs-server host

Use this command to specify the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

Use this command to specify the TACACS+ server TCP port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

Use this command to set 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: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

Use this command to display the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Global Configuration

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 10.11.12.13
 Communication key with TACACS server: green
 Server port number: 49
Console#
```

authentication dot1x default

Sets the default authentication server type. Use the **no** form to restore the default.

Syntax

authentication dot1x default radius
no authentication dot1x

Default Setting

RADIUS

Command Mode

Global Configuration

Example

```
Console(config)#authentication dot1x default radius
Console(config)#
```

dot1x default

Sets all configurable dot1x global and port settings to their default values.

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

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. 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

Global Configuration

Example

```
Console(config)#dot1x max-req 2
Console(config)#
```

dot1x port-control

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-authenticate

Forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

Enables periodic re-authentication globally for all ports. Use the **no** form to disable re-authentication.

Syntax

dot1x re-authentication
no dot1x re-authentication

Command Mode

Global Configuration

Example

```
Console(config)#dot1x re-authentication
Console(config)#
```

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. Use the **no** form of this command to reset the default.

Syntax

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period *seconds*

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout quiet-period 350
Console(config)#
```

dot1x timeout re-authperiod

Sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout re-authperiod 3600
Console(config)#
```

dot1x timeout tx-period

Sets the time that 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

Global Configuration

Example

```
Console(config)#dot1x timeout tx-period 300
Console(config)#
```

show dot1x

Use this command to show general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Displays the global port access control parameters that can be configured for this switch as described in the preceding pages, including reauth-period (page 3-126), quiet-period (page 3-126), tx-period (page 3-127), and max-req (page 3-124). It also displays the following global parameters which are set to a fixed value, including the following items:
  - supp-timeout – Supplicant timeout.
  - server-timeout – Server timeout.
  - reauth-max – Maximum number of reauthentication attempts.

- *802.1X Port Summary* – Displays the port access control parameters for each interface, including the following items:
  - Status – Administrative state for port access control.
  - Mode – Dot1x port control mode (page 3-124).
  - Authorized – Authorization status (yes or n/a - not authorized).
- *802.1X Port Details* – Displays detailed port access control settings for each interface as described in the preceding pages, including administrative status for port access control, Max request (page 3-124), Quiet period (page 3-126), Reauth period (page 3-126), and Tx period (page 3-127). It also displays the following information:
  - Status – Authorization status (authorized or unauthorized).
  - Supplicant – MAC address of authorized client.
- *Authenticator State Machine*
  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
  - Reauth Count – Number of times connecting state is re-entered.
- *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
 reauth-enabled: yes
 reauth-period:  300
 quiet-period:   350
 tx-period:      300
 supp-timeout:   30
 server-timeout: 30
 reauth-max:     2
 max-req:        2

802.1X Port Summary
 Port Name     Status           Mode          Authorized
         1       disabled    ForceAuthorized           n/a
         2       disabled    ForceAuthorized           n/a
:
        25       disabled    ForceAuthorized           yes
        26        enabled               Auto           yes

802.1X Port Details

802.1X is disabled on port 1
:
802.1X is enabled on port 26
Max request         2
Quiet period        350
Reauth period       300
Tx period           300
Status              Unauthorized
Port-control        Auto
Supplicant          00-00-00-00-00-00

Authenticator State Machine
State               Connecting
Reauth Count        3
Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  0

Reauthentication State Machine
State               Initialize
Console#
```

Access Control List Commands

Access Control Lists (ACL) provide packet 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). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

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 incoming packets against the conditions in an ACL one by one. If a list contains all permit rules, a packet will be accepted as soon as it passes any of the rules. If a list contains all deny rules, then a packet will be rejected as soon as it fails any one of the rules. In other words, if no rules match for a permit list, the packet is dropped; and if no rules match for a deny list, the packet is accepted.

There are three filtering modes:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and TCP/UDP port number. If the TCP protocol type is specified, then you can also filter packets based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters based on the source, destination MAC address and the Ethernet frame type (RFC 1060).

Caution: An access list can only contain all permit rules or all deny rules. In other words, for performance reasons, you cannot mix permit and deny rules in the same list.

Command Groups	Function	Page
IP ACLs	Configures ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code	3-131
MAC ACLs	Configures ACLs based on hardware addresses and Ethernet type	3-138
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port	3-141

IP ACLs

Command	Function	Mode	Page
access-list ip	Creates an IP ACL and enters configuration mode	GC	3-131
permit, deny	Filters packets matching a specified source IP address	STD-ACL	3-132
permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	EXT-ACL	3-133
ip access-group	Adds a port to an IP ACL	IC	3-135
show ip access-group	Shows port assignments for IP ACLs	PE	3-135
show ip access-list	Displays the rules for configured IP ACLs	PE	3-136
map access-list ip	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC	3-136
show map access-list ip	Shows CoS value mapped to an access list for an interface	PE	3-137

access-list ip

Use this command to add an IP access list and enter configuration mode for standard or extended IP ACLs. Use the **no** form to remove the specified ACL.

Syntax

access-list ip {**standard** | **extended**} *acl_name*
no access-list ip {**standard** | **extended**} *acl_name*

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An ACL can contain either all permit commands or all deny commands.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

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

Related Commands

permit, deny 3-132
ip access-group (3-135)
show ip access-list (3-136)

permit, **deny** (Standard ACL)

Use this command to add a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

{**permit | deny**} {**any** | *source bitmask* | **host** *source*}
no {**permit | deny**} {**any** | *source bitmask* | **host** *source*}

- **any** – Any source IP address.
- *source* – Source IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard ACL

Command Usage

- New rules are added to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bit 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 (3-131)

permit, **deny** (Extended ACL)

Use this command to add a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source and destination IP addresses, protocol types, source and destination TCP/UDP ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

{**permit | deny**} {**any** | *source bitmask* | **host** *source*}
{**any** | *destination bitmask* | **host** *destination*} [**protocol** *protocol-number*]
no {**permit | deny**} {**any** | *source bitmask* | **host** *source*}
{**any** | *destination bitmask* | **host** *destination*} [**protocol** *protocol-number*]

{**permit | deny**} {**tcp**} {**any** | *source bitmask* | **host** *source*}
{**any** | *destination bitmask* | **host** *destination*}
[**source-port** *source-port*] [**destination-port** *destination-port*]
[**control-flag** *control-flag flag-bitmask*]
no {**permit | deny**} {**tcp**} {**any** | *source bitmask* | **host** *source*}
{**any** | *destination bitmask* | **host** *destination*}
[**source-port** *source-port*] [**destination-port** *destination-port*]
[**control-flag** *control-flag flag-bitmask*]

{**permit | deny**} {**udp**} {**any** | *source bitmask* | **host** *source*}
{**any** | *destination bitmask* | **host** *destination*}
[**source-port** *source-port*] [**destination-port** *destination-port*]
no {**permit | deny**} {**udp**} {**any** | *source bitmask* | **host** *source*}
{**any** | *destination bitmask* | **host** *destination*}
[**source-port** *source-port*] [**destination-port** *destination-port*]

- **any** – Any IP address (source if first field, destination if second field).
- *source* – Source IP address.
- *destination* – Destination IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.
- *source-port* – TCP/UDP source port number. (Range: 0-65535)
- *destination-port* – TCP/UDP destination port number. (Range: 0-65535)
- *protocol-number* – A specific protocol number. (Range: 0-255)
- *control-flag* – 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.

Default Setting

None

Command Mode

Extended ACL

Command Usage

- All new rules are added to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bit to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-flag 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-flag 2 2”
  - Both SYN and ACK valid, use “control-flag 18 18”
  - SYN valid and ACK invalid, use “control-flag 2 18”

Examples

This permits only 192.168.1.1 and 210.244.51.x.

```
Console(config-ext-acl)#permit 192.168.1.1 255.255.255.0 any
Console(config-ext-acl)#permit 210.244.51.0 255.255.255.0 any
Console(config-ext-acl)#deny any any
Console(config-ext-acl)#
```

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 tcp 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 (3-131)

ip access-group

Use this command to bind a port to an IP ACL. Use the **no** form to remove the port.

Syntax

ip access-group *acl_name* **in**
no ip access-group *acl_name* **in**

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to input packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#int eth 1/12
Console(config-if)#ip access-group mark in
Console(config-if)#
```

Related Commands

show ip access-list (3-136)

show ip access-group

Use this command to show the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/25
 IP standard access-list david
Console#
```

Related Commands

ip access-group (3-135)

show ip access-list

Use this command to display the rules for configured IP ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
Console#
```

Related Commands

permit, deny 3-132
ip access-group (3-135)

map access-list ip

This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. Use the **no** form to remove the CoS mapping.

Syntax

[**no**] **map access-list ip** *acl_name* **cos** *cos-value*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *cos-value* – CoS value. (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

A packet matching a rule within the specified ACL is mapped to one of the output queues as shown in the following table. For information on mapping the CoS values to output queues, see **queue cos-map** on page 3-145.

Priority Level	0	1	2	3	4	5	6	7
Output Queue	1	0	0	1	2	2	3	3

Example

```
Console(config)#interface ethernet 1/25
Console(config-if)#map access-list ip bill cos 0
Console(config-if)#
```

Related Commands

queue cos-map (3-145)
show map access-list ip (3-137)

show map access-list ip

This command shows the CoS value mapped to an IP ACL for the current interface. (The CoS value determines the output queue for packets matching an ACL rule.)

Syntax

show map access-list ip [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#show map access-list ip
Access-list to COS of Eth 1/24
 Access-list ALS1 cos 0
Console#
```

Related Commands

map access-list ip (3-136)

MAC ACLs

Command	Function	Mode	Page
access-list mac	Creates a MAC ACL and enters configuration mode	GC	3-138
permit, deny	Filters packets matching a specified source and destination address and Ethernet type	MAC-ACL	3-139
mac access-group	Adds a port to a MAC ACL	IC	3-140
show mac access-group	Shows port assignments for MAC ACLs	PE	3-140
show mac access-list	Displays the rules for configured MAC ACLs	PE	3-141

access-list mac

Use this command to add a MAC access list and enter MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

access-list mac *acl_name*
no access-list mac *acl_name*

acl_name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An ACL can contain either all permit commands or all deny commands.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

permit, deny 3-139
mac access-group (3-140)
show mac access-list (3-141)

permit, **deny** (MAC ACL)

Use this command to add a rule to a MAC ACL. The rule filters by 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 bitmask*}
{**any** | **host** *destination* | *destination bitmask*}
{**any** | **ethertype** *protocol*}
no {**permit** | **deny**}
{**any** | **host** *source* | *source bitmask*}
{**any** | **host** *destination* | *destination bitmask*}
{**any** | **ethertype** *protocol*}

- **any** – Any MAC source address, destination address, or Ethernet protocol.
- *source* – Source MAC address.
- *source bitmask* – Binary mask for the source MAC address.
- *destination* – Destination MAC address.
- *destination bitmask* – Binary mask for the destination MAC address.
- *protocol* – A specific Ethernet protocol number. (Range: 0-65535)

Default Setting

None

Command Mode

MAC ACL

Command Usage

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

Related Commands

access-list mac (3-138)

mac access-group

Use this command to bind ports to a MAC ACL. Use the **no** form to remove the ports.

Syntax

mac access-group *acl_name* **in**

acl_name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Note although this is a per-port setting, changes affect all ports.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

show mac access-list (3-141)

show mac access-group

Use this command to show the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/25
 MAC access-list jerry
Console#
```

Related Commands

mac access-group (3-140)

show mac access-list

Use this command to display 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 3-139
mac access-group (3-140)

ACL Information

Command	Function	Mode	Page
show access-list	Show all ACLs and associated rules	PE	3-141
show access-group	Shows the ACLs assigned to each port	PE	3-142

show access-list

Use this command to show all ACLs and associated rules.

Command Mode

Privileged Exec

Example

```
Console#show access-list
MAC access-list jerry:
  permit any 00-30-29-94-34-de ethertype 0800
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
IP extended access-list bob:
  permit 10.7.1.1 0.0.0.255 any
  permit tcp 192.168.1.0 0.0.0.255 any destination-port 80
  permit tcp 192.168.1.0 0.0.0.255 any protocol tcp control-flag 2 2
Console#
```

show access-group

Use this command to show the port assignments of ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/25
 IP standard access-list david
 MAC access-list jerry in
Console#
```

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four egress queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Command	Function	Mode	Page
Layer 2 Priority Commands			
switchport priority default	Sets a port priority for incoming untagged frames	IC	3-143
queue mode	Sets the queue mode to strict priority or Weighted Round-Robin (WRR)	GC	3-144
queue bandwidth	Assigns round-robin weights to the priority queues	GC	3-144
queue cos map	Assigns class of service values to the priority queues	IC	3-145
show queue mode	Shows the current queue mode	PE	3-147
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	3-147
show queue cos-map	Shows the class of service map	PE	3-147
show interfaces switchport	Displays the administrative and operational status of an interface	PE	3-75
Layer 3 and 4 Priority Commands			
map ip port	Enables TCP class of service mapping	GC	3-148
map ip port	Maps TCP socket to a class of service	IC	3-148
map ip precedence	Enables IP precedence class of service mapping	GC	3-149
map ip precedence	Maps IP precedence value to a class of service	IC	3-150
map ip dscp	Enables IP DSCP class of service mapping	GC	3-151
map ip dscp	Maps IP DSCP value to a class of service	IC	3-151
show map ip port	Shows the IP port map	PE	3-152

Command	Function	Mode	Page
show map ip precedence	Shows the IP precedence map	PE	3-153
show map ip dscp	Shows the IP DSCP map	PE	3-154

switchport priority default

Use this command to set 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 level is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides four egress queues (traffic classes) for each port. It is configured to use Weighted Round Robin, which can be viewed with the **show queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console (config-if)#switchport priority default 5
```

queue mode

This command sets the queue mode to strict priority or Weighted Round-Robin (WRR) for the class of service (CoS) egress queues. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr**}
no queue mode

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1~31 for queues 0 - 3 respectively.

Default Setting

Weighted Round Robin

Command Mode

Global Configuration

Command Usage

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

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

queue bandwidth

Use this command to assign weighted round-robin (WRR) weights to the four class of service (CoS) egress queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight0...weight3*
no queue bandwidth

weight0...weight3 - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 31)

Default Setting

Weights 1, 2, 4 and 6 are assigned to queues 0, 1, 2 and 3 respectively.

Command Mode

Global Configuration

Command Usage

WRR controls bandwidth sharing at the egress port by defining scheduling weights.

Example

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

```
Console(config)#queue bandwidth 1 1 4 16
Console(config)#
```

Related Commands

show queue bandwidth (3-147)

queue cos-map

Use this command to assign Class of Service (CoS) values to the egress queues (i.e., hardware output queues 0 - 3). Use the **no** form to set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The ID of the priority queue.

  Range is 0 to 3, where 3 is the highest priority queue.
- *cos1 .. cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using four egress queues, with Weighted Round Robin queuing for each port. Eight separate priority levels are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

	Egress Queue			
	0	**1**	**2**	**3**
Priority Level		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

CoS assigned at the ingress port is used to select a CoS priority at the egress port.

Example

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

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 1 2
Console(config-if)#queue cos-map 1 0 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

Related Commands

show queue cos-map (3-147)

show queue mode

This command shows the current queue mode.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue mode

Queue mode: wrr
Console#
```

show queue bandwidth

Use this command to display the weighted round-robin (WRR) bandwidth allocation for the priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
        0      1
        1      1
        2      4
        3      16
Console#
```

show queue cos-map

Use this command to show the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/11
Information of Eth 1/11
 Priority Queue: 0 1 2 3 4 5 6 7
 Traffic Class : 1 0 0 1 2 2 3 3
Console#
```

map ip port (Global Configuration)

Use this command to enable IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

Syntax

map ip port
no map ip port

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

map ip port (Interface Configuration)

Use this command to set IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*
no map ip port *port-number*

- *port-number* - 16-bit TCP/UDP port number. (Range: 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.
- This command sets the IP port priority for all interfaces.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

map ip precedence (Global Configuration)

Use this command to enable IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

map ip precedence
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 precedence (Interface Configuration)

Use this command to set 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.

IP Precedence Value	CoS Value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	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 four 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)#
```

map ip dscp (Global Configuration)

Use this command to enable IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

map ip dscp
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 dscp (Interface Configuration)

Use this command to set 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 - 6-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.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3

26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the four hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip port

Use this command to show the IP port priority map.

Syntax

show map ip port [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

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

Related Commands

map ip port (Global Configuration) (3-148)
map ip port (Interface Configuration) (3-148)

show map ip precedence

Use this command to show the IP precedence priority map.

Syntax

show map ip precedence [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

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

Related Commands

map ip precedence (Global Configuration) (3-149)
map ip precedence (Interface Configuration) (3-150)

show map ip dscp

Use this command to show the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

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#
```

Related Commands

map ip dscp (Global Configuration) (3-151)
map ip dscp (Interface Configuration) (3-151)

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Command	Function	Mode	Page
Basic IGMP Commands			
ip igmp snooping	Enables IGMP snooping	GC	3-155
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	3-156
ip igmp snooping version	Configures the IGMP version for snooping	GC	3-156
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE	3-157
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE	3-158
IGMP Querier Commands			
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	3-158
ip igmp snooping query-count	Configures the query count	GC	3-159
ip igmp snooping query-interval	Configures the query interval	GC	3-160
ip igmp snooping query-max-response-time	Configures the report delay	GC	3-160
ip igmp snooping router-port-expire-timeout	Configures the query timeout	GC	3-161
show ip igmp snooping	Shows the IGMP snooping configuration	PE	3-157
Multicast Router Commands			
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	3-162
show ip igmp snooping mrouter	Shows multicast router ports	PE	3-162

ip igmp snooping

Use this command to enable IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

ip igmp snooping
no ip igmp snooping

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

Use this command to add a port to a multicast group. Use the **no** form to remove the port.

Syntax

ip igmp snooping vlan *vlan-id* **static** *ip-address interface*
no ip igmp snooping vlan *vlan-id* **static** *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

ip igmp snooping version

Use this command to configure the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

Use this command to show the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Configuring IGMP Snooping Parameters” on page 2-74 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Query time-out: 300 sec
 IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

Use this command to show known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4094)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

ip igmp snooping querier

Use this command to enable the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

ip igmp snooping querier
no ip igmp snooping querier

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

Use this command to configure the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max-response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (3-160)

ip igmp snooping query-interval

Use this command to configure the query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

Use this command to configure the snooping report delay. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-30)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (3-156)
ip igmp snooping query-max-response-time (3-160)

ip igmp snooping router-port-expire-time

Use this command to configure the query timeout. Use the no form of this command to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.
(Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping query-time-out 300
Console(config)#
```

Related Commands

ip igmp snooping version (3-156)

ip igmp snooping vlan mrouter

Use this command to statically configure 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: 1-4094)
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)

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 switch, 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

Use this command to display information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static 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
Console#
```

Appendix A: Upgrading Firmware via the Serial Port

The switch contains three firmware components that can be upgraded; the diagnostics (or Boot-ROM) code, runtime operation code and the loader code. The runtime code can be upgraded via the switch’s RS-232 serial console port, via a network connection to a TFTP server, or using SNMP management software. The diagnostics and the loader code can be upgraded only via the switch’s RS-232 serial console port.

Note: You can use the switch’s web interface to download runtime code via TFTP. Downloading large runtime code files via TFTP is normally much faster than downloading via the switch’s serial port.

You can upgrade switch firmware by connecting a PC directly to the serial Console port on the switch’s front panel and using VT100 terminal emulation software that supports the XModem protocol. (See “Required Connections” on page 1-2.)

1. Connect a PC to the switch’s Console port using a null-modem or crossover RS-232 cable with a female DB-9 connector.

2. Configure the terminal emulation software’s communication parameters to 9600 baud, 8 data bits, 1 stop bit, no parity, and set flow control to *none*.

3. Power cycle the switch.

4. When the switch initialization screen appears, enter firmware-download mode by pressing <Ctrl><u> immediately after power on or rebooting the switch. Screen text similar to that shown below displays:

```
File Name                         S/Up Type Size       Create Time
--------------------------------- ---- ---- ----------
$logfile_1                          0    3          64  00:00:16
$logfile_2                          0    3          64  00:00:33
Factory_Default_Config.cfg          0    5        2688  00:00:14
diag1011                            1    1       86944  00:00:00
mdc0115                             0    2     1120008  00:00:01
mdc0121.bix                         1    2     1135548  00:00:01
startup                             1    5        2783  00:03:28
--------------------------------- ---- ---- ----------
[X]modem Download  [D]elete File  [S]et Startup File
[C]hange Baudrate  [Q]uit
Select>
```

5. Press <C> to change the baud rate of the switch’s serial connection.

6. Press <B> to select the option for 115200 baud.

   There are two baud rate settings available, 9600 and 115200. Using the higher baud rate minimizes the time required to download firmware code files.

7. Set your PC’s terminal emulation software to match the 115200 baud rate. Press <Enter> to reset communications with the switch.

```
Select>
Change baudrate [A]9600 [B]115200
Baudrate set to 115200
```

8. Check that the switch has sufficient flash memory space for the new code file before starting the download.

   You can store a maximum of only two runtime and two diagnostic code files in the switch’s flash memory. Use the [**D]elete File** command to remove a runtime or diagnostic file.

9. Press <X> to start to download the new code file.

   If using Windows HyperTerminal, click the “Transfer” button, and then click “Send File....” Select the XModem Protocol and then use the “Browse” button to select the required firmware code file from your PC system. The “Xmodem file send” window displays the progress of the download procedure.

   Note: The download file must be a valid binary software file for this switch.

10. After the file has been downloaded, you are prompted with “Update Image File:” to specify the type of code file. Press <R> for runtime code, <D> for diagnostic code, or <L> for loader code.

    Caution: If you select <L> for loader code, be sure the file is a valid loader code file for the switch. If you download an invalid file, the switch will not be able to boot. Unless absolutely necessary, do not attempt to download loader code files.

11. Specify a name for the downloaded code file. File names are case-sensitive, should be 1 to 31 characters, should not contain slashes (\ or /), and the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

For example, the following screen text shows the download procedure for a runtime code file:

```
Select>x
Xmodem Receiving Start ::
        [R]untime
        [D]iagnostic
        [L]oader
Update Image File:r
Runtime Image Filename : run_1013
Updating file system.
File system updated.
[Press any key to continue]
```

12. To set the new downloaded file as the startup file, use the **[S]et Startup File** menu option.
13. When you have finished downloading code files, use the **[C]hange Baudrate** menu option to change the baud rate of the switch’s serial connection back to 9600 baud.
14. Set your PC’s terminal emulation software baud rate back to 9600 baud. Press <Enter> to reset communications with the switch.
15. Press <Q> to quit the firmware-download mode and boot the switch.

Appendix B: Troubleshooting

Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, Web browser, or SNMP software	• Be sure you have configured the agent with a valid IP address, subnet mask and default gateway. • If you are trying to connect to the agent via the IP address for a tagged VLAN group, your management station must include the appropriate tag in its transmitted frames. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Check network cabling between the management station and the switch. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted. Try connecting again at a later time.
Cannot access the on-board configuration program via a serial port connection	• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps. • Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B.
Forgot or lost the password	• Reinstall the switch defaults. Make a direct connection to the switch's console port and power cycle the switch. Immediately after powering on, press <Ctrl><u> to access the system file menu. Select <D> to delete all user-defined configuration files. Press <Q> to boot the switch.

Glossary

Access Control List (ACL)

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.

Boot Protocol (BOOTP)

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.

Class of Service (CoS)

CoS 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.

Differentiated Services Code Point Service (DSCP)

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.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)

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.

Extensible Authentication Protocol over LAN (EAPOL)

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.

GARP VLAN Registration Protocol (GVRP)

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.

Generic Attribute Registration Protocol (GARP)

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.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register endstations with multicast groups. GMRP requires that any participating network devices or endstations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol

See Generic Attribute Registration Protocol.

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 class of service priority 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 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3

Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3ab

Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3u

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX and 100BASE-FX Fast Ethernet.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IEEE 802.3z

Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet.

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.

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.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is made the “querier” and assumes responsibility for keeping track of group membership.

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.

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.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Media Access Control (MAC)

A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

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.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1x.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

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.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Secure Shell (SSH)

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.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP 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.

Spanning Tree Protocol (STP)

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.

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP)

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.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Index