TigerAccess Extended Ethernet System

Extended Ethernet System

- High-speed Internet access over existing phone lines
- Supports 24 Extended Ethernet lines
- Optional 1000BASE-X modules
- Concurrent data and telephone services (voice/ISDN) over a single connection
- Supports evolving ETSI, ANSI, and ITU standards for the copper local loop
- Spanning Tree Protocol
- Supports port trunks
- QoS support for four-level priority
- Full support for VLANs with GVRP
- IGMP multicast filtering and snooping
- Manageable via console, RMON

SMC® Networks

Management Guide

SMC7724M/VSW

TigerAccess Extended Ethernet System Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions

SMC®
Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

December 2002
Pub. # 150200022300A

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Trademarks:
SMC is a registered trademark; and EZ Switch, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

Contents

1 **Switch Management 1-1**

Connecting to the Switch 1-1

Configuration Options 1-1

Required Connections 1-3

Remote Connections 1-4

Basic Configuration 1-5

Console Connection 1-5

Setting Passwords 1-6

Setting an IP Address 1-7

Manual Configuration 1-7

Dynamic Configuration 1-9

Enabling SNMP Management Access 1-10

Community Strings 1-10

Trap Receivers 1-11

Saving Configuration Settings 1-12

Managing System Files 1-12

System Defaults 1-13

2 **Configuring the Switch 2-1**

Using the Web Interface 2-1

Navigating the Web Browser Interface 2-3

Home Page 2-3

Configuration Options 2-4

Panel Display 2-5

Main Menu 2-5

Basic Configuration 2-9

Displaying System Information 2-9

Setting the IP Address 2-11

Manual Configuration 2-12

Using DHCP/BOOTP 2-12

Renewing DCHP 2-14

Security 2-14

Configuring the Login Password 2-14

Configuring Radius Logon Authentication 2-15

Managing Firmware 2-16

Downloading System Software from a Server 2-17

Saving or Restoring Configuration Settings 2-18
Setting the Startup Configuration File 2-20
Copying the Running Configuration to a File 2-21
Reset 2-22
Displaying Bridge Extension Capabilities 2-22
Displaying Switch Hardware/Software Versions 2-24
Port Configuration 2-26
Displaying Connection Status 2-26
Configuring Interface Connections 2-28
Setting Broadcast Storm Thresholds 2-30
Configuring Port Mirroring 2-31
Configuring Port Security 2-32
Address Table Settings 2-33
Displaying the Address Table 2-33
Setting Static Addresses 2-35
Changing the Aging Time 2-36
Spanning Tree Protocol Configuration 2-37
Managing Global Settings 2-37
Displaying the current global settings for STA 2-39
Configuring the global settings for STA 2-40
Managing Interface Settings 2-41
VLAN Configuration 2-45
Assigning Ports to VLANs 2-46
Forwarding Tagged/Untagged Frames 2-47
Enabling or Disabling GVRP (Global Setting) 2-48
Displaying Basic VLAN Information 2-49
Displaying Current VLANs 2-50
Creating VLANs 2-52
Adding Interfaces Based on Membership Type 2-53
Adding Interfaces Based on Static Membership 2-55
Configuring VLAN Behavior for Interfaces 2-56
Configuring Private VLANs 2-59
Enabling Private VLANs 2-59
Configuring Uplink and Downlink Ports 2-59
Class of Service Configuration 2-63
Setting the Default Priority for Interfaces 2-63
Mapping Priority Classes to Egress Queues 2-65
Queue Scheduling 2-67

Mapping Layer 3/4 Priorities to CoS Values 2-69
Mapping IP Precedence 2-70
Mapping DSCP Priority 2-73
Mapping IP Port Priority 2-75
Copy Priority Settings 2-77
Port Trunk Configuration 2-78
Configuring SNMP 2-81
Setting Community Access Strings 2-82
Specifying Trap Managers 2-83
Multicast Configuration 2-84
Configuring IGMP Parameters 2-84
Interfaces Attached to a Multicast Router 2-87
Displaying Port Members of Multicast Services 2-90
Adding Multicast Addresses to VLANs 2-91
Showing Device Statistics 2-92
Rate Limit Configuration 2-95
VDSL Configuration 2-97
VDSL Global Configuration 2-97
VDSL Port Configuration 2-99
Configuring a User-specified EFM Profile 2-101
VDSL Port Link Status 2-103
Displaying VDSL Port Ethernet Statistics 2-106

3 Command Line Interface 3-1

Using the Command Line Interface 3-1
Accessing the CLI 3-1
Console Connection 3-1
Telnet Connection 3-2
Entering Commands 3-3
Keywords and Arguments 3-3
Minimum Abbreviation 3-4
Command Completion 3-4
Getting Help on Commands 3-4
Partial Keyword Lookup 3-6
Negating the Effect of Commands 3-6
Using Command History 3-6
Understanding Command Modes 3-7
Exec Commands 3-7
Configuration Commands 3-8

Command Line Processing 3-9
Command Groups 3-10
General Commands 3-12
enable 3-13
disable 3-14
configure 3-15
show history 3-15
reload 3-16
end 3-17
exit 3-17
quit 3-18
Flash/File Commands 3-19
copy 3-19
delete 3-22
dir 3-23
whichboot 3-24
boot system 3-25
System Management Commands 3-26
hostname 3-27
username 3-28
enable password 3-29
ip http port 3-30
ip http server 3-31
logging on 3-31
logging history 3-32
clear logging 3-33
show logging 3-34
show startup-config 3-35
show running-config 3-36
show system 3-37
show users 3-37
show version 3-38
RADIUS Commands 3-39
authentication login 3-39
radius-server host 3-40
radius-server port 3-41
radius-server key 3-41
radius-server retransmit 3-42
radius-server timeout 3-42

show radius-server 3-43
SNMP Commands 3-44
snmp-server community 3-45
snmp-server contact 3-46
snmp-server location 3-46
snmp-server host 3-47
snmp-server enable traps 3-48
IP Commands 3-51
ip address 3-52
ip dhcp restart 3-53
ip default-gateway 3-54
show ip interface 3-55
show ip redirects 3-55
ping 3-56
Line Commands 3-58
line 3-59
login 3-59
password 3-60
exec-timeout 3-61
password-thresh 3-62
silent-time 3-63
databits 3-64
parity 3-65
speed 3-65
stopbits 3-66
show line 3-67
Interface Commands 3-68
interface 3-69
description 3-69
speed-duplex 3-70
negotiation 3-71
capabilities 3-72
flowcontrol 3-73
clear counters 3-74
shutdown 3-74
switchport broadcast 3-75
show interfaces status 3-76
show interfaces counters 3-77
show interfaces switchport 3-78

Address Table Commands 3-79
bridge address 3-79
show bridge 3-81
clear bridge 3-82
bridge-group aging-time 3-82
show bridge group aging-time 3-83
port security 3-84
Spanning Tree Commands 3-85
bridge spanning-tree 3-86
bridge forward-time 3-87
bridge hello-time 3-88
bridge max-age 3-89
bridge priority 3-90
bridge-group path-cost 3-91
bridge-group priority 3-92
bridge-group portfast 3-93
show bridge group 3-94
VLAN Commands 3-95
vlan database 3-96
vlan 3-97
interface vlan 3-98
switchport mode 3-99
switchport acceptable-frame-types 3-100
switchport ingress-filtering 3-100
switchport native vlan 3-101
switchport allowed vlan 3-102
switchport forbidden vlan 3-103
show vlan 3-104
PVLAN Commands 3-105
pvlan 3-105
show pvlan 3-107
GVRP and Bridge Extension Commands 3-108
switchport gvrp 3-109
show gvrp configuration 3-109
garp timer 3-110
show garp timer 3-111
bridge-ext gvrp 3-112
show bridge-ext 3-113
IGMP Snooping Commands 3-114

ip igmp snooping 3-115
ip igmp snooping vlan static 3-115
ip igmp snooping version 3-116
show ip igmp snooping 3-117
show bridge multicast 3-117
ip igmp snooping querier 3-118
ip igmp snooping query-count 3-119
ip igmp snooping query-interval 3-119
ip igmp snooping query-max-response-time 3-120
ip igmp snooping query-time-out 3-121
ip igmp snooping vlan mrouter 3-122
show ip igmp snooping mrouter 3-123
Priority Commands 3-124
switchport priority default 3-125
queue bandwidth 3-126
queue cos-map 3-127
show queue bandwidth 3-129
show queue cos-map 3-129
map ip port (Global Configuration) 3-130
map ip port (Interface Configuration) 3-131
map ip precedence (Global Configuration) 3-131
map ip precedence (Interface Configuration) 3-132
map ip dscp (Global Configuration) 3-133
map ip dscp (Interface Configuration) 3-134
show map ip port 3-135
show map ip precedence 3-136
show map ip dscp 3-137
Mirror Port Commands 3-138
port monitor 3-138
show port monitor 3-140
Port Trunking Commands 3-141
interface port-channel 3-142
channel-group 3-142
show interfaces status port-channel 3-143
lacp 3-144
VDSL Commands 3-146
efm profile global 3-147
efm profile 3-149
efm define user-profile 3-150

efm reset 3-151
efm shutdown 3-151
efm rdl 3-152
efm flow-control 3-153
show controllers ethernet-controller 3-154
show controllers efm interface-id actual 3-156
show controllers efm interface-id admin 3-157
show controllers efm profile 3-158
show controllers efm status 3-160
show controllers efm remote ethernet mode 3-162
Rate Limit Commands 3-163
rate-limit (global) 3-163
rate-limit (interface) 3-164

A Troubleshooting A-1
Troubleshooting Chart A-1
Upgrading Firmware via the Serial Port A-2

B Pin Assignments B-1
Console Port Pin Assignments B-1
DB-9 Port Pin Assignments B-1
Console Port to 9-Pin DTE Port on PC B-2
Console Port to 25-Pin DTE Port on PC B-2

CHAPTER 1
SWITCH MANAGEMENT

Connecting to the Switch

Configuration Options

The TigerAccess Extended Ethernet (EE) Switch 7724M/VSW 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 the switch is assigned via DHCP by default. To change this address, see "Setting an IP Address" on page 1-7.

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, such as SMC's free EliteView 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 usernames and passwords for up to 16 users
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any VDSL or Ethernet port
- Set the speed/duplex mode for any port
- Assign operating profiles to any VDSL port
- Configure Private VLANs for port isolation
- Configure input traffic rate limit on any port
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- TFTP upload and download of system firmware
- TFTP upload and download of switch configuration files
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to six static or LACP trunks
- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics

Required Connections

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

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 Appendix B of this guide.

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

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.

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

3. Make sure the terminal emulation software is set as follows:

    - Select the appropriate serial port (COM port 1 or COM port 2).
    - Set the 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 3-58 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 3-10.

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 is assigned via DHCP by default. To manually configure this address, see "Setting an IP Address" on page 1-7.

Note: The 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 such as EliteView.

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

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 username 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 host 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 must 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 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 the 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>. In the screen below, the IP addresses given are merely examples.

```
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 seconds and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.

6. 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 such as SMC’s EliteView. 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 that 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** - with read-only access. Authorized management stations are only able to retrieve MIB objects.

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

Note: If you do not intend to use 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 EliteView rw
Console(config)#snmp-server community private
Console(config)#
```

Trap Receivers

You can also specify SNMP stations that are to receive trap messages 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 and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration 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 file system supports three types of system files that can be managed by the CLI program, Web Interface, or SNMP. The files can 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 the system default settings and cannot be deleted from the system.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operation and provides the CLI, Web and SNMP management interfaces.
- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test). This code also provides a facility to upload firmware files to the system directly through the console port.

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.

System Defaults

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

The following table lists some of the basic system defaults.

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"
	RADIUS Authentication	Disabled
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
	10/100 Mbps Port Capability	10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex Full-duplex flow control disabled
	10/100/1000 Mbps Port Capability	10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Symmetric flow control disabled
Link Aggregation	Static Trunks	none
	LACP (all ports)	Disabled
Spanning Tree Protocol	Status	Enabled (Defaults: All parameters based on IEEE 802.1D)
	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
	PVLAN	No Private VLAN

Function	Parameter	Default
Class of Service	Ingress Port Priority	0
	Weighted Round Robin	Class 0: 1 Class 1: 4 Class 2: 16 Class 3: 64
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
Multicast Filtering	IGMP Snooping	Enabled
	Act as Querier	Enabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
Rate Limit	Status	Disabled
VDSL	EFM Profile	Profile type: Private Downstream rate: 4.7 Mbps Upstream rate: 1.56 Mbps
	EFM User-profile	Profile type: Private Downstream rate: 4 Mbps Upstream rate: 1 Mbps
	EFM Shutdown	All ports enabled
	EFM RDSL	Disabled
	EFM Flow Control	Maximum transition rate available

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: The current firmware does not support stacking, so in all references to “units” and “ports”, the Unit ID will always be 1.

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 a user name and password using an out-of-band serial connection. Access to the Web agent is controlled by the same user name and password as the onboard configuration program. (See “Configuring the Login Password” on page 2-14.)

3. 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 "Managing Interface Settings" on page 2-41.)

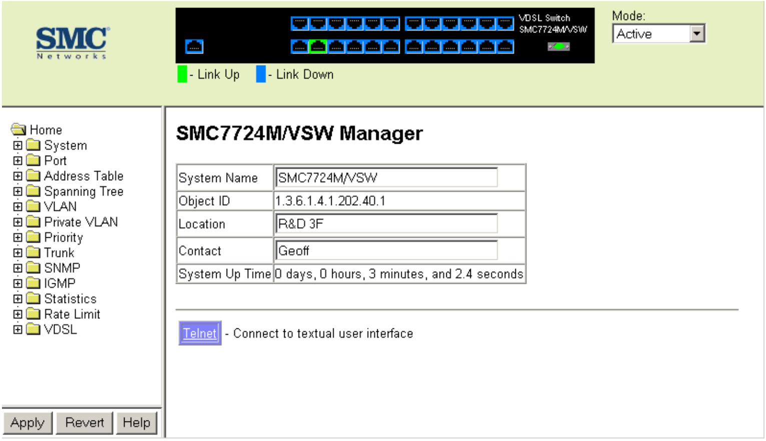
4. After you enter the user name and password, you will have access to the system configuration program.

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.



Mode: Active

SMC7724M/VSW Manager

System Name	SMC7724M/VSW
Object ID	1.3.6.1.4.1.202.40.1
Location	R&D 3F
Contact	Geoff
System Up Time	0 days, 0 hours, 3 minutes, and 2.4 seconds

Telnet - Connect to textual user interface

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" or "Apply Changes" button to confirm the new setting. The following table summarizes the Web page configuration buttons.

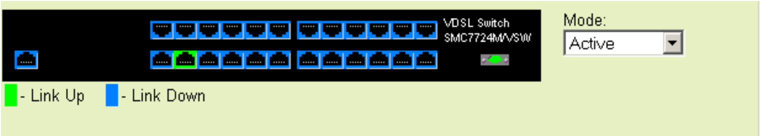
Button	**Action**
Apply	Sets specified values to the system for the displayed page.
Apply Changes	Sets specified values to the system for the specific parameter.
Revert	Cancels specified values and restores current values prior to pressing "Apply" or "Apply Changes."
Refresh	Immediately updates values for the current page.

Notes: **1.** To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools/Internet Options/General/Temporary Internet Files/Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

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

Panel Display

The Web agent displays an image of the switch's ports, indicating whether each link is up or down. Clicking on the image of a port opens the Port Configuration page as described on page 2-22.



Mode: Active

Main Menu

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

Menu	Description	Page
System		
System Information	Shows the number of ports, hardware/ firmware version numbers, and power status	2-9
IP	Sets the IP address for management access	2-11
Passwords	Assigns logon password	2-14
Radius	Configures RADIUS authentication parameters	2-15
Firmware	Manages code image files	2-17
Configuration	Manages switch configuration files	2-18
Reset	Reboots the switch	2-22
Bridge Extension	Shows the configuration for bridge extension commands; enables GVRP multicast protocol	2-22
Switch Information	Shows the number of ports, hardware/ firmware version numbers, and power status	2-24

Menu	**Description**	**Page**
Port		
Port Information	Displays port connection status	2-26
Trunk Information	Displays trunk connection status	2-26
Port Configuration	Configures port connection settings	2-28
Trunk Configuration	Configures trunk connection settings	2-28
Port Broadcast Control	Sets the broadcast storm threshold for each port	2-30
Monitor	Sets the source and target ports for mirroring	2-31
Port Security Configuration	Enables/disables port security	2-32
Address Table		
Dynamic Addresses	Displays or edits dynamic entries in the Address Table	2-33
Static Addresses	Displays or edits static entries in the Address Table	2-35
Address Aging	Sets timeout for dynamically learned entries	2-36
STA		
STA Information	Displays STA values used for the bridge	2-39
STA Configuration	Configures global bridge settings for STA	2-40
STA Port Configuration	Configures individual port settings for STA	2-41
STA Trunk Configuration	Configures individual trunk settings for STA	2-41
VLAN		
VLAN Base Information	Displays basic information on the VLAN type supported by this switch	2-49
VLAN Current Table	Shows the current port members of each VLAN and whether or not the port supports VLAN tagging	2-50
VLAN Static List	Used to create or remove VLAN groups	2-52
VLAN Static Table	Modifies the settings for an existing VLAN	2-53
VLAN Static Membership	Configures membership type for interfaces, including tagged, untagged or forbidden	2-55

Menu	Description	Page
VLAN Port Configuration	Specifies default PVID and VLAN attributes	2-56
VLAN Trunk Configuration	Specifies default trunk VID and VLAN attributes	2-56
Private VLAN		
Private VLAN Status	Enables or disables the Private VLAN feature	2-59
Private VLAN Link Configuration	Configures ports as downlink or uplink ports. Traffic from downlink ports can only be forwarded to, and from, the uplink ports	2-59
Priority		
Default Port Priority	Sets the default priority for each port	2-63
Default Trunk Priority	Sets the default priority for each trunk	2-63
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	2-65
Queue Scheduling	Configures Weighted Round Robin queueing	2-67
IP Precedence/DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both	2-70
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	2-70
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	2-73
IP Port Priority Status	Globally enables or disables IP Port Priority	2-75
IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value	2-75
Copy Settings	Copies port priority settings from source port to target port	2-77
Trunk		
LACP Configuration	Allows ports to dynamically join trunks	2-78
Trunk Configuration	Specifies ports to group into static trunks	2-78
SNMP	Configures community strings and related trap functions	2-81

Menu	Description	Page
IGMP		
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	2-84
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router/switch for each VLAN ID	2-87
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router/switch	2-88
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	2-88
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	2-91
Statistics	Lists Ethernet and RMON statistics	2-92
Rate Limit		
Rate Limit Status	Enables or disables the rate limit feature	2-95
Rate Limit Port Configuration	Sets the rate limit for each port	2-95
Rate Limit Trunk Configuration	Sets the rate limit for each trunk	2-95
VDSL		
VDSL Global Configuration	Batch assigns profiles for speed and distance range to all the VDSL ports on the switch	2-97
VDSL Port Configuration	For individual VDSL ports: Enables or disables the port Enables or disables Remote Digital Loopback (RDL) Limits the data rate flow from the switch to the CPE Assigns profiles for speed	2-99
VDSL Profile User Specified	Configures downstream rate, upstream rate and interleave depth for user-specified profiles	2-101

Menu	Description	Page
VDSL Port Link Status	Displays information on the link status of individual VDSL ports	2-103
VDSL Port Ethernet Statistics	Displays Ethernet statistics for individual switch VDSL ports and linked CPE Ethernet ports	2-106

Basic Configuration

Displaying System Information

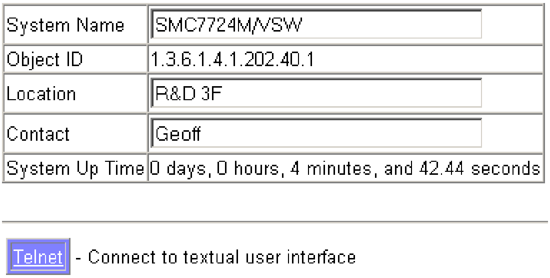
You can easily identify the system by providing a descriptive name, location, and contact information.

Fields and 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 Interface

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.)



System Name	SMC7724M/VSW
Object ID	1.3.6.1.4.1.202.40.1
Location	R&D 3F
Contact	Geoff
System Up Time	0 days, 0 hours, 4 minutes, and 42.44 seconds

Command Line Interface

Specify the hostname, location and contact information.

```
Console(config)#hostname SMC7724M/VSW                            3-27
Console(config)#snmp-server location R&D 3F                      3-46
Console(config)#snmp-server contact Geoff                        3-46
Console#show system                                              3-37
System description: SMC7724M/VSW Manager
System OID string: 1.3.6.1.4.1.259.6.13.1
System information
 System Up time: 0 days, 3 hours, 30 minutes, and 9.74 seconds
 System Name             : SMC7724M/VSW
 System Location         : R&D 3F
 System Contact          : Geoff
 MAC address             : 00-30-F1-4D-1E-80
 Web server              : enable
 Web server port         : 80
 POST result
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. If you wish to manually configure IP settings, you need to set the IP address and netmask to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

You may also need to a establish a default gateway between this device and management stations that exist on another network segment.

Fields and 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.

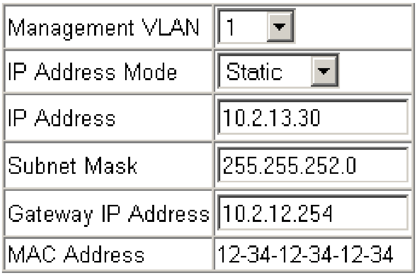
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.

- **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 Interface

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



Management VLAN	1
IP Address Mode	Static
IP Address	10.2.13.30
Subnet Mask	255.255.252.0
Gateway IP Address	10.2.12.254
MAC Address	12-34-12-34-12-34

Command Line Interface

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

```
Console#config
Console(config)#interface vlan 1                                    3-69
Console(config-if)#ip address 10.1.0.1 255.255.255.0                3-52
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254                       3-54
Console(config)#
```

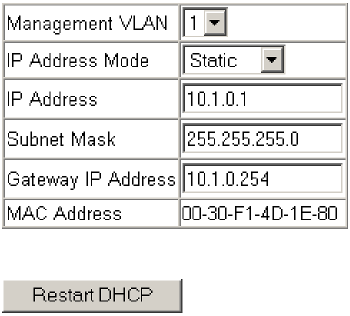
Using DHCP/BOOTP

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

Web Interface

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

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



Management VLAN	1
IP Address Mode	Static
IP Address	10.1.0.1
Subnet Mask	255.255.255.0
Gateway IP Address	10.1.0.254
MAC Address	00-30-F1-4D-1E-80

Command Line Interface

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

```
Console#config
Console(config)#interface vlan 1                                     3-69
Console(config-if)#ip address dhcp                                   3-52
Console(config-if)#end
Console#ip dhcp restart                                              3-53
Console#show ip interface                                            3-55
IP address and netmask: 10.1.0.1 255.255.255.0 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, reboot the switch or submit a client request to restart DHCP service.

Web Interface

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.

Command Line Interface

Enter the following command to restart DHCP service.

```
Console#ip dhcp restart                                          3-53
```

Security

Configuring the Login Password

The guest only has read access for most configuration parameters. However, the administrator has write access for parameters governing the onboard agent. You should therefore assign a password as soon as possible, and store it in a safe place.

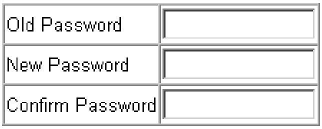
Notes: **1.** If you log into the Web interface as guest (Normal Exec level), you can view page information but only change the guest password. If you log in as admin (Privileged Exec level), you can apply changes on all pages.

2. If your password is lost, contact your local supplier for assistance.

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.

Web Interface

Click System/Passwords. Enter the old password, enter the new password, confirm it by entering it again, then click "Apply."



Old Password	
New Password	
Confirm Password	

Command Line Interface

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

```
Console(config)#username bob access-level 15                          3-28
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring Radius Logon Authentication

Remote Authentication Dial-in User Service (RADIUS) is a system that uses a central server running RADIUS software to control access to RADIUS-aware switches on the network. A RADIUS server can be used to create a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch using the console port, Telnet, or Web.

Fields and Attributes

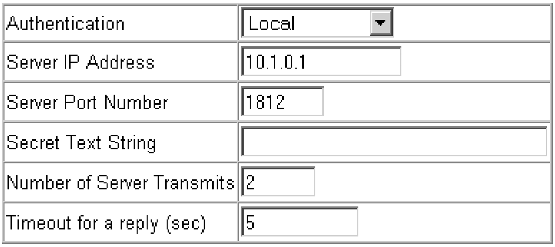
- **Authentication –** select the authentication type, or authentication sequence required.
- **Server IP Address –** the IP address of the RADIUS server.
- **Server Port Number –** the UDP port number used by the RADIUS server.
- **Secret Text String –** the text string that is shared between the switch and the RADIUS server.

- **Number of Server Transmits –** the number of request transmits to the RADIUS server before failure.

- **Timeout for a reply –** the number of seconds the switch waits for a reply from the RADIUS server before it resends the request.

Web Interface

Click System/Radius.



Authentication	Local
Server IP Address	10.1.0.1
Server Port Number	1812
Secret Text String	
Number of Server Transmits	2
Timeout for a reply (sec)	5

Command Line Interface

Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius                         3-39
Console(config)#radius-server host 192.168.1.25                     3-40
Console(config)#radius-server port 181                              3-41
Console(config)#radius-server key green                             3-41
Console(config)#radius-server retransmit 5                          3-42
Console(config)#radius-server timeout 10                            3-42
Console#show radius-server                                          3-43
Server IP address: 192.168.1.25
 Communication key with radius server:
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Console(config)#
```

Managing Firmware

You can upload/download firmware to/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 Usage

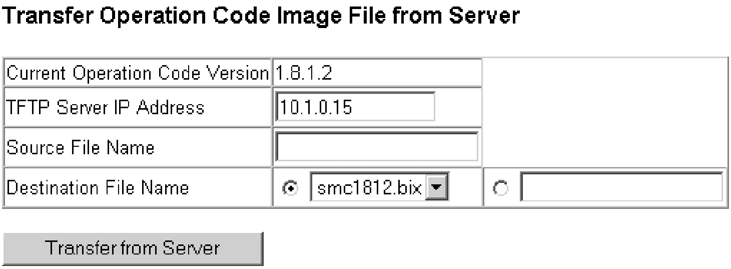
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the length of the file name should be 1 to 31 characters. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- The maximum number of runtime files is 2.

Downloading System Software from a Server

When downloading runtime code, specify the same Destination File Name as the current file to replace the current code file, 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 Interface

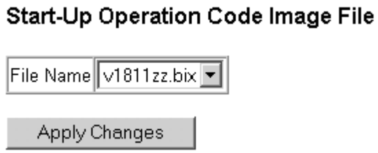
Click System/Firmware. Enter the IP address of the TFTP server, enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click “Transfer from Server.”



Transfer Operation Code Image File from Server

Current Operation Code Version	1.8.1.2	
TFTP Server IP Address	10.1.0.15	
Source File Name		
Destination File Name	● smc1812.bix ▾	○

If you download to a new destination file, select the new file from the “Start-Up Operation Code Image File” drop-down box, and click “Apply Changes.”



Start-Up Operation Code Image File

File Name v1811zz.bix

To start the new firmware, reboot the system.

Command Line Interface

Enter the IP address of the TFTP server. Select the config or opcode file type. Enter the source and destination file names. Set the new file to boot the system.

```
Console#copy tftp file                                              3-19
TFTP server ip address: 10.1.0.15
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: vdsl(v1.8.1.1ZZ.bix
Destination file name: v1811zz.bix
/
Console#config
Console(config)#boot system opcode: v1811zz.bix                     3-25
Console(config)#exit
Console#reload                                                      3-16
```

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 Usage

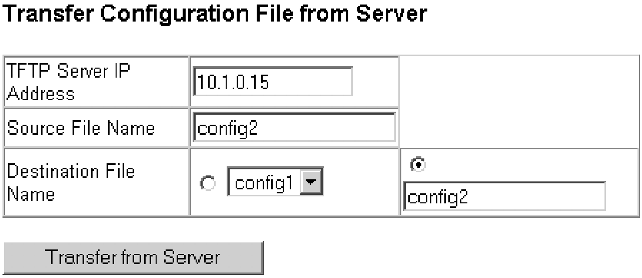
- The destination configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the length of file name should be 1 to 31. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

- The maximum number of user-defined configuration files is 2.

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 "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web Interface

Click System/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 click "Transfer from Server."



Transfer Configuration File from Server

TFTP Server IP Address	10.1.0.15	
Source File Name	config2	
Destination File Name	○ config1 ▾	● config2

Command Line Interface

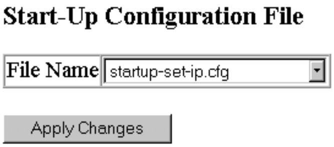
Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                        3-19
TFTP server ip address: 10.1.0.15
Source configuration file name: config2
Startup configuration file name [startup] : config2
/
Console#
```

Setting the Startup Configuration File

Web Interface

If you download to a new file name, select the new file from the drop-down box and click "Apply Changes."



Start-Up Configuration File

File Name: startup-set-ip.cfg

To use the new settings, reboot the system.

Command Line Interface

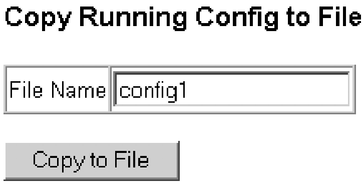
Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                         3-19
TFTP server ip address: 10.1.0.15
Source configuration file name: config2
Startup configuration file name [startup] : config2
/
Console#
Console#config
Console(config)#boot system config: config2                              3-25
Console(config)#exit
Console#reload
```

Copying the Running Configuration to a File

Web Interface

You can save the running configuration to a file. Just enter the file name and click “Copy to File.”



Copy Running Config to File

File Name: config1

Command Line Interface

If you copy the running configuration to a file, you can set this file as the startup file at a later time.

```
Console#copy running-config file                                    3-19
destination file name : 051902.cfg
/
Console#
Console#config
Console(config)#boot system config: 051902.cfg                      3-25
Console(config)#exit
Console#reload                                                      3-16
```

Reset

Web Interface

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

Command Line Interface

Use the reload command to reboot the system.

Example

```
Console#reload                                                      3-16
System will be restarted, continue <y/n>? y
Console#
```

Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. To display these extensions, use the Extended Bridge Configuration screen as shown below

Fields and 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 “This example sets the STP attributes for port 5.” on page 2-44.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to “Setting Static Addresses” on page 2-35.)
- **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 2-45.”)

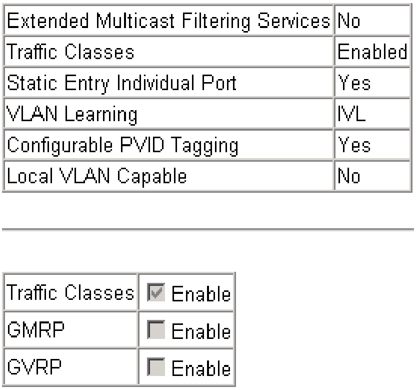
- **Local VLAN Capable** – This switch does not support multiple local bridges (i.e., multiple Spanning Trees.)

- **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 VLANs groups which extend beyond the local switch.

Web Interface

Click System/Bridge Extension.



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

Command Line Interface

Enter the following command.

```
Console#show bridge-ext                                            3-113
 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 Switch Hardware/Software Versions

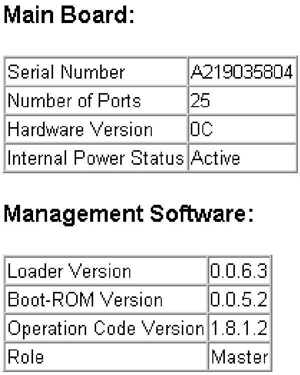
Fields and Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of ports on this switch.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status –** Displays the status of the internal power supply.
- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version number of boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is Master (i.e., operating stand-alone.)

Web Interface

Click System/Switch Information.



Main Board:

Serial Number	A219035804
Number of Ports	25
Hardware Version	0C
Internal Power Status	Active

Management Software:

Loader Version	0.0.6.3
Boot-ROM Version	0.0.5.2
Operation Code Version	1.8.1.2
Role	Master

Command Line Interface

Use the following command to display version information.

```
Console#show version                                                    3-38
Unit1
 Serial number           :A219035804
 Service tag             :
 Hardware version        :0C
 Module A type           :other
 Module B type           :other
 Number of ports         :25
 Main power status       :up
 Redundant power status  :not present
Agent(master)
 Unit id                 :1
 Loader version          :0.0.6.3
 Boot rom version        :0.0.5.2
 Operation code version  :1.8.1.1
Console#
```

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.

Fields and Attributes

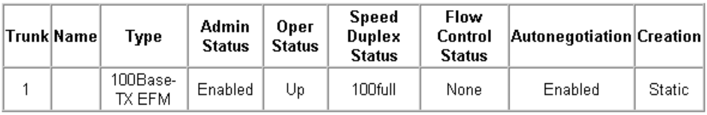
- **Name** – Interface label.
- **Type** – Indicates the port type (100Base-TX EFM, 100Base-TX NORMAL, 100Base-FX NORMAL, 1000Base-T NORMAL, or 1000Base-GBIC NORMAL.)

Note: "NORMAL" indicates that this is an Ethernet port.

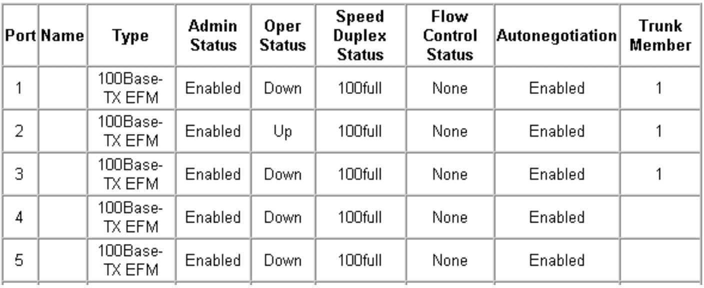
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed/Duplex Status** – Shows the current speed and duplex mode.
- **Flow Control Status** – Indicates the type of flow control currently in use.
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Trunk Member** – Shows if a port is a trunk member. (Port Information only.)
- **Creation** – Shows if a trunk is manually configured. (Trunk Information only.)

Web Interface

Click Port/Port Information or Trunk Information. Modify the required interface settings and click "Apply."



Trunk	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Creation
1		100Base-TX EFM	Enabled	Up	100full	None	Enabled	Static



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

Command Line Interface

This example shows the connection status for Port 13.

```
Console#show interfaces status ethernet 1/13                    3-69
Information of Eth 1/13
 Basic information:
  Port type: 100TX-EFM
  Mac address: 00-30-f1-4d-1e-8c
 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

Use the Port Configuration and Trunk Configuration pages to enable/disable an interface, manually set the speed and duplex mode, set flow control, and set auto-negotiation parameters.

Fields and Attributes

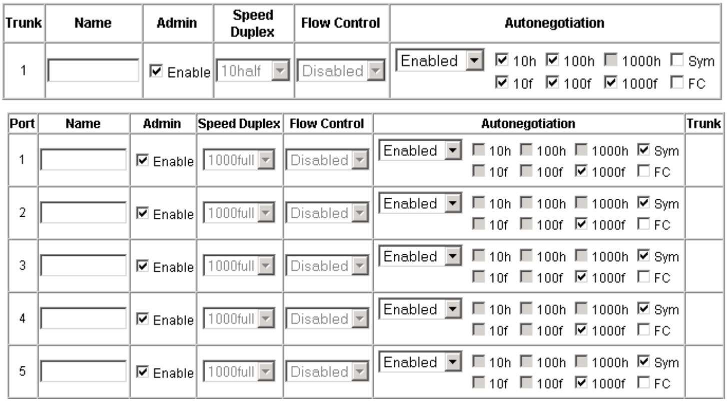
- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface 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.
  - 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.
  - Flow control should not be used if a port is connected to a hub. Otherwise flow control signals will be propagated throughout the segment.
- **Autonegotiation/Port Capabilities** – Allows auto-negotiation to be enabled/disabled. Specifies the capabilities to be advertised for a port during auto-negotiation. The following capabilities are supported:
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation

- **Sym** - Transmits and receives pause frames for flow control.
- **FC** - Supports flow control.
- **Trunk** – Indicates if a port is a member of a trunk. Creates trunks and selects port members (see “Port Trunk Configuration” on page 2-78.)

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

Web Interface

Click Port/Trunk Configuration or Port Configuration. Modify the required interface settings, and click “Apply.”



Trunk	Name	Admin	Speed Duplex	Flow Control	Autonegotiation
1		☑ Enable	10half	Disabled	Enabled ☑ 10h ☑ 100h □ 1000h □ Sym ☑ 10f ☑ 100f ☑ 1000f □ FC

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

Command Line Interface

Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13                             3-69
Console(config-if)#description RD SW#13                             3-69
Console(config-if)#shutdown                                         3-74
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                   3-71
Console(config-if)#speed-duplex 100half                             3-70
Console(config-if)#flowcontrol                                      3-73
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                             3-72
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
```

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 a complete halt.

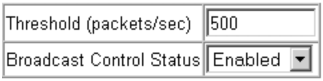
You can protect your network from broadcast storms by setting a threshold for broadcast traffic for all ports. Any broadcast packets exceeding the specified threshold will then be dropped.

Fields and Attributes

- Broadcast Storm Control default is 500 packets per second.
- Broadcast control does not affect IP multicast traffic.

Web Interface

Click Port/Port Broadcast Control. Set the threshold for all ports (Range: 500 to 262,143 packets per second), and then click “Apply.”



Threshold (packets/sec)	500
Broadcast Control Status	Enabled

Command Line Interface

Specify an interface, and then enter the threshold. This threshold will then be set for all ports. The following sets broadcast suppression at 1000 packets per second. Use the **no switchport broadcast** command to disable broadcast storm control.

```
Console(config)#interface ethernet 1/1                              3-69
Console(config-if)#switchport broadcast packet-rate 1000            3-75
Console(config-if)#
```

Configuring Port Mirroring

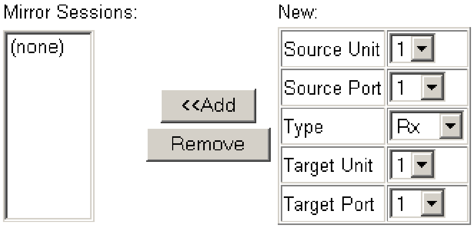
You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Command Usage

- The mirror port and monitor port speeds must match, otherwise traffic may be dropped from the monitor port.
- All mirror sessions must share the same destination port.

Web Interface

Click Port/Mirror. Specify the source port, the traffic type to be mirrored, and the monitor port. Click “Add.”



Mirror Sessions: (none)

New:

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

Command Line Interface

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                              3-69
Console(config-if)#port monitor ethernet 1/13                        3-138
Console(config-if)#
```

Configuring Port Security

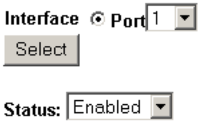
Use the Port Security Configuration page to enable port security on a per-port basis.

Command Usage

- When port security is enabled, the selected port will stop learning MAC addresses. This prevents unauthorized access to the switch. The MAC addresses already in the address table will be retained and will not age out.
- A secure port has the following restrictions:
    - Cannot use port monitoring
    - Cannot be a multi-VLAN interface
    - Cannot be connected to a network interconnection device
    - Cannot be a trunk port

Web Interface

Click Port/Port Security Configuration.



Interface ● Port 1

Status: Enabled

Command Line Interface

Specify the required interface, then enter “Port Security.” To disable this feature enter “No Port Security.”

```
Console(config)#interface ethernet 1/1                             3-69
Console(config-if)#port security                                   3-84
Console(config-if)#
```

Address Table Settings

The switch stores the addresses of known devices. This information is used to route traffic directly between the inbound and outbound ports. The addresses learned by monitoring traffic are stored in the dynamic address table. You may also manually configure static addresses that are bound to a specific port.

Displaying the Address Table

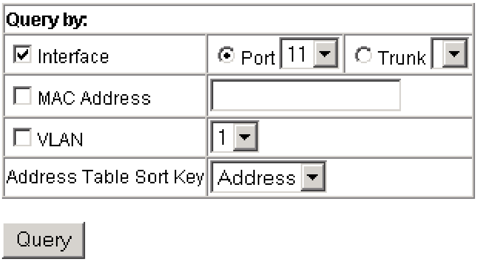
The Dynamic Address Table contains the MAC addresses learned by monitoring the source address of traffic entering the switch. When the destination address for inbound traffic is found in the database, packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic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

Command Usage

- Display entries in the dynamic address table by selecting an interface (either port or trunk), MAC address, or VLAN.
- Sort the information displayed based on interface (port or trunk), MAC address, or VLAN.

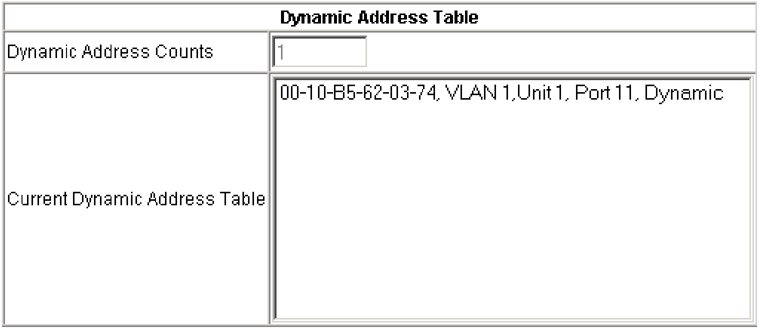
Web Interface

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



Query by:		
☑ Interface	● Port 11	○ Trunk
□ MAC Address		
□ VLAN	1	
Address Table Sort Key	Address	

For example, the following screen shows the dynamic addresses for port 11.



Dynamic Address Table	
Dynamic Address Counts	1
Current Dynamic Address Table	00-10-B5-62-03-74, VLAN 1,Unit 1, Port 11, Dynamic

Command Line Interface

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

```
Console#show bridge 1 ethernet 1/11                                   3-81
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/11 00-10-b5-62-03-74    1 Learned
Console#
```

Setting Static Addresses

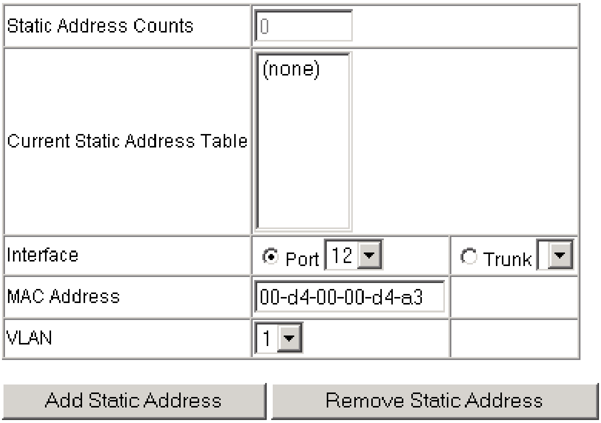
A static address can be assigned to a specific interface on this switch. Traffic sent from devices listed in the static address table will only be accepted on the specified interface. If any packets with a source address listed in this table enter another interface, they will be dropped.

Command Usage

Entries specified via the Web Interface are permanent. Entries specified via the CLI can be made permanent or can be set to be deleted on reset.

Web Interface

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



Static Address Counts	0	
Current Static Address Table	(none)	
Interface	● Port 12	○ Trunk
MAC Address	00-d4-00-00-d4-a3	
VLAN	1	

Command Line Interface

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

```
Console(config)#bridge 1 address 00-e0-29-94-34-de vlan 1 forward ethernet
1/1 delete-on-reset                                                   3-79
Console(config)#
```

Changing the Aging Time

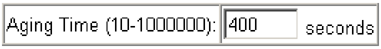
You can set the aging time for entries in the dynamic address table.

Command Usage

The range for aging time: 10 - 1000000 seconds. (The default is 300 seconds.)

Web Interface

Click Address Table/Address Aging. Specify the new aging time, then click "Apply."



Aging Time (10-1000000): 400 seconds

Command Line Interface

This example also sets the aging time to 400 seconds.

```
Console(config)#bridge-group 1 aging-time 400                   3-82
Console(config)#
```

Spanning Tree Protocol Configuration

The Spanning Tree Algorithm (STA) detects and disable network loops and provides backup links between switches, bridges, and routers to ensure that only one route exists between any two stations on the network. The backup links automatically take over when a primary link goes down.

Managing Global Settings

Global setting apply to the entire switch.

Fields and Attributes

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

- **Bridge ID** – The priority and MAC address of this device.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
- **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – The time since the Spanning Tree was last reconfigured.
- **Hold Time** – The minimum interval between the transmission of consecutive Configuration BPDUs. (CLI only.)

The following global attributes can be configured:

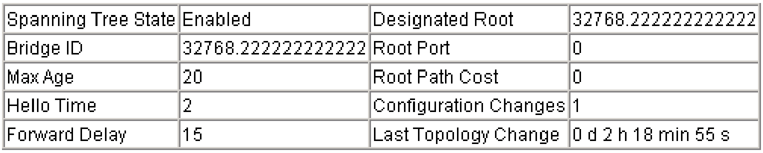
- **Spanning Tree State** – Enable/disable this switch to participate in an STA-compliant network.

- **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 - 65535
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section means "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) the root device will wait before changing states (i.e., listening 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.
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

Displaying the current global settings for STA

Web Interface

Click Spanning Tree/STA Information.



Spanning Tree State	Enabled	Designated Root	32768.222222222222
Bridge ID	32768.222222222222	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	1
Forward Delay	15	Last Topology Change	0 d 2 h 18 min 55 s

Command Line Interface

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

```
Console#show bridge group 1
3-81
Bridge-group information
------------------------------------------------------------
 Spanning tree protocol             :ieee8021d
 Spanning tree enable/disable       :enable
 Priority                           :32768
 Hello Time (sec.)                  :2
 Max Age (sec.)                     :20
 Forward Delay (sec.)               :15
 Designated Root                    :32768.0000e8a00090
 Curent root port                   :0
 Curent root cost                   :0
 Number of topology changes         :1
 Last topology changes time (sec.):9736
 Hold times (sec.)                  :1
```

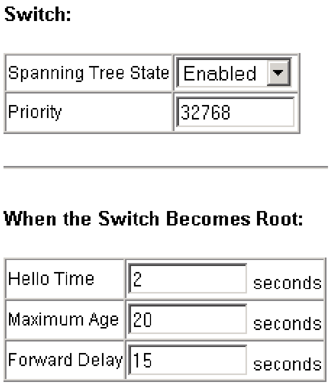
```
Eth  1/1 information
---------------------------------------------------------------
 Admin status           : enable
 STA state              : forwarding
 Path cost              : 18
 Priority               : 128
 Designated cost        : 0
 Designated port        : 128.1
 Designated root        : 32768.0030f14d1e80
 Designated bridge      : 32768.0030f14d1e80
 Fast forwarding        : disable
 Forward transitions    : 2
```

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

Configuring the global settings for STA

Web Interface

Click STA/STA Configuration. Modify the required attributes then click "Apply."



Switch:

Spanning Tree State	Enabled
Priority	32768

When the Switch Becomes Root:

Hello Time	2 seconds
Maximum Age	20 seconds
Forward Delay	15 seconds

Command Line Interface

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

```
Console(config)#bridge 1 spanning-tree                                      3-86
Console(config)#bridge 1 priority 40000                                     3-90
Console(config)#bridge 1 hello-time 5                                       3-88
Console(config)#bridge 1 max-age 40                                         3-89
Console(config)#bridge 1 forward-time 20                                    3-87
```

Managing Interface Settings

You can configure STA attributes for specific interfaces, including port priority, path cost, and fast forwarding. Use a different priority or path cost for ports of the same media type to indicate the preferred path.

Fields and Attributes

- **STA State** – Displays the current state of this port within the Spanning Tree:
  - **Disabled** - No link has been established on this port. Otherwise, the port has been disabled by the user or has failed diagnostics.
  - **Blocking** - Port receives STA configuration messages, but does not forward packets.
  - **Listening** - Port will leave blocking state due to a topology change, start transmitting configuration messages, but will not yet 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.
  - **Broken** - Port is malfunctioning or no link has been established.
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops.

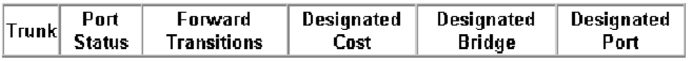
  Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

  - Default: 128
  - Range: 0 - 255

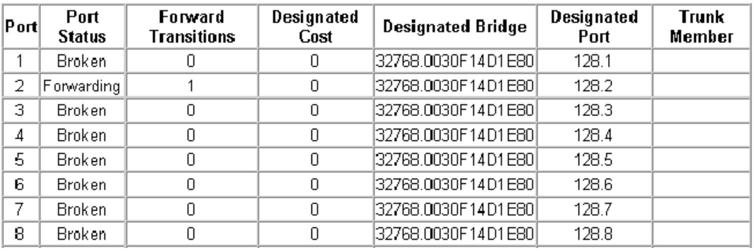
- **Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
    - Range:
        - Ethernet: 50-600
        - Fast Ethernet: 10-60
        - Gigabit Ethernet: 3-10
    - Default:
        - Ethernet - half duplex: 100; full duplex: 95; trunk: 90
        - Fast Ethernet - half duplex: 19; full duplex: 18; trunk: 15
        - Gigabit Ethernet - full duplex: 4; trunk: 3
- **Fast Forward** – Since end-nodes cannot cause forwarding loops, they can pass directly through to the forwarding state. Fast Forward can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that Fast Forward should only be enabled for ports connected to an end-node device.)

Web Interface

Click STA/STA Trunk Information or STA Port Information.



Trunk	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port



Port	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Trunk Member
1	Broken	0	0	32768.0030F14D1E80	128.1	
2	Forwarding	1	0	32768.0030F14D1E80	128.2	
3	Broken	0	0	32768.0030F14D1E80	128.3	
4	Broken	0	0	32768.0030F14D1E80	128.4	
5	Broken	0	0	32768.0030F14D1E80	128.5	
6	Broken	0	0	32768.0030F14D1E80	128.6	
7	Broken	0	0	32768.0030F14D1E80	128.7	
8	Broken	0	0	32768.0030F14D1E80	128.8	

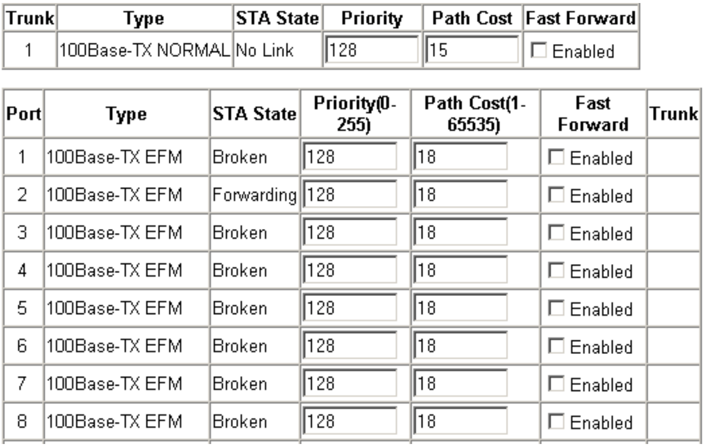
Command Line Interface

This example shows the STA attributes for port 5.

```
Console#show bridge group 1 ethernet 1/5                                3-94
Bridge-group information
--------------------------------------------------------------
 Spanning tree protocol           :IEEE Std 802.1D
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Hello Time (sec.)                :2
 Max Age (sec.)                   :20
 Forward Delay (sec.)             :15
 Designated Root                  :32768.0030F14D1E80
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :1
 Last topology changes time (sec.):8094
 Hold times (sec.)                :1
---------------------------------------------------------------
Eth  1/ 5 information
--------------------------------------------------------------
 Admin status          : enable
 STA state             : broken
 Path cost             : 18
 Priority              : 128
 Designated cost       : 0
 Designated port       : 128.5
 Designated root       : 32768.0030F14D1E80
 Designated bridge     : 32768.0030F14D1E80
 Fast forwarding       : disable
 Forward transitions   : 0
Console#
```

Web Interface

Click STA/STA Port Configuration or STA Trunk Configuration. Modify the required attributes, then click “Apply.”



Trunk	Type	STA State	Priority	Path Cost	Fast Forward
1	100Base-TX NORMAL	No Link	128	15	☐ Enabled

Port	Type	STA State	Priority(0-255)	Path Cost(1-65535)	Fast Forward	Trunk
1	100Base-TX EFM	Broken	128	18	☐ Enabled	
2	100Base-TX EFM	Forwarding	128	18	☐ Enabled	
3	100Base-TX EFM	Broken	128	18	☐ Enabled	
4	100Base-TX EFM	Broken	128	18	☐ Enabled	
5	100Base-TX EFM	Broken	128	18	☐ Enabled	
6	100Base-TX EFM	Broken	128	18	☐ Enabled	
7	100Base-TX EFM	Broken	128	18	☐ Enabled	
8	100Base-TX EFM	Broken	128	18	☐ Enabled	

Command Line Interface

This example sets the STP attributes for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 priority 0                         3-92
Console(config-if)#bridge-group 1 path-cost 50                       3-91
Console(config-if)#bridge-group 1 portfast                           3-93
Console(config-if)#
```

VLAN Configuration

In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBeui. By using IEEE 802.1Q-compliant VLANs, you can organize any group of network nodes into separate broadcast domains, thus confining broadcast traffic to the originating group. 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.

- 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
- 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 (that is, a port attached to a VLAN-aware device) if you want it to carry traffic for one or more VLANs and if the device at the other end of the link also supports VLANs. Then assign the port at the other end of the link to the same VLAN(s.) However, if you want a port on this switch to participate in one or more VLANs, but the device at the other end of the link does not support VLANs, then you must add this port as an untagged port (that is, a port attached to a VLAN-unaware device.)

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 PVID of the receiving port. 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 using a Layer-3 router or switch.

Port-based VLANs – Port-based (or static) VLANs are manually tied to specific ports. The switch's forwarding decision is based on the destination MAC address and its associated port. Therefore, to make valid forwarding or flooding decisions, the switch must learn the relationship of the MAC address to its related port—and thus to the VLAN—at run-time. However, when GVRP is enabled, this process can be fully automatic.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each endstation should be assigned. If an endstation (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 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, you must first configure the static VLANs required on switches that are connected to PCs, servers, and other devices, so that these VLANs can be propagated across the network (Web - VLAN/VLAN Static Membership.) For other core switches in the network, enable GVRP on the links between these devices.
(Web - VLAN/Port Configuration or Trunk Configuration.)

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 need to create a VLAN for that group and enable tagging on all ports.

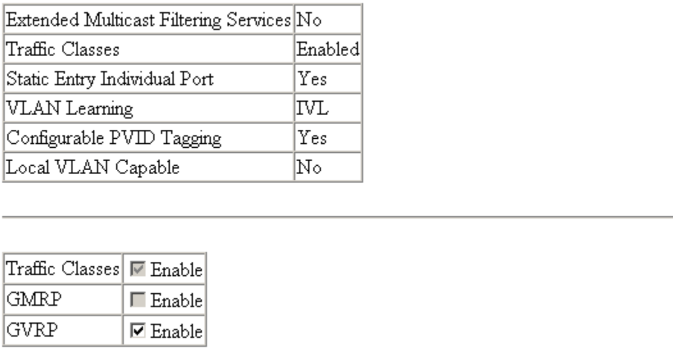
Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. To forward a frame from a VLAN-aware device to a VLAN-unaware device, the switch first decides where to forward the frame, and then strips off the VLAN tag. However, to forward a frame from a VLAN-unaware device to a VLAN-aware device, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting this 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: Enabled.)

Web Interface

Click System, Bridge Extension. Enable or disable GVRP. Click “Apply.”



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

Command Line Interface

This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp                                    3-107
Console(config)#
```

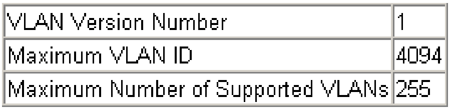
Displaying Basic VLAN Information

Fields and Attributes

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

Web Interface

Click VLAN/VLAN Base Information.



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

Command Line Interface

Enter the following command.

```
Console#show bridge-ext                                                    3-113
 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

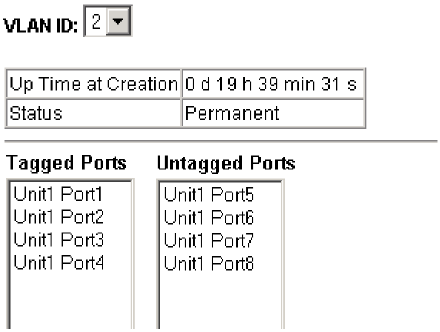
The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can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

Web Interface

Fields and Attributes

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes.)
- **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.
- **Tagged Ports** – Shows the tagged VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

Click VLAN/VLAN Current Table. Select a VLAN ID from the scroll-down list.



VLAN ID: 2

Up Time at Creation	0 d 19 h 39 min 31 s
Status	Permanent

Tagged Ports	Untagged Ports
Unit1 Port1 Unit1 Port2 Unit1 Port3 Unit1 Port4	Unit1 Port5 Unit1 Port6 Unit1 Port7 Unit1 Port8

Command Line Interface

Fields and Attributes

- **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.

Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                              3-104
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
Console#
```

Creating VLANs

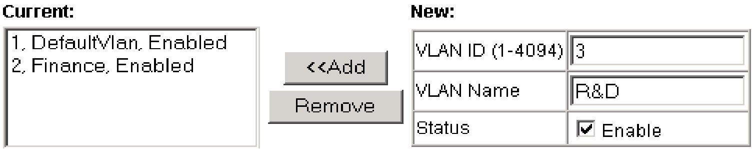
Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Fields and Attributes

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes.)
- **VLAN Name** – Name of the VLAN (1 to 32 characters.)
- **Status** – Shows if this VLAN is enabled or disabled (Web.)
  - **Enable** - VLAN is operational.
  - **Disable** - VLAN is suspended; i.e., does not pass packets.
- **State** – Shows if this VLAN is enabled or disabled (CLI.)
  - **Active** - VLAN is operational.
  - **Suspend** - VLAN is suspended; i.e., does not pass packets.

Web Interface

Click VLAN/VLAN Static List. Enter the VLAN ID and VLAN name, check the Enable box to activate the VLAN, and then click "Add."



Current:

1. DefaultVlan, Enabled
2. Finance, Enabled

New:

VLAN ID (1-4094)	3
VLAN Name	R&D
Status	☑ Enable

Command Line Interface

This example creates a new VLAN.

```
Console(config)#vlan database                                    3-95
Console(config-vlan)#vlan 5 name R&D media ethernet state active   3-97
Console(config-vlan)#
```

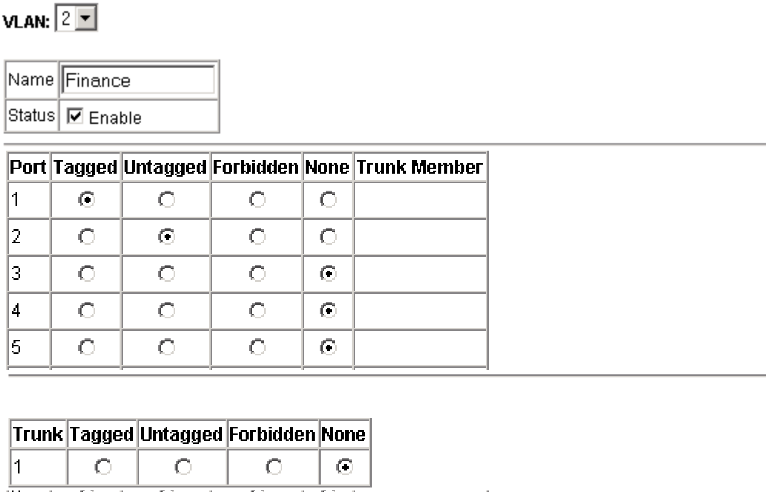
Adding Interfaces Based on Membership Type

Fields and Attributes

- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes.)
- **Name** – Name of the VLAN (1 to 32 characters.)
- **Status** – Shows if this VLAN is enabled or disabled.
  - **Enable** - VLAN is operational.
  - **Disable** - VLAN is suspended; i.e., does not pass packets.
- **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 “GVRP and Bridge Extension Commands” on page 3-108.
  - **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 Interface

Click VLAN/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: 2

Name	Finance
Status	☑ Enable

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

Trunk	Tagged	Untagged	Forbidden	None
1	○	○	○	●

Command Line Interface

This example adds the required interfaces, and then displays the VLAN members.

```
Console(config)#interface ethernet 1/1                               3-69
Console(config-if)#switchport allowed vlan add 2 tagged              3-102
Console(config-if)#exit
Console(config)#interface ethernet 1/2                               3-69
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13                              3-69
Console(config-if)#switchport allowed vlan add 2 tagged
```

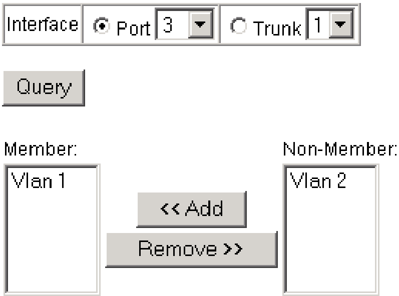
Adding Interfaces Based on Static Membership

Fields and 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 Interface

Click VLAN/VLAN Static Membership. Select an interface from the scroll-down box (Port or Trunk.) Click "Query" to display VLAN 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."



Interface ● Port 3 ○ Trunk 1

Member: Vlan 1

Non-Member: Vlan 2

Command Line Interface

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                           3-69
Console(config-if)#switchport allowed vlan add 1 tagged          3-102
Console(config-if)#switchport allowed vlan remove 2
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including 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.

Fields and Attributes

- **PVID** – The VLAN ID assigned to untagged frames received on the interface. If the (CLI) switchport mode is set to **trunk** (see page 3-99), the PVID will be inserted into all untagged frames sent from a tagged port. (Default: 1.)
- **Acceptable Frame Type** – Sets the interface to accept all frame types or only tagged frames. If only tagged frames are accepted, the switch will only accept frames if the frame tag matches a VLAN to which this interface has been assigned. (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. This will not affect VLAN independent BPDU frames, such as GVRP or STP. (Default: Disabled.)

- **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 2-22) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Enabled.)

- **GARP Join Timer** – The interval between transmitting requests/ queries to participate in a VLAN group. (Default: 20 centiseconds) (Range: 20-1000 centiseconds; Default: 20 centiseconds)
  - Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer.

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

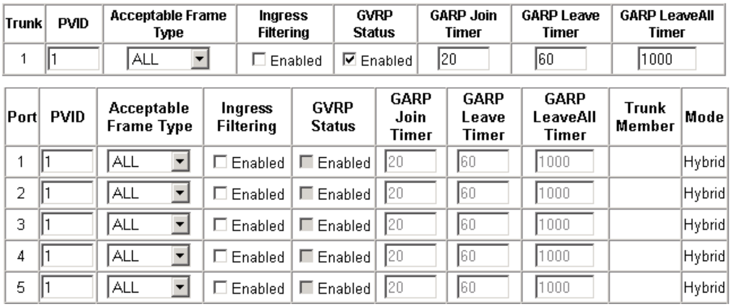
- **GARP LeaveAll Timer** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000 centiseconds.)
  - 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 a port. (Configure via CLI, see page 3-99.)
  - **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 and receives tagged frames that identify the source VLAN.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may receive or transmit tagged or untagged frames. Any frames that are not tagged will be assigned to the default VLAN.

Web Interface

Click VLAN/VLAN Trunk Configuration or VLAN Port Configuration. Fill in the required settings for each interface, click “Apply.”



Trunk	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer	GARP Leave Timer	GARP LeaveAll Timer
1	1	ALL	☐ Enabled	☑ Enabled	20	60	1000

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer	GARP Leave Timer	GARP LeaveAll Timer	Trunk Member	Mode
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

Command Line Interface

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                                3-69
Console(config-if)#switchport acceptable-frame-types tagged          3-100
Console(config-if)#switchport ingress-filtering                      3-100
Console(config-if)#switchport native vlan 3                          3-101
Console(config-if)#switchport gvrp                                   3-108
Console(config-if)#garp timer join 10                                3-110
Console(config-if)#garp timer leave 90                               3-110
Console(config-if)#garp timer leaveall 2000                          3-110
Console(config-if)#switchport mode hybrid                            3-99
Console(config-if)#
```

Configuring Private VLANs

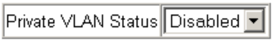
A Private VLAN allows modification of the default VLAN to provide port-based security and isolation between ports within the VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. Private VLANs and normal VLANs can exist simultaneously within the same switch. Both individual ports and port trunks can be configured as downlink or uplink interfaces.

Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function.

Web Interface

Click Private VLAN/Private VLAN Status, then select Enabled/Disabled to enable or disable the Private VLAN function.



Private VLAN Status: Disabled

Command Line Interface

This example enables private VLANs.

```
Console(config)#pvlan                                                  3-105
Console(config)#
```

Configuring Uplink and Downlink Ports

Use the Private VLAN Status and Private VLAN Status Link pages to enable/disable the Private VLAN function and to configure port groups as downlink or uplink ports.

When one port in a group is configured as a downlink or uplink port, all other ports in that group are also configured as downlink or uplink ports. The Web and Command Line Interface however, will only display the explicitly configured port as a downlink or uplink port.

Downlink ports and uplink ports can only be configured in certain groups.

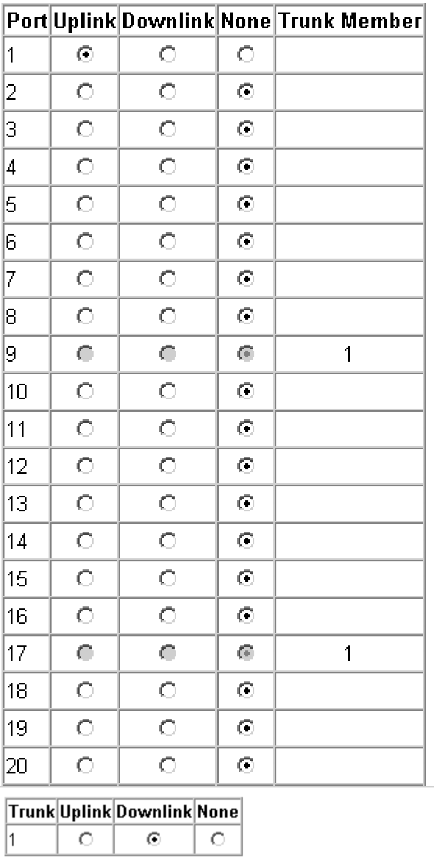
```
<<1-8>> <<9-16>> <<17-24>> <<25>> <<26>>
```

For example, on the Web screen shown on the following page, only trunk 1 displays as a downlink interface. However, since ports 9 and 17 are members of trunk 1, ports 9-24 would all be configured as downlink ports.

Fields and Attributes

- **Private VLAN Status** – Enables/disables the Private VLAN function.
- **Uplink** – Configures the port as an uplink port.
- **Downlink** – Configures the port as a downlink port.
- **None** – If selected, the port does not belong to the private VLAN.

Click Private VLAN/ Private VLAN Link Configuration, then select Uplink or Downlink to configure the ports as uplink or downlink ports.



Port	Uplink	Downlink	None	Trunk Member
1	●	○	○	
2	○	○	●	
3	○	○	●	
4	○	○	●	
5	○	○	●	
6	○	○	●	
7	○	○	●	
8	○	○	●	
9	○	○	●	1
10	○	○	●	
11	○	○	●	
12	○	○	●	
13	○	○	●	
14	○	○	●	
15	○	○	●	
16	○	○	●	
17	○	○	●	1
18	○	○	●	
19	○	○	●	
20	○	○	●	

Trunk	Uplink	Downlink	None
1	○	●	○

Command Line Interface

This example shows trunk 1 being configured as a downlink interface. However, since ports 9 and 17 are members of trunk 1, ports 9-24 would all become downlink ports.

```
Console(config)#pvlan                                         3-105
Console(config)#pvlan up-link ethernet 1/25 down-link port-channel 1
Console(config)#end
Console#show pvlan                                            3-107
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/1
Down-link port:
 Trunk 1
Console#
```

In this example ports 9 and 17 are shown being configured as downlink ports. Ports 10-16 and 18-24 will also become downlink ports as ports 9 and 17 are members of trunk 1.

```
Console(config)#pvlan up-link ethernet 1/25 down-link
ethernet 1/9,17                                              3-107
Console(config)#
```

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 priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues.

You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Setting the Default Priority for Interfaces

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

Command Usage

- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.

- The default priority applies if the incoming frame is an untagged frame received from a VLAN trunk or a static-access port. 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.

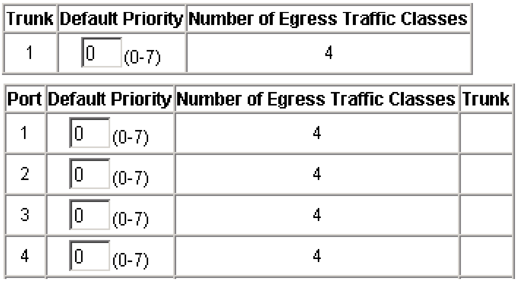
Fields and Attributes

- **Default Priority** – The priority that is assigned to untagged frames received on the specified port. (Range: 0 - 7, Default: 0.)

- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

Web Interface

Click Priority/Trunk Priority or Port Priority. Modify the default priority for any interface, then click “Apply.”



Trunk	Default Priority	Number of Egress Traffic Classes
1	0 (0-7)	4

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

Command Line Interface

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

```
Console(config)#interface ethernet 1/3                                3-69
Console(config-if)#switchport priority default 5                     3-125
```

Mapping Priority Classes to Egress Queues

This switch supports Class of Service by using four priority queues, with Weighted Round Robin Queuing for each port. Eight traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

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

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.

Note that the mapping of CoS priorities to switch output queues for any single port then applies to all ports on the switch.

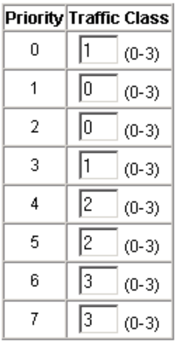
Priority Level	Traffic Type
0 (default)	Best Effort
1	Background
2	(Spare)
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Fields and Attributes

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

Web Interface

Click Priority/Traffic Class. Assign CoS priorities to the switch's four traffic class queues then click "Apply."



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

Command Line Interface

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

```
Console(config)#interface ethernet 1/1                             3-69
Console(config)#queue cos-map 0 1 2                                3-127
Console(config)#queue cos-map 1 0 3
Console(config)#queue cos-map 2 4 5
Console(config)#queue cos-map 3 6 7
Console(config)#exit
Console#show queue cos-map ethernet 1/1                            3-129
Information of Eth 1/1
 Queue ID Class of service
 -------- -------------
    0     1 2
    1     0 3
    2     4 5
    3     6 7
Console#
```

Queue Scheduling

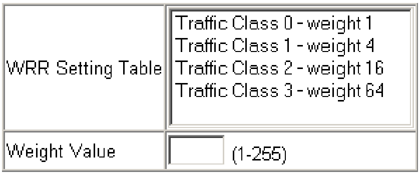
In the **Queue Scheduling** page, you can configure Weighted Round Robin (WRR) queueing for the switch. Note that setting weight values for traffic classes for any single port then applies to all the ports on the switch.

Fields and attributes

- **WRR Setting Table** – displays a list of weight values for each switch class of service queue (traffic class.)
- **Weight Value** – Sets a new weight value for a traffic class.

Web Interface

Click Priority/Queue Scheduling.



WRR Setting Table	Traffic Class 0 - weight 1 Traffic Class 1 - weight 4 Traffic Class 2 - weight 16 Traffic Class 3 - weight 64
Weight Value	(1-255)

Note: To change a table setting, select the entry in the WRR Setting Table and type the new weight in the Weight Value box, then click "Apply." To reset the fields to their current value, click "Refresh."

Command Line Interface

The following example shows how to assign weights of 10, 20, 30, and 40 to the CoS priority queues 1, 2, 3 and 4. To reset to default use the **no** form of the command.

```
Console(config)#queue bandwidth 10 20 30 40                    3-126
Console(config)#end
Console#show queue bandwidth                                   3-129
 Queue ID  Weight
 --------  ------
    0        10
    1        20
    2        30
    3        40
Console(config)#no queue bandwidth                             3-126
Console(config)#end
Console#show queue bandwidth
 Queue ID  Weight
 --------  ------
    0        1
    1        4
    2        16
    3        64
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.

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. Bits 6 and 7 are used for network control, and the other bits for various application types. The 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

Fields and Attributes

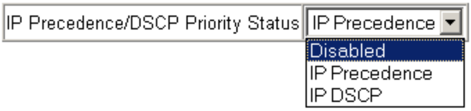
- **IP Precedence/DSCP Priority Status** – Selects IP Precedence, DSCP, or disables both priority services.

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.

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

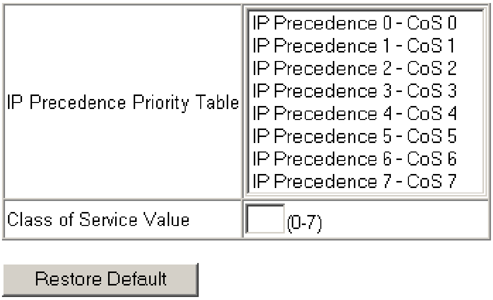
Web Interface

Click Priority/IP Precedence/DSCP Priority Status, and select IP Precedence.



IP Precedence/DSCP Priority Status	IP Precedence

Click IP Precedence Priority from the Priority menu. Select an IP Precedence value from the IP Precedence Priority Table by clicking on it with your cursor, enter a value in the Class of Service Value field, and then click "Apply." Note that the mapping of IP Precedence values to CoS values for any single port then applies to all ports on the switch.



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)

Command Line Interface

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

```
Console(config)#map ip precedence                                  3-131
Console(config)#interface ethernet 1/5                             3-69
Console(config-if)#map ip precedence 1 cos 0                       3-132
Console(config-if)#end
Console#show map ip precedence ethernet 1/5                        3-136
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 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 DSCP values that are not specified are mapped to CoS value 0.

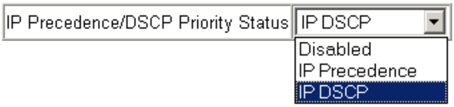
IP DSCP Value	**CoS Value**
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Fields and Attributes

- **IP Precedence/DSCP Priority Status** – Selects IP Precedence, DSCP, or disables both priority services.
- **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” represents high priority.

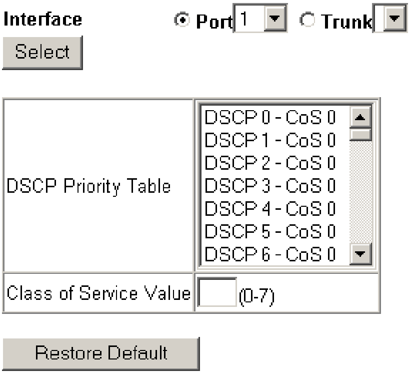
Web Interface

Click Priority/IP Precedence/DSCP Priority Status, and select IP DSCP.



IP Precedence/DSCP Priority Status: IP DSCP

Click IP DSCP Priority from the Priority menu. Select a DSCP priority value from the DSCP Priority Table by clicking on it with your cursor, enter a value in the Class of Service Value field, and then click "Apply."



Interface ● Port 1 ○ Trunk

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)

Command Line Interface

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 for that port.

```
Console(config)#map ip dscp                                             3-133
Console(config)#interface ethernet 1/5                                  3-69
Console(config-if)#map ip dscp 1 cos 0                                  3-134
Console(config-if)#end
Console#show map ip dscp ethernet 1/5                                   3-137
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 IP Port Priority

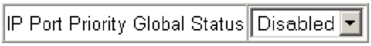
In the IP Port Priority page, for each switch port or trunk, you can map IP ports (TCP/UDP ports) to the switch's 4 traffic class queues.

Fields and Attributes

- **Current IP Port Table** – displays a list of IP ports with their mapped class of service queues.
- **IP Port** – sets a new IP port number.
- **Class of Service** – sets a new class of service for an IP port. Note that "0" represents low priority and "3" represents high priority.

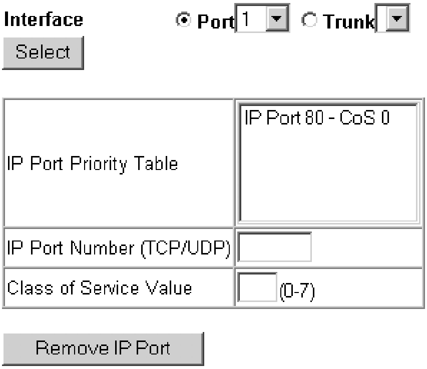
Web Interface

Click Priority/IP Priority Status and then select Enabled.



IP Port Priority Global Status: Disabled

Click IP Port Priority from the Priority menu. Select the port or trunk. To add an IP port, type the port number in the IP Port box and the new CoS value in the Class of Service box, then click “Apply.” To delete an IP port setting, select the entry in the Current IP Port Table, then click “Remove IP Port.”



Interface: ● Port 1 ○ Trunk

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

Command Line Interface

The following example shows IP Port 80 mapped to CoS value 0 for ethernet port 1.

```
Console(config)#map ip port                                   3-130
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0                       3-131
Console(config-if)#end
Console# show map ip port ethernet 1/5                        3-135
TCP port mapping status: enabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       23   0
  Eth 1/ 5       80   0
  Eth 1/ 5     1020   6
Console#
```

Copy Priority Settings

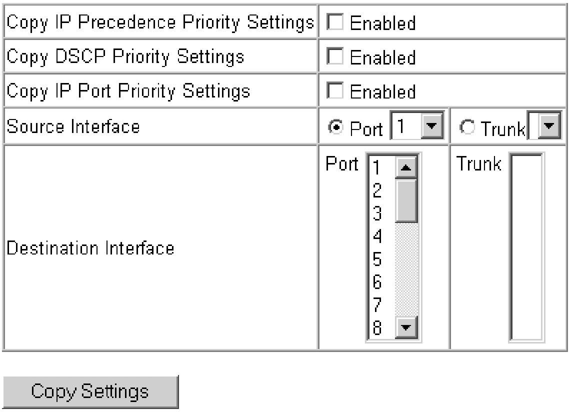
Use the Copy Settings page to copy priority settings from a one port or trunk to another port or trunk.

Fields and Attributes

- **Source Interface** – The port or trunk from which the priority settings are copied.
- **Destination Interface** – The port or trunk to which the priority settings are copied.

Web Interface

Click Priority/Copy Settings. Check the type of priority settings to be copied, select the source interface and destination interface, then click "Copy Settings."



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

Copy Settings

Port Trunk Configuration

Ports can be combined into an aggregate link to increase the bandwidth of a network connection where bottlenecks exist, or to ensure fault recovery. You can configure trunks between any two switches of the same type. You can create up to six trunks at a time. The uplink ports can be trunked together and the VDSL ports can be trunked together, the details are given in the table below.

Switch	Ports	Port Type	Number of Trunks	Ports per Trunk	Maximum Aggregate Bandwidth
SMC7724M/ VSW	1 - 24	VDSL	1 - 6	2 - 24	720 Mbps
	25, 26	1000BASE-T	1	2	4 Gbps

The switch supports both static trunking and dynamic LACP (Link Aggregation Control Protocol.) LACP configured ports will automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of the ports on the switch as LACP, as long as they are not already configured as part of another 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

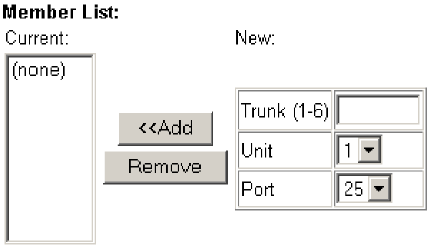
- Finish configuring a port trunk before you connect the corresponding network cables between switches.
- You can configure one trunk group, containing up to four ports as a dynamic LACP trunk.

- The ports on both ends of a trunk must be configured the same for speed, duplex mode, and flow control.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated.
- 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.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

A trunk formed with another switch using LACP will automatically be assigned the next available port-channel id.

Web Interface

Click Trunk/Trunk Configuration or LACP Configuration. LACP configured ports will automatically negotiate a trunked link with LACP-configured ports on another device. Enter "1" in the Trunk field, select ports from the scroll-down port list, and click "Add." After you have completed adding ports to the member list, click "Apply."



Member List:

Current: (none)

New:

Trunk (1-6)	
Unit	1
Port	25

Command Line Interface

This example creates trunk 1 with ports 25 and 26. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 1                           3-69
Console(config-if)#exit
Console(config)#interface ethernet 1/25                            3-69
Console(config-if)#channel-group 1                                 3-142
Console(config-if)#exit
Console(config)#interface ethernet 1/26
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1                      3-76
Information of Trunk 1
 Basic information:
  Mac address: 22-22-22-22-22-2c
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 1000full,
  Flow control status: Disabled
 Current status:
  Created by: User
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/25, Eth1/26,
Console#
```

The following shows LACP enabled on ports 1 and 2. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 2** command shows that Trunk 2 has been established.

```
Console(config)#interface ethernet 1/1                             3-69
Console(config-if)#lacp                                            3-144
Console(config-if)#exit
Console(config)#interface ethernet 1/2                             3-69
Console(config-if)#lacp                                            3-144
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 2                      3-76
Information of Trunk 2
 Basic information:
  Port type: 100TX-EFM
  Mac address: 00-30-F1-4D-1E-8B
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control: Disabled
 Current status:
  Created by: lacp
  Link status: Down
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12,
Console#
```

Configuring SNMP

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 AccView. 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

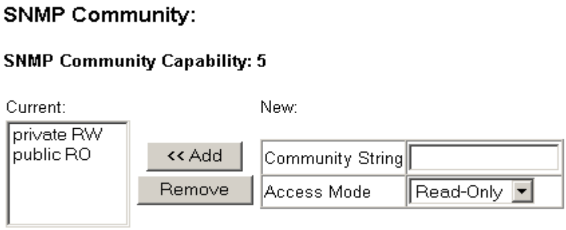
You may configure up to five community strings authorized for management access. For security reasons, you should consider removing the default strings.

Fields and Attributes

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

Click SNMP. Enter a new string in the Community String box and select the access rights from the Access Mode drop-down list, then click “Add.”



SNMP Community:

SNMP Community Capability: 5

Current:
private RW
public RO

New:

Community String	
Access Mode	Read-Only

Command Line Interface

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

```
Console(config)#snmp-server community spiderman rw                3-45
Console(config)#
```

Specifying Trap Managers

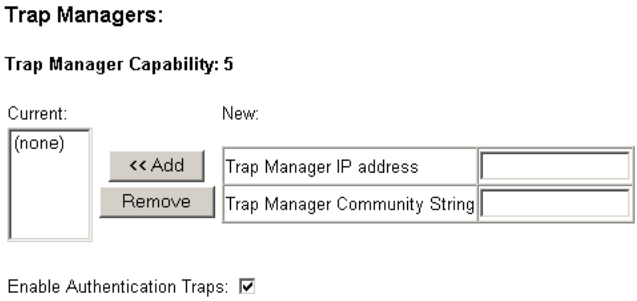
You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

- Enable or disable authentication messages via the Web Interface.
- Enable or disable authentication messages, link-up-down messages, or all notification types via the CLI.

Web Interface

Click SNMP/Traps. Fill in the Trap Manager IP Address box and the Trap Manager Community String box, check Enable Authentication Traps if required, and then click “Add.”



Trap Managers:

Trap Manager Capability: 5

Current: (none)

Enable Authentication Traps: ☑

Command Line Interface

This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 batman                3-47
Console(config)#snmp-server enable traps authentication           3-48
```

Multicast Configuration

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

Fields and Attributes

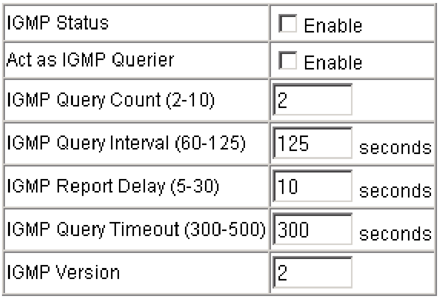
- **IGMP Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Disabled.)
- **Act as IGMP Querier** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled.)
- **IGMP Query Count** – Sets the maximum number of queries issued for which there has been no response before the switch takes action to solicit reports. (Default: 2, Range: 2 - 10.)
- **IGMP Query Interval** – Sets the frequency (in seconds) at which the switch sends IGMP host-query messages. (Default: 125, Range: 60 - 125.)

- **IGMP Report Delay –** Sets the time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Default: 10 seconds, Range: 5 - 30.)
- **Query Timeout –** Sets the time (in seconds) the switch waits after the previous querier has stopped querying before it takes over as the querier. (Default: 300 seconds, Range: 300 - 500.)
- **IGMP Version –** Sets the protocol version for compatibility with other devices on the network. (Default: 2, Range: 1 - 2.)

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

Web Interface

Click IGMP/IGMP Configuration. Adjust the IGMP settings as required, and then click “Apply.” (The default settings are shown below.)



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	2

Command Line Interface

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

```
Console(config)#ip igmp snooping                                  3-115
Console(config)#ip igmp snooping querier                          3-118
Console(config)#ip igmp snooping query-count 10                   3-119
Console(config)#ip igmp snooping query-interval 100               3-119
Console(config)#ip igmp snooping query-max-response-time 20       3-120
Console(config)#ip igmp snooping query-time-out 300               3-121
Console(config)#ip igmp snooping version 2                        3-116
Console(config)#exit
Console#show ip igmp snooping                                     3-117
 Igmp Snooping Configuration
 ----------------------------------------------
 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 use the information obtained from IGMP Query, 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.

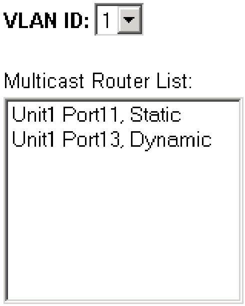
Displaying Interfaces Attached to a Multicast Router

Fields and 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 Interface

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



VLAN ID: 1

Multicast Router List:

Unit1 Port11, Static
Unit1 Port13, Dynamic

Command Line Interface

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                     3-123
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
```

Specifying Interfaces Attached to a Multicast Router

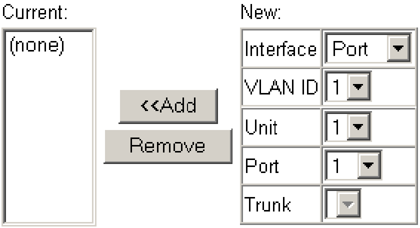
Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the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

Fields and 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 Interface

Click IGMP/Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN that will forward the corresponding multicast traffic, and then click "Apply."


Current:
(none)

New:

Interface	Port
VLAN ID	1
Unit	1
Port	1
Trunk	

Command Line Interface

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

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11      3-122
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                       3-123
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11  Static
```

Displaying Port Members of Multicast Services

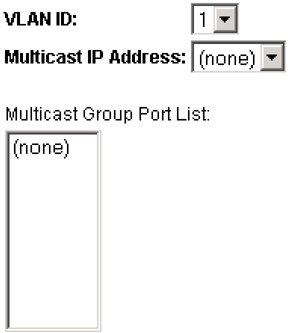
You can display the port members associated with a specified VLAN and multicast IP address.

Fields and Attributes

- **VLAN ID** – Selects the VLAN from 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 Interface

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.



VLAN ID: 1

Multicast IP Address: (none)

Multicast Group Port List:

(none)

Command Line Interface

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

```
Console#show bridge 1 multicast vlan 1                                  3-117
 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 “Port Trunk Configuration” on page 2-78. For 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

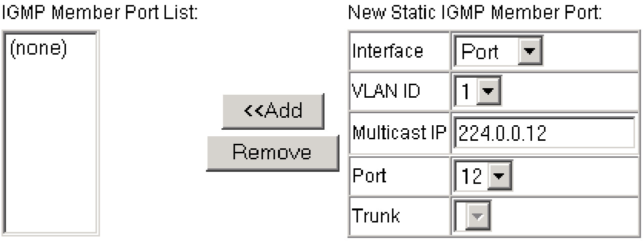
- Static multicast addresses are never aged out.
- When a multicast address is assigned to a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Fields and 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 Interface

Click IGMP/GMP 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 “Apply.”



(none)

Interface	Port
VLAN ID	1
Multicast IP	224.0.0.12
Port	12
Trunk	

Command Line Interface

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

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet 1/12                                                      3-115
Console(config)#exit
Console#show bridge 1 multicast vlan 1                             3-117
 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#
```

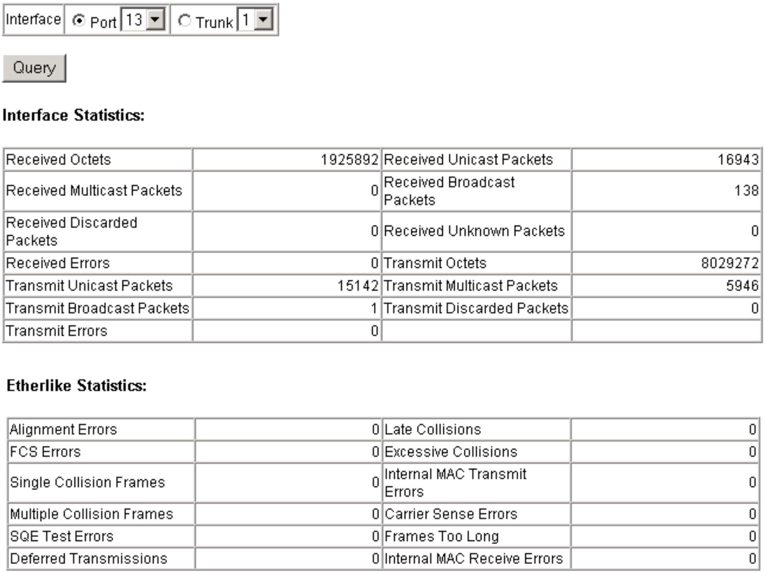
Showing Device Statistics

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.

Web Interface

Click 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.



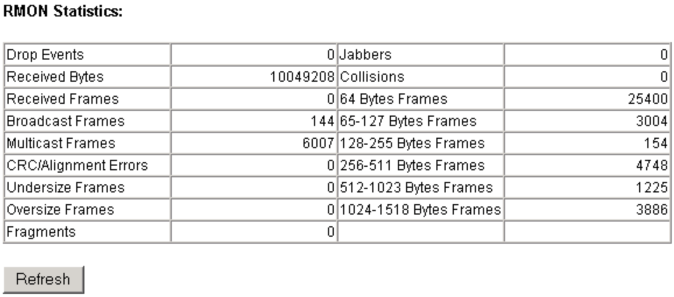
Interface ● Port 13 ○ Trunk 1

Interface Statistics:

Received Octets	1925892	Received Unicast Packets	16943
Received Multicast Packets	0	Received Broadcast Packets	138
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	8029272
Transmit Unicast Packets	15142	Transmit Multicast Packets	5946
Transmit Broadcast Packets	1	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	10049208	Collisions	0
Received Frames	0	64 Bytes Frames	25400
Broadcast Frames	144	65-127 Bytes Frames	3004
Multicast Frames	6007	128-255 Bytes Frames	154
CRC/Alignment Errors	0	256-511 Bytes Frames	4748
Undersize Frames	0	512-1023 Bytes Frames	1225
Oversize Frames	0	1024-1518 Bytes Frames	3886
Fragments	0		

Command Line Interface

This example shows statistics for port 13.

```
Console#show interfaces counters ethernet 1/13                      3-77
Ethernet 1/13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

Rate Limit Configuration

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.

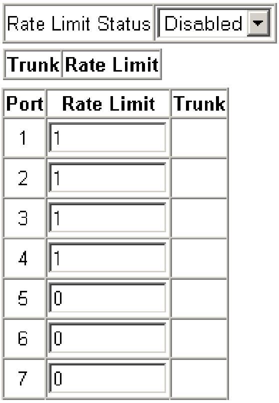
Rate limiting can be applied to individual ports. When a port is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Fields and Attributes

- The *rate* range is:
  - Fast Ethernet interface – 1 to 100 Mbps.
  - Gigabit Ethernet interface – 1 to 1000 Mbps.
- Resolution – the unit increment of *rate* change:
  - Fast Ethernet interface – 1 Mbps.
  - Gigabit Ethernet interface – 8 Mbps
- The maximum data rate for VDSL ports depends on the physical link and the selected EFM profile (see page 3-147.)

Web Interface

Click Rate Limit/Rate Limit Status to enable/disable this feature globally. Then click Rate Limit Port Configuration or Rate Limit Trunk Configuration to configure the rate limit for individual ports or trunks.



Rate Limit Status	Disabled

Trunk Rate Limit

Port	Rate Limit	Trunk
1	1	
2	1	
3	1	
4	1	
5	0	
6	0	
7	0	

Command Line Interface

Use the **rate-limit input** command in Global configuration mode to turn on rate limit. Use the **no** form of this command to disable it.

```
Console#config
Console(config)#rate-limit input                                    3-163
Console(config)#
```

Use the **rate limit input** command in Interface Configuration mode to configure the rate limit on data received on a specific port. Use the **no** form of this command to return to default. In the example below, port 1 is configured to have a rate limit of 10 Mbps.

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 10                              3-164
Console(config-if)#
```

VDSL Configuration

You can configure and display communication parameters for VDSL and Ethernet ports on the switch and connected CPEs.

Note: The term EFM used in this section stands for Ethernet in the First Mile. The "first mile" is the connection between business and residential users and the public network. The VDSL Intelligent Switch uses VDSL-based technology for this connection.

VDSL Global Configuration

Assigns the same profile to each VDSL switch port. Details of these profiles are given in the table below.

Profile Name	ProfileType	Downstream Rate (Mbps)	Upstream Rate (Mbps)
default	Private	4.17	1.56
efm-5	Private	6.25	6.25
efm-10	Private	12.50	12.50
efm-15	Private	16.67	18.75
public-ansi	Public	16.67	4.67
public-etsi	Public	12.50	4.67
efm-5 LL	Private	6.25	6.25
efm-10 LL	Private	12.50	12.50
efm-15 LL	Private	16.67	18.75
public-ansiLL	Public	16.67	4.67
public-etsiLL	Public	12.50	4.67
efm-15-3LL	Private	16.67	3.13
efm-15-2LL	Private	16.67	2.08
efm-15-1LL	Private	16.67	1.56
efm-10-2 LL	Private	12.50	2.08
user-1	Private	4.00	1.00
user-2	Private	4.00	1.00

Notes: **1.** The actual data rates may be less than those shown in the table depending on the protocols/applications used.

2. If the "LL" type profile is selected, the error rate due to noise in transmission, is increased, but the signal latency is reduced.

3. The "Public" profiles conform to specific standards such as ANSI or ETSI. The "Private" profiles do not conform to these standards.

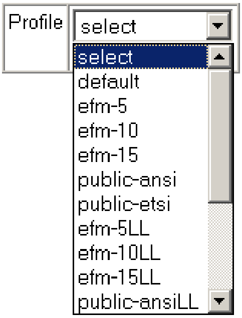
4. Profiles "user-1" and "user-2" are user-configured profiles. The values shown for the downstream and upstream rates are the default values. These rates may be configured to values between 1 Mbps and 15 Mbps. (See "Configuring a User-specified EFM Profile" on page 2-101.)

Fields and Attributes

- **Profile Name –** The name for the specific set of communication parameters.
- **Profile Type –** "Public" profiles are those that meet specific standards e.g., ETSI or ANSI. "Private" profiles do not meet these standards. The ports on a VDSL switch can be assigned the same or different private profiles. If a public profile is configured on the switch and you want the switch VDSL ports to use private profiles, you must first disable the public profile by using the **no efm profile global** configuration command.
- **Downstream Rate –** Rate of data transmission from the switch to the CPE.
- **Upstream Rate –** Rate of data transmission from the CPE to the switch.

Web Interface

Click VDSL/VDSL Global Configuration.



Command Line Interface

This example shows configuring the switch to public-ansi profile.

```
Console#config
Console(config)#efm profile global public-ansi                    3-147
Console(config)#
```

VDSL Port Configuration

You can enable/disable a selected port, enable/disable Remote Digital Loopback (RDL), set the value for EFM flow control (the maximum speed of transmission of data from a specific switch VDSL port to the CPE), and configure an EFM profile for the selected port.

Command Usage

Use this command to disable the VDSL chipset transmitter of a VDSL port that is not connected to a working CPE. In some unusual circumstances, the power emitted by VDSL ports can affect other VDSL ports. It is recommended that ports that are not wired to CPEs be shutdown in this way.

Also use this command to disable access to the switch from this port.

Fields and Attributes

- **Active Status** – Check this box to enable the selected port.
- **RDL** – Check this box to enable Remote Digital Loopback (RDL.) RDL tests the link between the switch and the CPE by sending out, and returning data through the CPE, over the VDSL link (see "efm-rdl" on page 3-152.) (Default: Disabled.)
- **Flow Control** – This is EFM flow control and determines the maximum speed of transmission of data from a specific switch VDSL port to the CPE.
  (Range 0 - 128 Mbps, default 100 Mbps.)

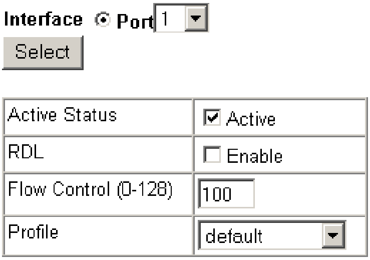
Notes: **1.** If set to 0, this feature is disabled.

2. Since the maximum transmission speed of VDSL ports is lower than 100 Mbps, when this feature is set to default, the actual maximum transmission rate is determined by the EFM profile and the physical link.

- **Profile -** Configures an EFM profile for the selected port.

Web Interface

Click VDSL/VDSL Port Configuration.



Interface ● **Port** 1 ▾

Select

Active Status	☑ Active
RDL	□ Enable
Flow Control (0-128)	100
Profile	default ▾

Command Line Interface

The following examples show how these features are configured in the CLI.

This example disables VDSL port 1.

```
Console (config)#interface ethernet 1/1                        3-69
Console(config-if)#efm shutdown
3-151
Console(config-if)#
```

The following example shows how to enable/disable RDL on VDSL port 1.

```
Console (config)#interface ethernet 1/1                       3-69
Console(config-if)#efm rdl                                    3-152
Console(config-if)#no efm rdl
Console(config-if)#
```

The following example shows VDSL port 1 configured to a maximum transmission rate of 1 Mbps.

```
onsole#config
Console(config)#interface ethernet 1/1                        3-69
Console(config-if)#efm flow-control 1                         3-153
Console(config-if)#
```

The following example shows EFM profile efm-10 assigned to VDSL port 1.

```
Console#config
Console(config)#efm profile global public-ansi                3-147
Console(config)#interface ethernet 1/1                        3-69
Console(config-if)#efm profile efm-10                         3-149
Console(config-if)#
```

Configuring a User-specified EFM Profile

Use this command to set user specified downstream rate, upstream rate and interleave depth.

Fields and Attributes

- **Profile –** The name of the user-specified profile. This can be “user-1” or “user-2.”

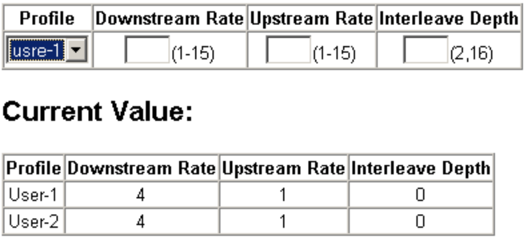
- **Downstream Rate –** The rate at which data is transmitted from the switch to the CPE.

- **Upstream Rate –** The rate at which data is transmitted from the CPE to the switch.

- **Interleave Depth –** The interleave depth is a parameter that determines the degree of protection of the data signal against impulse noise provided by interleaving. The default value is 0. This means that the interleaver is disabled. The values of the interleave depth that can be set by the user are 0, 1, 2, 8, and 16; 16 specifies maximum protection.

Web Interface

Click VDSL/VDSL Profile User Specified.



Profile	Downstream Rate	Upstream Rate	Interleave Depth
usre-1 ▾	□ (1-15)	□ (1-15)	□ (2,16)

Current Value:

Profile	Downstream Rate	Upstream Rate	Interleave Depth
User-1	4	1	0
User-2	4	1	0

Command Line Interface

The following example shows user-profile 1 configured to a downstream rate of 15 Mbps, an upstream rate of 5 Mbps, and an interleave depth of 2.

```
Console(config)#efm define user-profile 1 15 5 2                3-150
Console(config)#
```

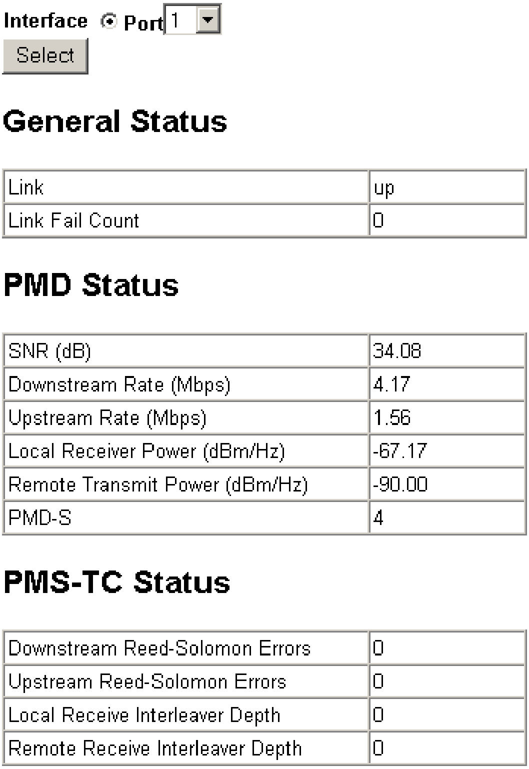
VDSL Port Link Status

Fields and Attributes

- **Link –** Shows the status of the VDSL link.
- **Link Fail Count –** The number of times the switch has tried to re-establish the link with the CPE since the link went down.
- **SNR** (dB) **–** The signal-to-noise ratio of the switch.
- **Downstream Rate (Mbps) –** The rate at which data is transmitted from the switch to the CPE.
- **Upstream Rate (Mbps) –** The rate at which data is transmitted from the CPE to the switch.
- **Local Receiver Power** (dBm/Hz) **–** The power at which the signal from the CPE port is received on the switch VDSL port.
- **Remote Transmit Power** (dBm/Hz) – The power at which the signal is transmitted from the CPE port to the switch.
- **PMD-S –** Physical Media Dependent Flag for the VDSL chip.
- **Downstream Reed-Solomon Errors –** The number of errors in the downstream data that have been corrected by the Reed-Solomon code.
- **Upstream Reed-Solomon Errors –** The number of errors in the upstream data that have been corrected by the Reed-Solomon code.
- **Local/Remote Receive Interleave Depth –** The interleave depth is a parameter that determines the degree of protection of the data signal against impulse noise provided by interleaving. The values of the interleave depth that can be set by the user are 0, 1, 2, 8, and 16; 16 specifies maximum protection. Local Receive Interleave Depth refers to protection provided on the signal received at on the VDSL switch port. Remote Receive Interleave Depth refers to protection provided on the signal received on the CPE port.

Web Interface

Click VDSL/VDSL Port Link Status.



General Status

Link	up
Link Fail Count	0

PMD Status

SNR (dB)	34.08
Downstream Rate (Mbps)	4.17
Upstream Rate (Mbps)	1.56
Local Receiver Power (dBm/Hz)	-67.17
Remote Transmit Power (dBm/Hz)	-90.00
PMD-S	4

PMS-TC Status

Downstream Reed-Solomon Errors	0
Upstream Reed-Solomon Errors	0
Local Receive Interleaver Depth	0
Remote Receive Interleaver Depth	0

Command Line Interface

The following example displays VDSL link current values on VDSL switch port 2.

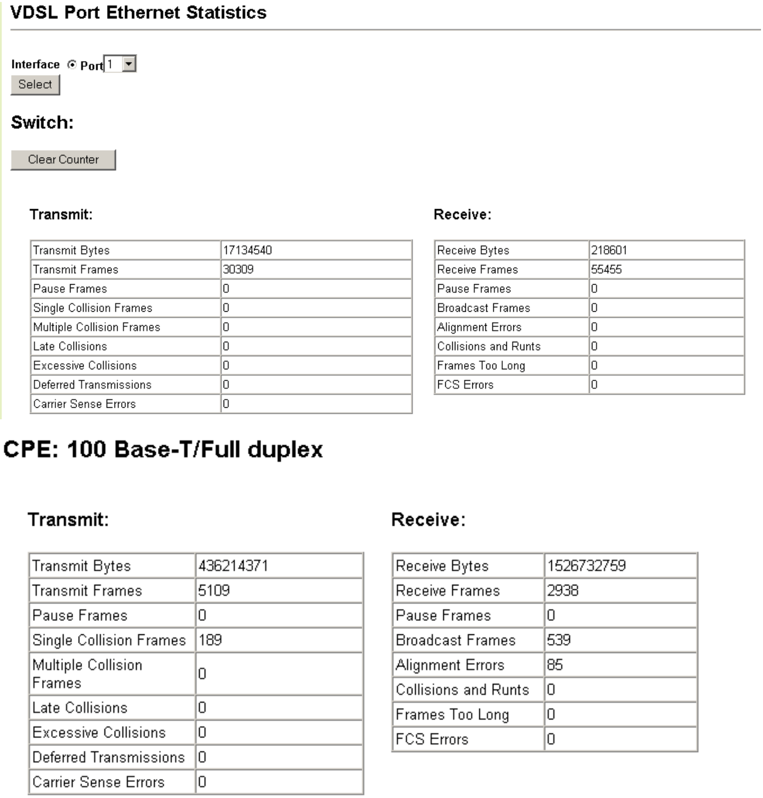
```
Console#show controller efm Ethernet 1/2 actual dsrserrs          3-156
 Downstream Reed-Solomon errors: 0
Console#show controller efm Ethernet 1/2 actual link
 Link status: Down
Console#show controller efm Ethernet 1/2 actual rxpower
 Local receive power: 26.00 dBm/Hz
Console#show controller efm Ethernet 1/2 actual snr
 SNR: 27.00 dB
Console#show controller efm Ethernet 1/2 actual txpower
 Remote transmit power: -89.70 dBm/Hz
Console#show controller efm Ethernet 1/2 actual usrserrs
 Upstream Reed-Solomon errors: 0
Console#
```

Displaying VDSL Port Ethernet Statistics

VDSL Port Ethernet Statistics displays key statistics for an interface.

Web Interface

Click VDSL/VDSL Port Ethernet Statistics.



VDSL Port Ethernet Statistics

Interface ● Port 1

Switch:

Transmit:

Transmit Bytes	17134540
Transmit Frames	30309
Pause Frames	0
Single Collision Frames	0
Multiple Collision Frames	0
Late Collisions	0
Excessive Collisions	0
Deferred Transmissions	0
Carrier Sense Errors	0

Receive:

Receive Bytes	218601
Receive Frames	55455
Pause Frames	0
Broadcast Frames	0
Alignment Errors	0
Collisions and Runts	0
Frames Too Long	0
FCS Errors	0

CPE: 100 Base-T/Full duplex

Transmit:

Transmit Bytes	436214371
Transmit Frames	5109
Pause Frames	0
Single Collision Frames	189
Multiple Collision Frames	0
Late Collisions	0
Excessive Collisions	0
Deferred Transmissions	0
Carrier Sense Errors	0

Receive:

Receive Bytes	1526732759
Receive Frames	2938
Pause Frames	0
Broadcast Frames	539
Alignment Errors	85
Collisions and Runts	0
Frames Too Long	0
FCS Errors	0

Command Line Interface

Use the **show interfaces counters** command.

Example

```
Console#show interfaces counters ethernet 1/11                          3-77
Ethernet 1/11
 Iftable stats:
  Octets input: 19648, Octets output: 714944
  Unitcast input: 0, Unitcast output: 0
  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: 10524
  Broadcast input: 136, Broadcast output: 0
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: 734720, Packets: 10661
  Broadcast pkts: 136, Multi-cast pkts: 10525
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 9877, Packet size 65 to 127 octets: 93
  Packet size 128 to 255 octets: 691, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

Chapter 3
Command Line Interface

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.)
- 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. 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 host 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.)

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 you may 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. 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 host is opened.
To end the CLI session, enter [Exit].

Vty-0#
```

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

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

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

You can enter commands as follows:

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

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

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

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

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 **config**. 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 "configuration" example, typing **con** followed by a tab will result in printing the command up to "**configure**."

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 ?
  bridge          Bridge information
  bridge-ext      Bridge extend information
  controllers     Interface controller status
  garp            Garp property
  gvrp            Show gvrp information of interface
  history         Information of history
  interfaces      Information of interfaces
  ip              Ip
  line            TTY line information
  logging         Show the contents of logging buffers
  map             Map priority
  port            Characteristics of the port
  pvlan           Information of private VLAN
  queue           Information of priority queue
  radius-server   Radius server information
  running-config  The system configuration of running
  snmp            SNMP statistics
  startup-config  The system configuration of starting up
  system          Information of system
  users           Display information about terminal lines
  version         System hardware and software status
  vlan            Switch VLAN Virtual Interface
Console#show
```

The command "**show interfaces ?**" displays 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            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. A 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

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

Exec Commands

When you open a new console session on the switch with the user name "guest," the system enters Normal Exec command mode (or guest mode.) Only a limited number of commands are available in this mode. You may access all commands only in Privileged Exec command mode (or administrator mode.) To access Privilege Exec mode, open a new console session with the user name "admin," or enter the **enable** command (followed by the privileged level access password — the default is "super".) The command prompt displays "Console>" for Normal Exec mode and "Console#" for Privileged Exec mode.

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

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

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

Console#
```

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

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

Console#enable
Password: [privileged level password]
Console#
```

Configuration Commands

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

The configuration commands are organized into three different modes:

- Global Configuration – These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.

- Interface Configuration – These commands modify the port configuration such as **speed-duplex** and **negotiation**.

- Line Configuration – These commands modify the console port configuration, and include command such as **parity** and **databits**.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to

“Console(config)#” which indicates you have privileged level access to Global Configuration commands.

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

To enter Interface, Line Configuration, or VLAN mode you must enter the “**interface** ...,” “**line**...” or “**vlan database**” command while in Global Configuration mode. The system prompt will change to “Console(config-if)#,” “Console(config-line)#” or Console(config-vlan)#” indicating that you have access privileges to the associated commands. You can use the **end** command to return to the Privileged Exec mode.

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

Command Line Processing

Commands are not case sensitive. You may abbreviate commands and parameters as long as they contain enough letters to differentiate them from other currently available commands or parameters. 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 may also use the following editing keystrokes for command-line processing:

Keystroke	**Function**
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Backspaces one character.
Ctrl-E	Shifts cursor to end of command line.
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	3-12
Flash/File	Manages code image or switch configuration files	3-19
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	3-26
Radius Client	Configures RADIUS client-server authentication for logon access	3-39
SNMP	Activates authentication failure traps; configures community access strings, and trap managers	3-44
IP	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	3-51
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	3-68
Address Table	Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time	3-79
Port Security	Configures secure addresses for a port	3-84
Spanning Tree	Configures Spanning Tree settings for the switch	3-85
VLAN	Configures VLAN settings, and defines port membership for VLAN groups	3-95
PVLAN	Enables or configures Private VLAN	3-105
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB	3-105
IGMP Snooping	Configures IGMP multicast filtering, querier eligibility, query parameters, and specifies ports attached to a multicast router	3-114

Command Group	Description	Page
Priority	Sets port priority for untagged frames, relative weight for each priority queue, and the maximum number of queues enabled; also sets priority for TCP/UDP traffic types, IP precedence, and DSCP	3-124
Monitor Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	3-138
Port Trunking and LACP	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	3-141
VDSL	Configures and displays communication parameters for VDSL and Ethernet ports on the switch and connected CPEs	3-146
Rate Limit	Controls the maximum rate for traffic transmitted or received on a port	3-163

General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	3-13
disable	Returns to normal mode from privileged mode	PE	3-14
configure	Activates global configuration mode	PE	3-15
reload	Restarts the system	PE	3-16
end	Returns to Privileged Exec mode	GC, IC, LC, VC	3-17
exit	Returns to the previous configuration mode, or exits the CLI	any	3-17
quit	Exits a CLI session	NE, PE	3-18
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes" on page 3-7.

Syntax

enable [*level*]

level - Privilege level to log in to 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 3-29.)
- The "#" character is appended to the end of the prompt to indicate that the system is in privileged access mode.
- You only need to use Level 15. Setting the password for Level 0 has no effect.

- You cannot set a null password with the **enable password** command. You will have to enter a password to access the Privileged Exec mode.

Example

```
Console#enable
Console#
```

Related Commands

disable
enable password

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 VDSL/Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes" on page 3-7.

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

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 "Understanding Command Modes" on page 3-7.

Default Setting

None

Command Mode

Privileged Exec

Example

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

Related Commands

end

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.

Note: When the system is restarted, it will run the Power-On Self-Test. It will also retain all configuration information stored in nonvolatile 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
```

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	3-19
delete	Deletes a file or code image	PE	3-22
dir	Displays a list of files in Flash memory	PE	3-23
whichboot	Displays the files booted	PE	3-24
boot system	Specifies the file or image used to start up the system	GC	3-25

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

copy

Use this command to copy (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**}

- *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.

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 length of file name should be 1 to 31.
  (Valid characters: A-Z, a-z, 0-9, ".", "-", "_").
- The maximum number of user-defined configuration files depends on available Flash memory.
- You can use "Factory_Default_Config.cfg" as the source file to copy from, but you cannot use "Factory_Default_Config.cfg" 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 follow the console messages displayed during boot up to download the Boot ROM (or Diagnostic) image.

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#
```

Example

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name : startup
/
Console#
```

Example

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
/
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 boot-ROM or 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

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
- **config** - Configuration file
- **opcode** - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.
- *filename* - Name of the file to display.

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

The following example shows how to display all file information:

```
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 booted at the last boot.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table on page 3-10 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.
- 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
whichboot

System Management Commands

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

Command	Function	Mode	Page
Device Description Command			
hostname	Specifies or modifies the host name for the device	GC	3-27
User Access Commands			
enable password	Sets a password to control access to the privileged mode from the normal mode	GC	3-29
Web Server Commands			
ip http port	Specifies the port to be used by the Web browser interface	GC	3-30
ip http server	Allows the switch to be monitored or configured from a browser	GC	3-31
Event Logging Commands			
logging on	Controls logging of error messages	GC	3-31
logging history	Limits syslog messages sent to the SNMP network management station based on severity	GC	3-32
clear logging	Clears messages from the logging buffer	PE	3-33
show logging	Displays the state of logging	PE	3-34
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	3-35
show running-config	Displays the configuration data currently in use	PE	3-36
show system	Displays system information	NE, PE	3-37

Command	Function	Mode	Page
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client	NE, PE	3-37
show version	Displays version information for the system	NE, PE	3-38

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

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 SMC7724M/VSW
Console(config)#
```

username

Use this command to require user name authentication at login. 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; maximum number of 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, case sensitive)

Default Setting

- The default access mode is Privileged Exec.
- The default passwords are “guest” in Normal Exec mode, and “admin” in Privileged Exec mode.

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 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 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the administrator (Privileged Exec) and guest (Normal Exec) passwords. Remember to record them in a safe place. Use the **enable password** command to control access to Privileged Exec mode from the Normal Exec mode. 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 for which the password applies.
- The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Only level 15 (Privileged Exec) is valid for this command.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.

Default Setting

- The default is level 15.
- The default password is "super."

Command Mode

Global Configuration

Command Usage

The encrypted password is for machine use only. To create an encrypted password, you must use an appropriate encryption algorithm.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable

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

ip http server

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

ip http server
no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

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

Related Commands

ip http port

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 to be sent to SNMP trap receivers. You can use the logging history command to control the type of error messages that are stored in memory and sent to a specified SNMP trap receiver.

Example

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

Related Commands

logging history
clear logging

logging history

Use this command to limit syslog messages sent to the Simple Network Management Protocol network management station 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 below. Messages sent include the selected level up through level 0.

Level Argument	Level	Description
emergencies	0	System unusable
alerts	1	Immediate action needed
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warning conditions

Level Argument	Level	Description
notifications	5	Normal but significant condition
informational	6	Informational messages only
debugging	7	Debugging messages

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

Sending syslog messages to the SNMP network management station occurs when you enable syslog traps with the snmp enable traps command.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

Related Commands

snmp-server enable traps
snmp-server host

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

None

Command Mode

Privileged Exec

Example

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

Related Commands

show logging

show logging

Use this command to display the logging configuration for system and event messages.

Syntax

show 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

None

Command Mode

Privileged Exec

Example

```
Console#show logging flash
Syslog logging: Disable
History logging in FLASH: level errors
Console#
```

show startup-config

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

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show startup-config
building startup-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
!
.
.
.
Console#
```

Related Commands

show running-config

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 nonvolatile memory.

Example

```
Console#show running-config
building running-config, please wait.....
!
hostname VDSL Switch-VS2524
!
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
 rate-limit input 0
 switchport allowed vlan add 1 untagged
 switchport native vlan 1.
.
.
.
Console#
```

Related Commands

show startup-config

show system

Use this command to display system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show system
System description: SMC7724M/VSW Manager
System OID string: 1.3.6.1.4.1.259.6.13.1
System information
 System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
 System Name            : SMC7724M/VSW
 System Location        : R&D 3F
 System Contact         : Geoff
 MAC address            : 00-00-e8-00-00-01
 Web server             : enable
 Web server port        : 80
POST result :
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

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

Example

```
Console#show version
Unit1
 Serial number           :123
 Service tag             :
 Hardware version        :3021b
 Module A type           :Stacking Module
 Module B type           :1000BaseX-GBIC
 Number of ports         :25
 Main power status       :up
 Redundant power status :not present
Agent(master)
 Unit id                 :1
 Loader version          :0.0.6.3
 Boot rom version        :0.0.5.2
 Operation code version :1.8.1.2
Console#
```

RADIUS Commands

Remote Authentication Dial-in User Service (RADIUS) is a system that uses a central server running RADIUS software to control access to RADIUS-aware devices on the network. A RADIUS 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 using the console port, Telnet, or Web.

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	3-39
radius-server host	Specifies the RADIUS server	GC	3-40
radius-server port	Sets the RADIUS server network port	GC	3-41
radius-server key	Sets the RADIUS encryption key	GC	3-41
radius-server retransmit	Sets the number of retries	GC	3-42
radius-server timeout	Sets the interval between sending authentication requests	GC	3-42
show radius-server	Shows the current RADIUS settings	PE	3-43

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

authentication login

Use this command to define the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {**radius** | **local** | **radius local** | **local radius**}
no authentication login

- **radius** - Use RADIUS server password only.
- **local** - Use local password only.

- **radius local** - Use RADIUS server password first and local password next.
- **local radius** - Use local password first and RADIUS server password next.

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

enable password - for setting the local password

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

None

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

None

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: 20 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 is 1 - 30)

Default Setting

None

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

None

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
Server IP address: 10.1.0.99
 Communication key with radius server:
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

SNMP Commands

Controls access to this switch from SNMP management stations, 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	3-45
snmp-server contact	Sets the system contact string	GC	3-46
snmp-server location	Sets the system location string	GC	3-46
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	3-47
snmp-server enable traps	Enables the device to send SNMP traps or inform requests (i.e., SNMP notifications)	GC	3-48
show snmp	Displays the status of SNMP communications	NE, PE	3-49

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

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)
- **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 (SNMPv1.) 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 Geoff
Console(config)#
```

Related Commands

snmp-server location

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 R&D 3F
Console(config)#
```

Related Commands

snmp-server contact

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*
no snmp-server host *host-addr*

- *host-addr* - Name or 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. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (maximum length: 32 characters)

Default Setting

None

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. 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.
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

snmp-server enable traps

Use this command to enable this device to send Simple Network Management Protocol traps or informs (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.

Note: The link-up-down trap can only be enabled/disabled via the command line interface.

Default Setting

Issue all 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, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

The notification types used in this command all have an associated MIB object that allows them to be globally enabled or disabled. Not all of the notification types have notification Enable MIB objects, so some of these cannot be controlled using the **snmp-server enable traps** command.

Example

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

Related Commands

snmp-server host

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 counter information for SNMP operations.

Example

```
Console#show snmp
 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 PDUsConsole#

SNMP logging: disabled
Console#
```

IP Commands

An IP address may be used for management access to the switch over your network. By default, the switch's IP address is set via DHCP. If you wish to manually configure an IP address, you need to change the switch's default settings (IP address 0.0.0.0 and netmask 255.0.0.0) so that they are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

Command	Function	Mode	Page
ip address	Sets the IP address for this device	IC	3-52
ip dhcp restart	Submits a BOOTP or DCHP client request	PE	3-53
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

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

ip address

Use this command to set the IP address for this device. 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

IP address: 0.0.0.0
Netmask: 255.0.0.0

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.

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.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart

ip dhcp restart

Use this command to submit a BOOTP or DCHP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- 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

ip default-gateway

Use this command to 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

show ip interface

Use this command to display the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Command Usage

This switch can only be assigned one IP address. This address is used for managing the switch.

Example

```
Console#show ip interface
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Related Commands

show ip redirects

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

ping

Use this command to send ICMP echo request packets to another node on the network.

Syntax

ping *host* [**size** *size*][**count** *count*]

- *host* - IP address or IP alias of the host.
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32 bytes)
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- 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 “no answer from host” 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 10.1.0.19
Type Ctrl-C to abort.
PING to 10.1.0.19, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 0 ms
response time: 0 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
Ping statistics for 10.1.0.19:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 6 ms
Console#
```

Related Commands

interface

Line Commands

Access the on-board 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	3-59
login	Enables password checking at login	LC	3-59
password	Specifies a password on a line	LC	3-60
exec-timeout	Sets the interval with no user input after which the current session will be terminated	LC	3-61
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	3-62
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	3-63
databits	Sets the number of data bits per character that are interpreted and generated by hardware	LC	3-64
parity	Defines the generation of a parity bit	LC	3-65
speed	Sets the terminal baud rate	LC	3-65
stopbits	Sets the number of the stop bits transmitted per byte	LC	3-66
show line	Displays a terminal line's parameters	NE, PE	3-67

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

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.

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**.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line
show users

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

By default, virtual terminals require a password. If you do not set a password for a virtual terminal, it will respond to attempted connections by displaying an error message and closing the connection.

Command Mode

Line Configuration

Command Usage

If you specify login without the local option, authentication is based on the password specified with the password line configuration command.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username
password

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. The string can contain any alphanumeric characters, besides spaces, and can contain up to 8 characters. The password is 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 several functions such as booting up the system, or for compatibility with legacy password settings (i.e., plain text or encrypted) that are copied from a tftp server. There is no need for the user to enter encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login
password-thresh

exec-timeout

Use this command to set the interval with no user input after which the current session will be terminated. Use the **no** form to disable the timeout function.

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 there is user input within the exec-timeout interval, the current session will be maintained. If there is no user input within this time interval, the current 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 120 seconds, 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 inaccessible for a specified amount of time before allowing the next logon attempt. Use the **silent-time** command to set this interval.

- 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

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

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

parity

Use this command to define generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**non**e | **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.

- 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	3-69
description	Adds a description to an interface configuration	IC	3-69
speed-duplex	Configures the speed and duplex operation of a given interface when auto-negotiation is disabled	IC	3-70
negotiation	Enables auto-negotiation of a given interface	IC	3-71
capabilities	Advertises the capabilities of a given interface for use in auto-negotiation	IC	3-72
flowcontrol	Enables flow control on a given interface	IC	3-73
clear counters	Clears the statistics on a given interface	PE	3-74
shutdown	Disables an interface	IC	3-74
switchport broadcast	Configures broadcast storm control	IC	3-75
show interfaces status	Displays status for the specified interface	NE, PE	3-76
show interfaces counters	Displays statistics for the specified interface	NE, PE	3-77
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	3-78

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

interface

Use this command to configure an interface type and enter interface configuration mode.

Syntax

interface *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

None

Command Mode

Global Configuration

Example

To specify the Ethernet port, 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 Ethernet 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 auto-negotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** - Forces 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, 100full for 100BASE-FX 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.

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

negotiation

Use this command to enable auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

Syntax

negotiation
no negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 uplink ports.

Example

The following example configures port 11 to use auto-negotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

capabilities

Use this command to advertise the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values

Syntax

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}
no port-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** - Transmits and receives pause frames for flow control (Gigabit ports only)

Default Setting

The default values for Fast Ethernet include 10half, 10full, 100half, 100full and flow control. The default values for Gigabit Ethernet include all settings.

Command Mode

Interface Configuration (Ethernet, Port Channel)

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)#
```

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.
- Flow control should not be used if a port is connected to a hub. Otherwise flow control signals will be propagated throughout the segment.
- To force operation to the mode specified in a flowcontrol command, use the no negotiation command to disable auto-negotiation on the selected interface.

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

capabilities (flowcontrol, symmetric)

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 Executive

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 re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables VDSL port 5.

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

switchport broadcast

Use this command to configure broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast packet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second. (Range: 500 to 262,143 packets per second)

Default Setting

500 packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control and set the threshold value for the selected interface.
- However, this configuration then applies to the entire switch.

Example

The following shows how to configure broadcast suppression at 1000 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 1000
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

none

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#$
Console#show interfaces status ethernet 1/11
Information of Eth 1/11
 Basic information:
  Port type: 100tx-efm
  Mac address: 00-30-f1-4d-1e-8a
 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#
```

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.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show interfaces counters ethernet 1/11
Ethernet 1/11
 Iftable stats:
  Octets input: 19648, Octets output: 714944
  Unicast input: 0, Unicast output: 0
  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: 10524
  Broadcast input: 136, Broadcast output: 0
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: 734720, Packets: 10661
  Broadcast pkts: 136, Multi-cast pkts: 10525
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 9877, Packet size 65 to 127 octets: 93
  Packet size 128 to 255 octets: 691, 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 advanced interface configuration settings.

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

Example

This example shows the configuration setting for Ethernet port 25.

```
Console#show interfaces switchport ethernet 1/25
Information of Eth 1/25
broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,0M 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: Enabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

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
bridge address	Maps a static address to a port in a VLAN	GC	3-79
show bridge	Displays classes of entries in the bridge-forwarding database	PE	3-81
clear bridge	Removes any learned entries from the forwarding database and clears the transmit and receive counts for any statically or system configured entries	PE	3-82
bridge-group aging-time	Sets the aging time of the address table	GC	3-82
show bridge aging-time	Shows the aging time for the address table	PE	3-83

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

bridge address

Use this command to map a static address to a port in a VLAN. Use the **no** form to remove an address.

Syntax

bridge *bridge-group* **address** *mac-address* **vlan** *vlan-id* **forward** *interface* [*action*]
no bridge *bridge-group* **address** mac-*address* **vlan** *vlan-id*

- *bridge-group* - Bridge group index (bridge 1.)
- *mac-address* - MAC address.
- *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)
- *action* -
    - delete-on-reset - Assignment lasts until 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.
- When a static address is dynamically learned on an interface, it will not be written to the address table..

Example

```
Console(config)#bridge 1 address 00-e0-29-94-34-de vlan 1 forward ethernet
1/1 delete-on-reset
Console(config)#
```

show bridge

Use this command to view classes of entries in the bridge-forwarding database.

Syntax

show bridge *bridge-group* [*interface*] [*address* [*mask*]] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *bridge-group* - Bridge group index (bridge 1)
- *interface*
  - **ethernet** *unit/port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Range: 1-6)
- *address* - MAC address.
- *mask* - Bits to ignore in the address.
- *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

Example

```
Console#show bridge 1
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

clear bridge

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.

Syntax

clear bridge [*bridge-group*]

bridge-group - Bridge group index (bridge 1.)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear bridge 1
Console#
```

bridge-group 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

bridge-group *bridge-group* **aging-time** *seconds*
no bridge-group *bridge-group* **aging-time**

- *bridge-group* - Bridge group index (bridge 1.)
- *seconds* - Time is number of seconds (10-1000000.)

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)#bridge-group 1 aging-time 300
Console(config)#
```

show bridge group aging-time

Use this command to show the aging time for entries in the address table.

Syntax

show bridge group *bridge-group* **aging-time**

bridge-group - Bridge group index (bridge 1)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show bridge group 1 aging-time
 Aging time: 300 sec.
Console#
```

port security

Use this command to configure a secure port. Use the **no** form to disable port security.

Syntax

port security
no port security

Default Setting

All port security is disabled.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When port security is enabled, the selected port will stop learning MAC addresses. This prevents unauthorized access to the switch. The MAC addresses aefmady in the address table will be retained and will not age out.
- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - Cannot be a multi-VLAN interface.
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.

Example

This example enables port security for port 5.

```
Console(config)# interface ethernet 1/5
Console(config-if)# port security
Console(config-if)#
```

Spanning Tree Commands

This section includes commands that configure STP for the overall switch, and commands that configure STP for the selected interface.

Command	Function	Mode	Page
bridge spanning-tree	Enables the spanning tree protocol	GC	3-87
bridge forward-time	Configures the spanning tree bridge forward time	GC	3-87
bridge hello-time	Configures the spanning tree bridge hello time	GC	3-88
bridge max-age	Configures the spanning tree bridge maximum age	GC	3-89
bridge priority	Configures the spanning tree bridge priority	GC	3-90
bridge-group path-cost	Configures the spanning tree path cost of an interface	IC	3-91
bridge-group priority	Configures the spanning tree priority of an interface	IC	3-92
bridge-group portfast	Sets an interface to fast forwarding	IC	3-93
show bridge group	Shows spanning tree configuration for the overall bridge or a selected interface	PE	3-94

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

bridge spanning-tree

Use this command to enable the spanning tree algorithm globally for this switch. Use the **no** form to disable it.

Syntax

bridge *bridge-group* **spanning-tree**
no bridge *bridge-group* **spanning-tree**

bridge-group - Bridge group index (bridge 1.)

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm 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

The following example shows how to enable the Spanning Tree Algorithm for this switch:

```
Console(config)#bridge 1 spanning-tree
Console(config)#
```

bridge 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

bridge *bridge-group* **forward-time** *seconds*
no bridge *bridge-group* **forward-time**

- *bridge-group* - Bridge group index (bridge 1.)
- *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., listening 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)#bridge 1 forward-time 20
Console(config)#
```

bridge 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

bridge *bridge-group* **hello-time** *time*
no bridge *bridge-group* **hello-time**

- *bridge-group* - Bridge group index (bridge 1.)
- *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)#bridge 1 hello-time 5
Console(config)#
```

bridge 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

bridge *bridge-group* **max-age** *seconds*
no bridge *bridge-group* **max-age**

- *bridge-group* - Bridge group index (bridge 1.)
- *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)#bridge 1 max-age 40
Console(config)#
```

bridge priority

Use this command to configure the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

bridge *bridge-group* **priority** *priority*
no bridge *bridge-group* **priority**

- *bridge-group* - Bridge group index (bridge 1.)
- *priority* - Priority of the bridge. (Range: 0 - 65535)

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)#bridge 1 priority 40000
Console(config)#
```

bridge-group path-cost

Use this command to configure the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

bridge-group *bridge-group* **path-cost** *cost*
no bridge-group *bridge-group* **path-cost**

- *bridge-group* - Bridge group index (bridge 1.)
- *cost* - The path cost for the port. (Range: 1-65535)
- The recommended range is -
  - Ethernet: 50-600
  - Fast Ethernet: 10-60
  - Gigabit Ethernet: 3-10

Default Setting

- Ethernet – half duplex: 100; full duplex: 95; trunk: 90
- Fast Ethernet – half duplex: 19; full duplex: 18; trunk: 15
- Gigabit Ethernet – full duplex: 4; trunk: 3

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.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 path-cost 50
Console(config-if)#
```

bridge-group priority

Use this command to configure the priority for the specified port. Use the **no** form to restore the default.

Syntax

bridge-group *bridge-group* **priority** *priority*
no bridge-group *bridge-group* **priority**

- *bridge-group* - Bridge group index (bridge 1.)
- *priority* - The priority for a port. (Range: 0-255)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the spanning-tree algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 priority 0
Console(config-if)#
```

bridge-group portfast

Use this command to set a port to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

bridge-group *bridge-group* **portfast**
no bridge-group *bridge-group* **portfast**

bridge-group - Bridge group index (bridge 1.)

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 Blocked, Listening 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 an end-node device.)

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

show bridge group

Use this command to show the spanning tree configuration.

Syntax

show bridge group *bridge-group* [*interface*]

- *bridge-group* - Bridge group index (bridge 1.)
- *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 bridge group 1 ethernet 1/11
Bridge-group information
-------------------------------------------------------
 Spanning tree protocol           :ieee8021d
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Hello Time (sec.)                :2
 Max Age (sec.)                   :20
 Forward Delay (sec.)             :15
 Designated Root                  :32768.0000e9000066
 Curent root                      :0
 Curent root cost                 :0
 Number of topology changes       :1
 Last topology changes time (sec.):2167
 Hold times (sec.)                :1
-------------------------------------------------------
Eth 1/11 information
-------------------------------------------------------
 Admin status           : enable
 STA state              : broken
 Path cost              : 18
 Priority               : 128
 Designated cost        : 0
 Designated port        : 128.11
 Designated root        : 40000.123412341234
 Designated bridge      :32768.0000e9000066
 Fast forwarding        :disable
 Forward transitions    :0
Console#
```

VLAN Commands

A VLAN is a group of ports that may 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	3-95
vlan	Configures a VLAN, including VID, name and state	VC	3-97
Configure VLAN Interfaces			
interface vlan	Enters interface configuration mode for specified VLAN	IC	3-98
switchport mode	Configures VLAN membership mode for an interface	IC	3-99
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	3-100
swicthport ingress-filtering	Enables ingress filtering on an interface	IC	3-100
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	3-101
switchport allowed vlan	Configures the VLANs associated with an interface	IC	3-102
switchport gvrp	Enables GVRP for an interface	IC	3-108
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	3-103

Command	Function	Mode	Page
Display VLAN Information			
show vlan	Shows VLAN information	NE, PE	3-104
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	3-76
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	3-78

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

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

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

- When **no vlan** *vlan-id* is used, the VLAN is deleted.
- When **no vlan** *vlan-id* **name** is used, the VLAN name is removed.
- When **no vlan** *vlan-id* **state** is used, the VLAN returns to the default state (i.e., active.)

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

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

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 and receives tagged frames that identify the source VLAN.
- **hybrid** - Keyword that specifies a hybrid VLAN interface. The port may receive or transmit tagged or untagged frames. Any frames that are not tagged will be assigned to the default VLAN.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Configures VLAN membership mode for a port.

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

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 passes 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

- If a port is is connected to a VLAN-aware device at the other end of a VLAN trunk, you can set the port to pass only tagged frames. Otherwise, you must configure the port to pass all frame types.

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

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

- 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.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

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 VID) 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 the switchport mode is set to **trunk**, the PVID will be inserted into all untagged frames sent from a tagged port.
- If ingress filtering in disabled, all untagged frames received on this port will be assigned to the VLAN indicated by the PVID.

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. 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

You must enter the switchport mode command before the switchport allowed vlan command can take effect.

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 IDs to add.
- **remove** *vlan-list* - List of VLAN IDs to remove.
  Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. (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.

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 Name     Status    Ports/Channel groups
---- -------- --------- ---------------------------------
   1 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
Console#
```

PVLAN Commands

pvlan

Use this command in global configuration mode to enable a Private VLAN. Once enabled, use the **pvlan up-link - down-link** command to configure the PVLAN. Use the **no** form of the command to disable it.

Syntax

pvlan
pvlan up-link *interface-list* **down-link** *interface-list*
no pvlan

- **up-link** – Specifies a list of uplink interfaces. To make a list of ports, use a comma (,) between port nunumbers. (See Example 2 on the next page.)
- **down-link** – Specifies a list of downlink interfaces. To make a list of ports, use a comma (,) between port numbers. (See Example 2 on the next page.)

Default Setting

For the two commands:
Disabled with no PVLAN interfaces.

Command Mode

Global configuration

Command Usage

A Private VLAN allows modification of the default VLAN to provide port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the uplink port.

The pvlan command without an argument enables/disables the PVLAN. The pvlan up-link down-link command configures the interface members, but does not enable the PVLAN.

Private VLANs and normal VLANs can exist simultaneously within the same switch. The members of private VLANs can only consist of certain groups. The port groups permitted include:

For the 24-Line VDSL Switch:

```
<<1-8>> <<9-16>> <<17-24>> <<25>> <<26>>
```

For the 12-Line VDSL Switch:

```
<<1-8>> <<9-12>> <<13-16>>
```

When one port in a group is configured as a downlink or uplink port, all other ports in that group are also configured as downlink or uplink ports.

Example 1

This example shows trunk 1 being configured as a downlink interface. However, since ports 9 and 17 are members of trunk 1, ports 9-24 would all become downlink ports.

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/25 down-link port-channel 1
Console(config)#
```

Example 2

In this example ports 9 and 17 are shown being configured as downlink ports but in fact ports 9-24 will all become downlink ports. To make a list of ports, use a comma (,) between port numbers.

```
Console(config)#pvlan up-link ethernet 1/25 down-link ethernet 1/9,17
Console(config)#
```

show pvlan

Use this command in privileged configuration mode to display the configured private VLANs.

Syntax

show pvlan

Command Mode

Privileged exec

Example

```
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/25
Down-link port:
 Trunk 1
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	3-108
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	3-103
show gvrp configuration	Displays GVRP configuration for selected interface	NE, PE	3-109
garp timer	Sets the GARP timer for the selected function	IC	3-110
show garp timer	Shows the GARP timer for the selected function	NE, PE	3-111
Global Commands			
bridge-ext gvrp	Enables GVRP globally for the switch	GC	3-112
show bridge-ext	Shows bridge extension configuration	PE	3-113

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

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

Enabled

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
Whole system:
GVRP configuration: Enabled
Eth 1/ 1:
 Gvrp configuration: Enabled
Eth 1/ 2:
 Gvrp configuration: Enabled
```

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**} - The timer to be 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: 100 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.

- Timer values must meet the following restrictions:
  - leave >= (2 x join)
  - leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP will 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

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 sec.
 Leave timer: 60 sec.
 Leaveall timer: 1000 sec.
Console#
```

Related Commands

garp timer

bridge-ext gvrp

Use this command to enable GVRP. Use the **no** form to disable it.

Syntax

bridge-ext gvrp
no bridge-ext gvrp

Default Setting

Enabled

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

Example

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

IGMP Snooping 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	3-115
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	3-115
ip igmp snooping version	Configures the IGMP version for snooping	GC	3-116
show ip igmp snooping	Shows the IGMP snooping configuration	PE	3-117
show bridge multicast	Shows the IGMP snooping MAC multicast list	PE	3-117
IGMP Querier Commands			
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	3-118
ip igmp snooping query-count	Configures the query count	GC	3-119
ip igmp snooping query-interval	Configures the query interval	GC	3-119
ip igmp snooping query-max-response-time	Configures the report delay	GC	3-120
ip igmp snooping query-time-out	Configures the query timeout	GC	3-121
show ip igmp snooping	Shows the IGMP snooping configuration	PE	3-117

Command	Function	Mode	Page
Mulitcast Router Commands			
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	3-122
show ip igmp snooping mrouter	Shows multicast router ports	PE	3-123

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

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

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 bridge multicast

Use this command to show known multicast addresses.

Syntax

show bridge *bridge-group* **multicast** [**vlan** *vlan-id*]
[**user** | **igmp-snooping**]

- *bridge-group* - Bridge group index.
- *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

Example

The following shows the multicast entries learned through IGMP snooping for bridge group 1, VLAN 1:

```
Console#show bridge 1 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 snooping 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 solicit reports. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

ip igmp snooping query-interval

Use this command to configure the snooping 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.

- The command sets the time the switch waits after receiving an IGMP report (for an IP multicast address) on a port before it sends an IGMP Query out that port and then removes the entry from its list.

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

ip igmp snooping query-time-out

Use this command to configure the snooping query-timeout. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping query-time-out *seconds*

no ip igmp snooping query-time-out

seconds - The time the switch waits after the previous querier has stopped querying before it takes over as the querier. (Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using 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

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

Example

The following shows the ports in VLAN 1 which are attached to multicast routers:

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

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Command	Function	Mode	Page
Layer 2 Priority Commands			
switchport priority default	Sets a port priority for incoming untagged frames	IC	3-125
queue bandwidth	Assigns round-robin weights to the priority queues	GC	3-126
queue cos map	Assigns class of service values to the priority queues	IC	3-127
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	3-129
show queue cos-map	Shows the class of service map	PE	3-129
show interfaces switchport	Displays the administrative and operational status of an interface	PE	3-78
Layer 3 and 4 Priority Commands			
map ip port	Enables TCP/UDP class of service mapping	GC	3-130
map ip port	Maps TCP/UDP socket to a class of service	IC	3-131
map ip precedence	Enables IP precedence class of service mapping	GC	3-131
map ip precedence	Maps IP precedence value to a class of service	IC	3-132
map ip dscp	Enables IP DSCP class of service mapping	GC	3-133
map ip dscp	Maps IP DSCP value to a class of service	IC	3-134

Command	Function	Mode	Page
show map ip port	Shows the IP port map	PE	3-135
show map ip precedence	Shows the IP precedence map	PE	3-136
show map ip dscp	Shows the IP DSCP map	PE	3-137

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

switchport priority default

Use this command to set a priority for incoming untagged frames, or the priority of frames received by the device connected to the specified interface. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero. The switch is not instructed what to do with the priority.

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 port priority applies if the incoming frame is an untagged frame received from a VLAN trunk or a static-access port. 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 priority queues for each port. It is configured to use Weighted Round Robin, which can viewed with the **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 ports 3 to 5:

```
Console(config)#interface ethernet 1/3
Console (config-if)#switchport priority default 5
```

queue bandwidth

Use this command to assign weighted round-robin (WRR) weights to the four class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1...weight255*

no queue bandwidth

- *weight1...weight255* - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 255)

Default Setting

WRR is disabled. Strict priority is used for default scheduling. Weights 1, 4, 16 and 64 are assigned to queue 0, 1, 2 and 3 respectively.

Command Mode

Global Configuration

Command Usage

WRR allows bandwidth sharing at the egress port by defining scheduling weights.

Example

The following example shows how to assign WRR weights of 1, 3, 5 and 7 to the CoS priority queues 0, 1, 2 and 3:

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

Related Commands

show queue bandwidth

queue cos-map

Use this command to assign class of service (CoS) values to the CoS priority queues. Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The queue id of the CoS priority queue.
- Ranges are 0 to 3, where 3 is the highest CoS priority queue.
- *cos1* .. *cosn* - The CoS values that are mapped to the queue id. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using four priority queues, with Weighted Round Robin queuing for each port. Up to 8 separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

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

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 CoS priority queue 0, value 3 to CoS priority queue 1, values 4 and 5 to CoS priority queue 2, and values 6 and 7 to CoS priority queue 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

Related Commands

show queue cos-map

show queue bandwidth

Use this command to display the Weighted Round Robin (WRR) bandwidth allocation for the four class of service (CoS) priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
        0      1
        1      4
        2     16
        3     64
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
 Queue ID Traffic class
 -------- -------------
    0     1 2
    1     0 3
    2     4 5
    3     6 7
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.

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.

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* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping. 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.

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 - Maps CoS values to IP ports (i.e., TCP/UDP ports)

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 - Maps CoS values to IP precedence values

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 - Maps CoS values to IP DSCP values

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	3-138
show port monitor	Shows the configuration for a mirror port	PE	3-140

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

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.

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)#
```

Related Commands

show port monitor

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

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#
```

Related Commands

port monitor

Port Trunking Commands

Ports can be statically grouped into an aggregate link 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. You can configure trunks between switches of the same type. This switch supports up to six trunks. The uplink ports can be trunked together and the VDSL ports can be trunked together.

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	3-142
channel-group	Adds a port to a trunk	IC	3-142
Dynamic Configuration Command			
lacp	Configures LACP for the current interface	IC	3-144
Trunk Status Display Command			
show interfaces status port-channel	Shows trunk information	NE, PE	3-76

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

interface port-channel

Use this command to configure a trunk and enter interface configuration mode for the trunk. Use the **no** form of this command to delete a trunk.

syntax

interface port-channel *port-channel-number*
interface port-channel *port-channel-number*

port-channel-number - Trunk index

Default Setting

No trunks configured

Command Mode

Global Configuration

Example

The following creates trunk 1 and enters interface configuration mode:

```
Console#config
Console(config)#interface port-channel 1
Console(config-if)#
```

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 - The current port will be added to this trunk

Default Setting

A new trunk contains no ports

Command Mode

Interface Configuration

Command Usage

- The uplink ports can be trunked together.
- The VDSL ports can be trunked together.
- All links in a trunk must operate at the same data rate and duplex mode.

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)#
```

show interfaces status port-channel

Use this command to show trunk information.

Syntax

show interfaces status port-channel [*port channel number*]

port channel number - Number of the trunk to show.

Default Setting

No default

Command Mode

Privileged EXEC

Example

The following shows information on Trunk 1.

```
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 100TX-efm
  Mac address: 00-30-F1-4D-1E-8B
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control: Disabled
 Current status:
  Created by: User
  Link status: Down
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12,
Console#
```

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

- Finish configuring a port trunk before you connect the corresponding network cables between switches.
- You can configure one trunk group, containing up to four ports as a dynamic LACP trunk.
- The ports on both ends of a trunk must be configured the same for speed, duplex mode, and flow control.
- If the target switch has also enabled LACP on the connected ports, the

trunk will be activated.

- 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.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel id.

Example

The following shows LACP enabled on ports 1 and 2. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 2** command shows that Trunk 2 has been established.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/2
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-efm
  Mac address: 00-30-F1-4D-1E-8B
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control: Disabled
 Current status:
  Created by: lacp
  Link status: Up
  Port operational status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/1, Eth1/2,
Console#
```

VDSL Commands

These commands are used to to configure and display communication parameters for VDSL and Ethernet ports on the switch and connected CPEs.

Note: The term EFM used in this section stands for Ethernet in the First Mile. The "first mile" is the connection between business and residential users and the public network. The Extended Ethernet switch uses VDSL-based technology for this connection.

Command	Function	Mode	Page
efm profile global	Batch assigns profiles for speed to all the VDSL ports on the switch	GC	3-147
efm profile	Assigns profiles for speed to individual VDSL ports	IC	3-149
efm define user-profile	Configures downstream rate, upstream rate, and interleave depth for user-specified profiles	GC	3-150
efm reset	Resets the switch VDSL chipset or, if a CPE is connected, the CPE VDSL chipset	IC	3-151
efm shutdown	Disables the VDSL chipset transmitter of an efm port that not being used.	PE	3-151
efm rdl	Enables/disables Remote Digital Loopback (RDL) mode.	IC	3-152
efm flow-control	Configures the maximum speed of transmission of data from a specific switch VDSL port to the CPE.	IC	3-153
show controllers ethernet-controller	Displays the Ethernet link transmit and receive statistics on a specific VDSL port.	PE	3-154
show controllers efm interface-id actual	Displays the current values of the VDSL link on a specific VDSL port.	PE	3-156
show controllers efm interface-id admin	Displays the administrative settings of the VDSL link on a specific VDSL port.	PE	3-157

Command	Function	Mode	Page
show controllers efm profile	Displays information about the EFM profiles available on the switch, and how they are assigned to the VDSL ports.	PE	3-158
show controllers efm status	Displays the VDSL link statistics and profile information on a specific VDSL port	PE	3-160
show controllers efm remote ethernet mode	Displays the connected CPE ethernet mode.	PE	3-162

Note: The access mode shown in the table is indicated by these abbreviations: **NE** (Normal Exec), **PE** (Privileged Exec), **GC** (Global Configuration), **IC** (Interface Configuration), **LC** (Line Configuration), **VC** (VLAN Database Configuration.)

efm profile global

Use this command to batch assign profiles for speed to all the VDSL ports on the switch.

Syntax

efm profile global *profile name*

profile name - Name of the profile.

Default Setting

None

Command Mode

Global Configuration

Command Usage

Assigns the same profile to each VDSL switch port. Details of these profiles are given in the table below:

Profile Name	Profile Type	Downstream Rate (Mbps)	Upstream Rate (Mbps)
default	Private	4.17	1.56
efm-5	Private	6.25	6.25
efm-10	Private	12.50	12.50
efm-15	Private	16.67	18.75
public-ansi	Public	16.67	4.67
public-etsi	Public	12.50	4.67
efm-5 LL	Private	6.25	6.25
efm-10 LL	Private	12.50	12.50
efm-15 LL	Private	16.67	18.75
public-ansiLL	Public	16.67	4.67
public-etsiLL	Public	12.50	4.67
efm-15-3LL	Private	16.67	3.13
efm-15-2LL	Private	16.67	2.08
efm-15-1LL	Private	16.67	1.56
efm-10-2 LL	Private	12.50	2.08
user-1	Private	4.00	1.00
user-2	Private	4.00	1.00

Notes:

1. The actual data rates may be somewhat less than those shown in the table above depending on the protocols/applications used.
2. If the "LL" type profile is selected, the error rate due to noise in transmission is increased but the signal latency is reduced.
3. The "Public" profiles conform to specific standards such as ANSI or ETSI. The "Private" profiles do not conform to these standards.
4. Profiles "user-1" and "user-2" are user-configured profiles. The values shown for the downstream and upstream rates are

the default values. These rates may be configured to values between 1 Mbps and 15 Mbps.

Example

```
Console#config
Console(config)#efm profile global public-ansi
Console(config)#
```

Related Commands

efm profile

efm profile

Use this command to assign profiles for speed to a specific VDSL port on the switch.

Syntax

efm profile *profile name*

profile name - Name of the profile.

Default Setting

None

Command Mode

Interface Configuration

Command Usage

Assigns a profile to a specific VDSL port. For details of these profiles see the table under Command Usage for **efm profile global**.

Example

The following example shows profile “efm-10” assigned to VDSL port 1.

```
Console#config
Console(config)#efm profile global public-ansi
Console(config)#interface ethernet 1/1
Console(config-if)#efm profile efm-10
Console(config-if)#
```

Related Commands

efm profile global
efm define user-profile

efm define user-profile

Use this command to configure downstream rate, upstream rate and interleave depth for user-specified profiles.

Syntax

efm define user-profile [*profile number*] [*downstream rate*] [*upstream rate*] [*interleave depth*]

- *profile number* – user-specified profiles can be user-1 or user-2
- *downstream rate* – Rate of data transmission from the switch to the CPE. (Range 1 Mbps - 15 Mbps)
- *upstream rate* - Rate of data transmission from the CPE to the switch. (Range 1 Mbps - 15 Mbps)
- *interleave depth* - Determines the degree of protection of the data signal against impulse noise provided by interleaving.
  (Values: 2 or 16. 16 specifies maximum protection)

Default Setting

0 - interleaving is disabled

Command Mode

Global Configuration

Command Usage

User-specified EFM profiles can be assigned to all the VDSL ports by using the **efm profile global** command, or to specific VDSL ports by using the **efm profile command**.

Example

The following example shows user-profile 1 configured to a downsteam rate of 15 Mbps, an upstream rate of 5 Mbps, and an interleave depth of 2.

```
Console(config)#efm define user-profile 1 15 5 2
Console(config)#
```

Related Commands

efm profile global
efm profile

efm reset

Use this command to reset the switch VDSL chipset or, if a CPE is connected, the CPE VDSL chipset.

Syntax

efm reset {**local** | **remote**}

- **local** - Resets the VDSL chipset for an EFM port.
- **remote** - Resets the CPE side VDSL chipset of an EFM port.

Default Setting

None

Command Mode

Interface Configuration

Command Usage

Use this command to troubleshoot EFM port performance.

Example

The following example resets the switch and CPE side VDSL chipset of VDSL port 1

```
Console#config
Console(config)#interface ethernet 1/1
Console(config-if)#efm reset local
Console(config-if)#efm reset remote
Console(config-if)#
```

efm shutdown

Use this command to disable a VDSL interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown
no shutdown

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration

Command Usage

Use this command to disable the VDSL chipset transmitter of a VDSL port that is not connected to a working CPE. In some unusual circumstances, the power emitted by VDSL ports can affect other VDSL ports. It is recommended that ports that are not wired to CPEs be shutdown in this way. Also use this command to disable access to the switch from this port.

Example

The following example disables VDSL port 1.

```
Console (config)#interface ethernet 1/1
Console(config-if)#efm shutdown
Console(config-if)#
```

Related Commands

shutdown

efm rdl

Use this command to enable RDL. To disable RDL use the **no** form of the command.

Syntax

efm rdl
no efm rdl

Default Setting

Off

Command Mode

Interface Configuration

Command Usage

Remote Digital Loopback (RDL) tests the link between the switch and the CPE by sending out, and returning data through the CPE, over the VDSL link.

Example

The following example shows how to enable/disable RDL on VDSL port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm rdl
Console(config-if)#no efm rdl
Console(config-if)#
```

efm flow-control

Use this command to configure the maximum speed of transmission of data from a specific switch VDSL port to the CPE.

Syntax

efm flow-control flow-control-value

flow-control-value - from 0 to the maximum transmission rate available. 0 means the port is disabled. The maximum transmission rate is determined by the physical link and the EFM profile selected (see page 3-147.)

Default Setting

The maximum transition rate available. This is determined by the physical link and the EFM profile selected (see page 3-147.)

Command Mode

Interface Configuration

Example

The following example shows VDSL port 1 configured to a maximum transmission rate of 1 Mbps.

```
Console#config
Console(config)#interface ethernet 1/1
Console(config-if)#efm flow-control 1
Console(config-if)#
```

Related Commands

rate-limit (global)
rate-limit

show controllers ethernet-controller

Use this command to display the Ethernet link transmit and receive statistics for a specific VDSL port, or for all the VDSL ports on the switch and the connected CPE.

Syntax

show controllers ethernet-controller *interface-id*

interface-id - ID of the EFM port

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

Using this command without specifying a VDSL port displays the Ethernet link statistics of all ports on the switch and on the connected CPE devices. The output shows the statistics collected by the VDSL chipset on the switch, and the statistics collected by the VDSL chipset on the CPE.

Example

The following example resets the switch and CPE side VDSL chipset of VDSL port 1

```
Console#show controllers ethernet-controller ethernet 1/2
Ethernet 1/2 :
efm PHY on Switch:
Transmit
         0 Bytes Transmitted
         0 Frames Transmitted
         0 Pause frames
         0 Single Collision Frames
         0 Multiple collisions
         0 Late collisions
         0 Excessive collisions
         0 Deferred frames
         0 Carrier sense errors
Receive
         0 Bytes Received
         0 Frames Received
         0 Broadcast frames
         0 Pause frames
         0 Alignment errors
         0 Collisions and Runts
         0 Oversize frames
         0 FCS errors

efm MAC on CPE:
```

Related Commands

clear controllers
ethernet-controller

show controllers efm interface-id actual

Use this command to display the current values of the VDSL link on a specific VDSL port.

Syntax

show controllers efm *interface-id* **actual** {**dsrserrs** | **usrserrs** | **txpower** | **rxpower** | **snr** | **link**}

- *interface-id* - ID of the VDSL port.
- **actual** - Displays the VDSL port current status, which might not be the same as the administratively configured settings.
- **dsrserrs** - Displays the downstream Reed-Solomon errors on the VDSL port.
- **link** - Displays the VDSL link status of the VDSL port.
- **rxpower** - Displays the local receive power (dBm/Hz) on the remote customer premises equipment (CPE) port.
- **snr** - Displays the signal-to-noise ratio (SNR) ratio on the VDSL port.
- **txpower** - Displays the remote transmit power (dBm/Hz) on the VDSL port.
- **usrserrs** - Displays the upstream Reed-Solomon errors on the VDSL port.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

SNR and Reed-Solomon error information displays the quality of the VDSL link.

- The SNR represents the upper limit of received signal to noise ratio that the switch will handle before disconnecting from the remote CPE.

- The Reed-Solomon errors show the number of errors detected and corrected in the data being received on, and transmitted from, the VDSL ports. Reed-Solomon errors are the result of noise exceeding the noise margin.

Example

The following example displays the current values of the VDSL link on VDSL switch port 2.

```
Console#show controller efm Ethernet 1/2 actual dsrserrs
 Downstream Reed-Solomon errors: 0
Console#show controller efm Ethernet 1/2 actual link
 Link status: Down
Console#show controller efm Ethernet 1/2 actual rxpower
 Local receive power: 26.00 dBm/Hz
Console#show controller efm Ethernet 1/2 actual snr
 SNR: 27.00 dB
Console#show controller efm Ethernet 1/2 actual txpower
 Remote transmit power: -89.70 dBm/Hz
Console#show controller efm Ethernet 1/2 actual usrserrs
 Upstream Reed-Solomon errors: 0
Console#
```

Related Commands

show controllers efm interface-id admin
show controllers efm profile

show controllers efm interface-id admin

Use this command to display the actual values of the VDSL link on a specific VDSL port.

Syntax

show controllers efm *interface-id* **admin** {**dsrate** | **usrate**}

- *interface-id* - ID of the VDSL port.
- **admin** - Display the administrative settings, which might not be the same as the actual values.
- **dsrate** - Displays the downstream rate (Mbps) of the VDSL link.
- **usrate** - Displays the upstream rate (Mbps) of the VDSL link.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

This command displays the profile settings of a VDSL port. This profile determines the upstream and downstream rates.

Example

```
Console#show controller efm Ethernet 1/1 admin usrate
 Upstream rate: 12.50 Mbps
Console#show controller efm Ethernet 1/1 admin dsrate
 Downstream rate: 12.50 Mbps
Console#
```

Related Commands

show controllers efm interface-id actual
show controllers efm profile

show controllers efm profile

Use this command to to display information about the Ethernet in the First Mile (EFM) profiles available on the switch, and how they are assigned to the VDSL ports.

Syntax

show controllers efm profile {**mapping** | **names**}

- **mapping** - Displays a list of the VDSL ports and their assigned profiles.
- **names** - Displays the names, types, and upstream and downstream data rates of all profiles available on the switch. Overall data rates are displayed. The usable data rates are somewhat lower.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

See the table under “VDSL Commands” on page 3-146 for the EFM profiles shipped with the switch, and for their upstream and downstream data rates.

Examples

This example shows sample output from the **show controllers efm profile mapping** command.

```
Console#show controllers efm profile mapping
Interface        Port Profile            Status
-------------    --------------------   --------
Ethernet 1/1     efm-10                  Active
Ethernet 1/2     public-ansi             Active
Ethernet 1/3     public-ansi             Active
Ethernet 1/4     public-ansi             Active
Ethernet 1/5     public-ansi             Active
Ethernet 1/6     public-ansi             Active
Ethernet 1/7     public-ansi             Active
Ethernet 1/8     public-ansi             Active
Ethernet 1/9     public-ansi             Active
Ethernet 1/10    public-ansi             Active
Ethernet 1/11    public-ansi             Active
Ethernet 1/12    public-ansi             Active
Console#
```

This example shows sample output from the **show controllers efm profile names** command.

```
Console#show controllers efm profile names
Profile Name         Type     Downstream Rate(Mbps)   Upstream Rate(Mbps)
--------------------  -------  ---------------------   ------------------
default                Private   4.17                    1.56
efm-5                  Private   6.25                    6.25
efm-10                 Private   12.50                   12.50
efm-15                 Private   16.67                   18.75
public-ansi            Public    16.67                   4.67
public-etsi            Public    12.50                   4.67
efm-5LL                Private   6.25                    6.25
efm-10LL               Private   12.50                   12.50
efm-15LL               Private   16.67                   18.75
public-ansiLL          Public    16.67                   4.67
public-etsiLL          Public    12.50                   4.67
efm-15-3LL             Private   16.67                   3.13
efm-15-2LL             Private   16.67                   2.08
efm-15-1LL             Private   16.67                   1.56
efm-10-2LL             Private   12.50                   2.08
user-1                 Private   4.00                    1.00
user-2                 Private   4.00                    1.00
Console#
```

Note: If an "LL" type profile is selected, the error rate due to noise in transmission, is increased, but the signal latency is decreased

Related Commands

show controllers efm interface-id actual
show controllers efm interface-id admin

show controllers efm status

Use this command to display the VDSL link statistics and profile information on a specific VDSL port including link state, link duration, data rates, power levels, signal-to-noise ratio, and Reed-Solomon errors.

Syntax

show controllers efm status {**link** | **profile**} [*interface-id*]

- *interface-id* - ID of the VDSL port
- **link** - Displays VDSL link parameters and status.
- **profile** - Displays VDSL link parameters and status.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

SNR and Reed-Solomon error information display the quality of the VDSL link.

- Using this command without specifying a VDSL port displays the status of all VDSL ports.
- The SNR represents the upper limit of received signal to noise ratio that the switch will handle before disconnecting from the remote CPE.
- The Reed-Solomon errors show the number of errors detected and corrected in the data being received on and transmitted from

the VDSL ports. Reed-Solomon errors are the result of noise exceeding the noise margin.

Note: The Reed-Solomon errors are reset each time the **show controllers efm status link** command is performed.

- The interleaver prevents loss of Ethernet data packets. The interleaver columns display the interleaver block size for both directions of data.
- The PMD-S displays the physical media dependent status and provides diagnostic information.

Examples

This example shows sample output from the **show controllers efm status link** command

```
Console#show controllers efm status link Ethernet 1/1
Interface      Link  SNR    RS Errs   CPE-Tx    Interleaver     PMD-S
                     (dB)             (dBm/Hz)  Rx-Bsz  Tx-Bsz
-------------  ----  -----  --------  --------  --------------  -----
Ethernet 1/1   Up    27.62  0         -90.00    0       16      0x4
Console#
```

This example shows sample output from the **show controllers efm status profile** command

```
Interface      Link  Uptime    Profile Name          DSRate  USRate  Fail
-------------  ----  --------  --------------------  ------  ------  ----
Ethernet 1/1   Up     0:38:30  default               4.17    1.56    0
Ethernet 1/2   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/3   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/4   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/5   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/6   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/7   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/8   Down   0: 0: 0  default               0.00    0.00    0
```

Related Commands

show controllers efm interface-id actual
show controllers efm interface-id admin

show controllers efm remote ethernet mode

Use this command to display the connected CPE Ethernet mode.

Syntax

show controllers efm remote ethernet mode *interface-id*

interface-id – ID of the VDSL port.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

To obtain the Ethernet mode from CPE side VDSL chip

Examples

```
Console#show controllers efm remote ethernet mode ethernet 1/1
Interface        Speed         Duplex
-------------    ----------    --------
Ethernet 1/1     100               Full
Console#
```

Related Commands

show controllers efm interface-id actual
show controllers efm interface-id admin
show controllers efm status

Rate Limit Commands

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. When a port 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 (global)

Use this command in global configuration mode to set the rate limit. Use the **no** form of this command to return to the default setting.

Syntax

rate-limit input
no rate-limit input

Default Setting

None

Command Mode

Privileged EXEC

Example

```
Console#config
Console(config)#rate-limit input
Console(config)#
```

Related Commands

rate limit (interface)

rate-limit (interface)

Use this command in Interface Configuration mode to configure the rate limit on data received on a specific port. Use the **no** form of this command to return to the default settings. Note that the maximum data rate for VDSL ports depends on the physical link and the selected efm profile (see page 3-147.)

Syntax

rate-limit input *rate*

rate – The *rate* unit is Mbps

Default Setting

Fast Ethernet interface – 100 Mbps
Gigabit Ethernet interface – 1000 Mbps

Command Mode

Interface Configuration

Command Usage

- The *rate* range is:
  - Fast Ethernet interface – 1 to 100 Mbps.
  - Gigabit Ethernet interface – 1 to 1000 Mbps.
- Resolution – the unit increment of *rate* change:
  - Fast Ethernet interface – 1 Mbps.
  - Gigabit Ethernet interface – 8 Mbps

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 10
Console(config-if)#
```

APPENDIX A
TROUBLESHOOTING

Troubleshooting Chart

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. • Be sure that your management station has management VLAN access to the switch (default is VLAN 1). • 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, there may already be four active sessions. 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.

Upgrading Firmware via the Serial Port

The switch contains three firmware components that can be upgraded; the diagnostics (or Boot-ROM) code, the 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 (see "Downloading System Software from a Server" on page 2-17). Downloading large runtime code files via TFTP is normally much faster than downloading via the switch's serial port.

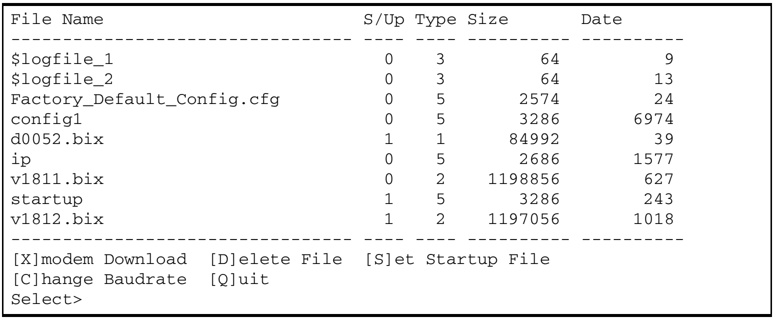
You can upgrade switch firmware by connecting a PC directly to the serial Console port on the switch's front panel and using VT100 terminal emulation software that supports the XModem protocol (see "Required Connections" on page 1-3).

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 the diagnostic test results. Screen text similar to that shown on the following page displays:

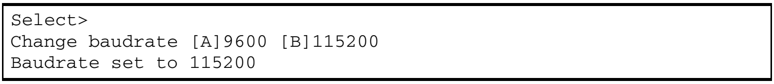


```
File Name                        S/Up Type Size       Date
-------------------------------- ---- ---- ---------- ----------
$logfile_1                          0    3        64          9
$logfile_2                          0    3        64         13
Factory_Default_Config.cfg          0    5      2574         24
config1                             0    5      3286       6974
d0052.bix                           1    1     84992         39
ip                                  0    5      2686       1577
v1811.bix                           0    2   1198856        627
startup                             1    5      3286        243
v1812.bix                           1    2   1197056       1018
-------------------------------- ---- ---- ---------- ----------
[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. There are two baud rate settings available, 9600 and 115200. Using the higher baud rate minimizes the time required to download firmware code files. Press <b> to select the option for 115200 baud.

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. 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 that is not set as the startup file (i.e, the S/Up setting for the file must be set to “0” before it can be deleted).

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 an SMC7724M/VSW binary software file from SMC.

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.

11. Specify a name for the downloaded code file. Filenames are case-sensitive. The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the length of the file name should be 1 to 31 characters. (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 ::
Image downloaded to buffer.


        [R]untime
        [D]iagnostic
        [L]oader (Warning: you sure what you are doing?)
Update Image File:r
Runtime Image Filename : v1812.bix
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.

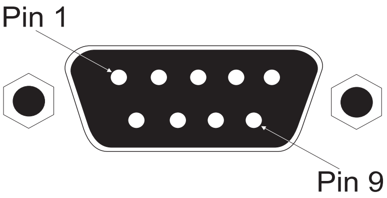
14. Set your PC’s terminal emulation software baud rate back to 9600 baud. Press <Enter> to reset communications with the switch.

15. Press <q> to quit the firmware-download mode and boot the switch.

APPENDIX B
PIN ASSIGNMENTS

Console Port Pin Assignments

The DB-9 serial port on the switch's rear panel is used to connect to the switch for out-of-band console configuration. The onboard menu-driven configuration program can be accessed from a terminal, or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.



DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #
BB	104	**RxD** (Received Data)	2	2
BA	103	**TxD** (Transmitted Data)	3	3
AB	102	**SGND** (Signal Ground)	5	5

No other pins are used.

Console Port to 9-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port
2 RXD	<---------TXD ------------	3 TXD
3 TXD	-----------RXD ---------->	2 RXD
5 SGND	-----------SGND ----------	5 SGND

No other pins are used.

Console Port to 25-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
2 RXD	<---------TXD ------------	2 TXD
3 TXD	-----------RXD ---------->	3 RXD
5 SGND	-----------SGND ----------	7 SGND

No other pins are used.

Glossary

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 UTP cable.

100BASE-FX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two strands of 50/125 or 62.5/125 micron core fiber cable.

1000BASE-SX

IEEE 802.3z specification for Gigabit Ethernet over two strands of 50/125 or 62.5/125 micron core fiber cable.

1000BASE-LX

IEEE 802.3z specification for Gigabit Ethernet over two strands of 9/125 micron core fiber cable.

1000BASE-LH

Gigabit Ethernet over two strands of 9/125 micron core fiber cable.

1000BASE-T

IEEE 802.3ab specification for Gigabit Ethernet over 100-ohm Category 5 or 5e twisted-pair cable (using all four wire pairs).

Auto-negotiation

Signalling method allowing each node to select its optimum operational mode (e.g., 10 Mbps or 100 Mbps and half or full duplex) based on the capabilities of the node to which it is connected.

Bandwidth

The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.

Collision

A condition in which packets transmitted over the cable interfere with each other. Their interference makes both signals unintelligible.

Collision Domain

Single CSMA/CD LAN segment.

Customer Premises Equipment (CPE)

Terminating equipment, such as terminals, phones, and routers installed at customer sites and connected to the service provider's company network.

CSMA/CD

CSMA/CD (Carrier Sense Multiple Access/Collision Detect) is the communication method employed by Ethernet, Fast Ethernet, or Gigabit Ethernet.

End Station

A workstation, server, or other device that does not forward traffic.

Ethernet

A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax, and twisted-pair cable.

Fast Ethernet

A 100 Mbps network communication system based on Ethernet and the CSMA/CD access method.

FTTH

Fibre To The Home: a network where an optical fibre runs to the subscriber's premises or home.

Gigabit Ethernet

A 1000 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Full Duplex

Transmission method that allows two network devices to transmit and receive concurrently, effectively doubling the bandwidth of that link.

IEEE

Institute of Electrical and Electronic Engineers.

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 Fast Ethernet.

IEEE 802.3u

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX 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.

LAN Segment

Separate LAN or collision domain.

LED

Light emitting diode used for monitoring a device or network condition.

Local Area Network (LAN)

A group of interconnected computer and support devices.

Main Distribution Frame (MDF)

The termination equipment where outside telephone lines connect to a building or site

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.

MTU

A building that contains more than a single tenant, such as an apartment block, office complex, or hotel.

Management Information Base (MIB)

Aset of database objects that contains information about the device.

Network Diameter

Wire distance between two end stations in the same collision domain.

Private Branch Exchange (PBX)

A telephone exchange local to a particular organization who use, rather than provide, telephone services.

POTS

Plain Old Telephone Service.

RJ-45 Connector

A connector for twisted-pair wiring.

Splitter

A filter to separate DSL signals from POTS signals to prevent mutual interference.

Straight-through Port

An RJ-45 port which does not cross the receive and transmit signals internally (MDI) so it can be connected with straight-through twisted-pair cable to any device having a crossover port (MDI-X). Also referred to as a "Daisy-Chain" port.

Switched Ports

Ports that are on separate collision domains or LAN segments.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

UTP

Unshielded twisted-pair cable.

VDSL

Very high data rate Digital Subscriber Line: A family of digital telecommunications protocols designed to allow high speed data communication at data rates from below 1 Mbps to 52.8 Mbps with corresponding maximum reach ranging from 4500 feet to 1000 feet of 24 gauge twisted pair cable over the existing copper telephone lines between end-users and telephone companies.

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, allowing users to share information and resources as though located on the same LAN.

INDEX

A

address table 2-33

B

BOOTP 2-12
  for IP configuration 1-4
broadcast storm, threshold 2-30

C

Class of Service
  configuring 2-63
  queue mapping 2-63
community string 2-82
configuration settings, saving or restoring 2-18
connections
  Web browser 1-1
console port
  pin assignments B-1

D

default priority, ingress port 2-63
default settings 1-13
DHCP 2-12
downloading software 2-17, A-2

E

EliteView management software 1-1

F

firmware version, displaying 2-24
firmware, upgrading 2-17
firmware,upgrading A-2

H

hardware version, displaying 2-24

I

IP address
  BOOTP/DHCP service 2-12
  setting 2-11

L

log-in
  Web interface 2-3

M

main menu 2-5
management
  options 1-1
mirror port, configuring 2-31
multicast
  router 2-87, 3-122

P

passwords
  administrator setting 2-14
pin assignments
  25-pin DTE port B-2
pin assignments, console port B-1
port priority
  configuring 2-63
  default ingress 2-63
ports
  configuring 2-26
priority, default port ingress 2-63
problems, troubleshooting A-1

R

RADIUS, configuring logon authentication 2-15
rate limiting, configuration 2-95

S

serial port
  configuring 3-58
  XModem downloads A-2
SNMP
  community string 2-82
  enabling traps 2-83
  trap manager 2-83
SNMP (Simple Network Management Protocol)
  management 1-1
software downloads 2-17, A-2
software version, displaying 2-24
Spanning Tree Protocol 2-37
startup files
  displaying 2-17
  setting 2-17
statistics, switch 2-92
system software
  downloading from server 2-17

T

trap manager 2-83
troubleshooting A-1
trunk
  configuration 2-78

U

upgrading software 2-17, A-2
user password 2-14

V

VLANs
  configuring 2-45

W

Web
  browser connection 1-1
Web interface
  access requirements 2-1
  configuration buttons 2-4
  home page 2-3
  menu list 2-5
  panel display 2-5

X

XModem download A-2

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; (949) 679-8000; Fax: (949) 679-1481
From Europe (8:00 AM - 5:30 PM UK Time)
44 (0) 118 974 8700; Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com
Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads
World Wide Web:
http://www.smc.com/
http://www.smc-europe.com/

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-93-477-4935;	Fax 34-93-477-3774
UK:	44 (0) 118 974 8700;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 02 739 12 33;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Switzerland:	41 (0) 1 9409971;	Fax 41 (0) 1 9409972
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Northern Europe:	44 (0) 118 974 8700;	Fax 44 (0) 118 974 8701
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharan Africa:	27-11 314 1133;	Fax 27-11 314 9133
North Africa:	34 93 477 4920;	Fax 34 93 477 3774
Russia:	7 (095) 290 29 96;	Fax 7 (095) 290 29 96
PRC:	86-10-6235-4958;	Fax 86-10-6235-4962
Taiwan:	886-2-2659-9669;	Fax 886-2-2659-9666
Asia Pacific:	(65) 238 6556;	Fax (65) 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-3-5645-5715;	Fax 81-3-5645-5716
Australia:	61-2-8875-7887;	Fax 61-2-8875-7777
India:	91-22-8204437;	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com or www.smc-europe.com.

SMC®
Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

Model Number: SMC7724M/VSW
Publication Number: 150200022300A
Revision Number: v1.8.2.2 E122002-R01