Dell PowerEdge VRTX Switch Modules R1-2401 and R1-2210 User Guide

Regulatory Model: E12M

Regulatory Type: E12M001, E12M002

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware, or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

March 2014 P/N 5MM18 Rev. A00

Contents

1

Preface

The VRTX Switch Modules R1-2401 and R1-2210 devices are modular switches that are installed in the Dell PowerEdge VRTX chassis.

This guide contains the information needed for installing, configuring, and maintaining these devices through the web-based network administrator. In addition, it describes a subset of the CLI available of the GUI features.

The Dell PowerEdge VRTX Switch Modules R1-2401 and R1-2210 CLI Reference Guides provide additional information about the CLI commands, which can be downloaded from the Dell support website at dell.com/support.

Features

This section describes the features of the R1-2401 and R1-2210 devices.

For a complete list of all updated device features, see the latest software version **Release Notes** at dell.com/support.

This section provides a brief description of the following features:

- IP Version 6 (IPv6) Support
- Head of Line Blocking Prevention
- Back Pressure Support
- Virtual Cable Testing (VCT)
- Auto-Negotiation
- MDI/MDIX Support
- MAC Address Supported Features
- Layer 2 Features
- IGMP Snooping
- MLD Snooping
- Port and VLAN Mirroring
- Broadcast Storm Control
- VLAN Supported Features
- Spanning Tree Protocol Features
- Link Aggregation
- Quality of Service Features
- Device Management Features
- Security Features
- DHCP Server
- Protected Ports
- Proprietary Protocol Filtering
- UDLD

- Static Routing
- IPv6 Router
- sFlow

IP Version 6 (IPv6) Support

The device functions as an IPv6-compliant host, as well as an IPv4 host (also known as dual stack). This enables device operation in a pure IPv6 network as well as in a combined IPv4/IPv6 network.

For more information, see IPv6 Addressing.

Head of Line Blocking Prevention

Head of Line (HOL) blocking results in traffic delays and frame loss caused by traffic competing for the same egress port resources. To prevent HOL blocking, the device queues packets. The packets at the head of the queue are forwarded before packets at the end of the queue.

Back Pressure Support

On half-duplex links, the receiving port prevents buffer overflows by occupying the link so that it is unavailable for additional traffic.

For more information, see Back Pressure.

Virtual Cable Testing (VCT)

VCT detects and reports copper link cabling faults, such as open cables and cable shorts.

For more information, see Diagnostics.

Auto-Negotiation

Auto-negotiation enables the device to advertise modes of operation. The auto-negotiation function enables an exchange of information between two devices that share a point-to-point link segment, and automatically configures both devices to take maximum advantage of their transmission capabilities.

The R1-2401 1Gb and R1-2210 10G VRTX switches enhance auto-negotiation by providing port advertisement. Port advertisement enables the system administrator to configure the port speeds that are advertised.

For more information, see Port Configuration or LAG Configuration.

MDI/MDIX Support

Standard wiring for end stations is known as **Media-Dependent Interface** (MDI), and standard wiring for hubs and switches is known as **Media-Dependent Interface with Crossover** (MDIX).

If auto-negotiation is enabled, the device automatically detects whether the cable connected to an RJ-45 port is MDIX (crossed) or MDI (straight). This enables both types to be used interchangeably.

If auto-negotiation is not enabled, only MDI (straight) cables can be used.

For more information, see MDI/MDIX.

MAC Address Supported Features

MAC Address Capacity Support

The device supports up to 16K MAC addresses and it reserves specific MAC addresses for system use.

Static MAC Entries

MAC entries can be manually entered in the Bridging Table, as an alternative to learning them from incoming frames. These user-defined entries are not subject to aging and are preserved across resets and reboots.

For more information, see Address Tables.

Self-Learning MAC Addresses

The device enables controlled MAC address learning from incoming packets. The MAC addresses are stored in the Bridging Table.

For more information, see Dynamic Address Table.

Automatic Aging for MAC Addresses

MAC addresses from which no traffic is received for a given period, are aged out. This prevents the Bridging Table from overflowing.

For more information, see Dynamic Address Table.

VLAN-Aware MAC-Based Switching

The device always performs VLAN-aware bridging. Classic bridging (IEEE802.1D), in which frames are forwarded based only on their destination MAC address, is not performed. However, a similar functionality can be configured for untagged frames. Frames addressed to a destination MAC address that is not associated with any port are flooded to all ports of the relevant VLAN.

MAC Multicast Support

Multicast service is a limited Broadcast service that enables one-to-many and many-to-many connections for information distribution. In Layer 2 Multicast service, a single frame is addressed to a specific Multicast address, from which copies of the frame are transmitted to the relevant ports. When Multicast groups are statically enabled, you can set the destination port of registered groups, as well as define the behavior of unregistered Multicast frames.

For more information, see Multicast Support.

Layer 2 Features

IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping examines IGMP frame contents, when they are forwarded by the device from work stations to an upstream Multicast router. From the frame, the device identifies work stations configured for Multicast sessions, and which Multicast routers are sending Multicast frames. The IGMP Querier simulates the behavior of a Multicast router. This enables snooping of the Layer 2 Multicast domain even if there is no Multicast router.

For more information, see IGMP Snooping.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping performs the function of IGMP Snooping for IPv6.

For more information, see MLD Snooping.

Port and VLAN Mirroring

Port and VLAN mirroring monitors network traffic by forwarding copies of incoming and outgoing packets from a monitored port to a monitoring port. Users specify which target port receives copies of all traffic passing through a specified source port.

For more information, see Port and VLAN Mirroring.

Broadcast Storm Control

Storm Control enables limiting the number of Multicast and Broadcast frames accepted and forwarded by the device.

When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth and loads all nodes connected on all ports.

For more information, see Storm Control.

VLAN Supported Features

VLAN Support

VLANs are collections of switching ports that comprise a single Broadcast domain. Packets are classified as belonging to a VLAN, based on either the VLAN tag or on a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN.

For more information, see VLANs.

Port-Based Virtual LANs (VLANs)

Port-based VLANs classify incoming packets to VLANs, based on their ingress port.

For more information, see VLAN Membership.

Full 802.1Q VLAN Tagging Compliance

IEEE 802.1Q defines an architecture for virtual, bridged LANs, the services provided in VLANs, and the protocols and algorithms involved in the provision of these services.

For more information, see Overview.

GVRP Support

GARP VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. When GVRP is enabled, the device registers and propagates VLAN membership on all ports that are part of the active underlying Spanning Tree Protocol topology.

For more information, see GVRP Parameters.

Voice VLAN

Voice VLAN enables network administrators to enhance VoIP service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. VoIP traffic has a preconfigured Organizationally Unique Identifiers (OUI) prefix in the source MAC address. Network administrators can configure VLANs from which voice IP traffic is forwarded. Non-VoIP traffic is dropped from the Voice VLAN in Auto-Voice VLAN Secure mode. Voice VLAN also provides QoS to VoIP, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly.

For more information, see Voice VLAN.

Guest VLAN

Guest VLAN provides limited network access to unauthorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access through the Guest VLAN.

For more information, see Dot1x Authentication.

Private VLAN

The Private VLAN feature provides Layer 2 isolation between ports that share the same Broadcast domain, or in other words, it creates a point-to-multipoint Broadcast domain. The ports can be located anywhere in the Layer 2 network.

For more information, see Private VLAN.

Multicast TV VLAN

The Multicast TV VLAN feature provides the ability to supply multicast transmissions to Layer 2-isolated subscribers, without replicating the multicast transmissions for each subscriber VLAN. The subscribers are the only receivers of the multicast transmissions.

For more information, see Multicast TV VLAN.

Spanning Tree Protocol Features

Spanning Tree Protocol (STP)

802.1d Spanning tree is a standard Layer 2 switch requirement that enables bridges to automatically prevent and resolve Layer 2 forwarding loops. Switches exchange configuration messages using specifically-formatted frames, and selectively enable and disable forwarding on ports.

For more information, see Spanning Tree.

Fast Link

STP can take 30–60 seconds to converge. During this time, STP detects possible loops, enabling time for status changes to propagate and for relevant devices to respond. This period of 30-60 seconds is considered too long a response time for many applications. The Fast Link option bypasses this delay, and can be used in network topologies, where forwarding loops do not occur.

For more information on enabling Fast Link for ports and LAGs, see STP Port Settings.

IEEE 802.1w Rapid Spanning Tree

Spanning Tree takes 30–60 seconds for each host to decide whether its ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects uses of network topologies to enable faster convergence, without creating forwarding loops.

For more information, see Spanning Tree.

IEEE 802.1s Multiple Spanning Tree

Multiple Spanning Tree (MSTP) operation maps VLANs into STP instances. MSTP provides a different load balancing scenario. Packets assigned to various VLANs are transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more MSTP bridges by which frames can be transmitted. The standard lets administrators assign VLAN traffic to unique paths.

For more information, see Spanning Tree.

STP BPDU Guard

BPDU Guard is used as a security mechanism, to protect the network from invalid configurations.

BPDU Guard is usually used either when fast link ports (ports connected to clients) are enabled or when the STP feature is disabled. When it is enabled on a port, the port is shut down if a BPDU message is received and an appropriate SNMP trap is generated.

For more information, see Spanning Tree.

Link Aggregation

Up to 32 Aggregated Links may be defined, each with up to eight member ports, to form a single Link Aggregated Group (LAG). This enables:

- Fault tolerance protection from physical link disruption
- Higher bandwidth connections
- Improved bandwidth granularity
- High bandwidth server connectivity

A LAG is composed of ports with the same speed, set to full-duplex operation.

For more information, see LAG Configuration.

Link Aggregation and LACP

LACP uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of devices. LACP automatically determines, configures, binds, and monitors the port binding within the system.

For more information, see Link Aggregation.

BootP and DHCP Clients

DHCP enables additional setup parameters to be received from a network server upon system startup. DHCP service is an on-going process. DHCP is an extension of BootP.

For more information, see IPv6 Addressing.

Quality of Service Features

Class of Service 802.1p Support

The IEEE 802.1p signaling technique is an OSI Layer 2 standard for marking and prioritizing network traffic at the data link/MAC sub-layer. 802.1p traffic is classified and sent to the destination. No bandwidth reservations or limits are established or enforced. 802.1p is a spin-off of the 802.1Q (VLANs) standard. 802.1p establishes eight levels of priority, similar to the IP Precedence IP Header bit-field.

For more information about QoS, see Quality of Service.

Advanced QoS

Frames that match an ACL and were permitted entrance are implicitly labeled with the name of the ACL that permitted their entrance. Advanced mode QoS actions defined in network policies can then be applied to these flows.

The switch can set DSCP values and map IPv6 DSCP to egress queues in the same way it does for IPv4. The switch detects IPv6 frames by the IPv6 ether-type.

For more information about Advanced QoS, see QoS Advanced Mode.

TCP Congestion Avoidance

The TCP Congestion Avoidance feature activates an algorithm that breaks up or prevents TCP global synchronization on a congested node, where the congestion is due to multiple sources sending packets with the same byte count.

For more information, see TCP Congestion Avoidance.

Device Management Features

SNMP Alarms and Trap Logs

The system logs events with severity codes and timestamps. Events are sent as SNMP traps to a Trap Recipient List.

For more information, see SNMP.

SNMP Versions 1, 2, and 3

Simple Network Management Protocol (SNMP) over the UDP/IP protocol controls access to the system. A list of community entries is defined, each consisting of a community string and its access privileges. There are three levels of SNMP security: read-only, read-write, and super. Only a super user can access the Community table.

For more information, see SNMP.

Web-Based Management

Web-based management enables managing the system from any web browser. The system contains an Embedded Web Server (EWS) that serves HTML pages, through which the system can be monitored and configured. The system internally converts web-based input into configuration commands, MIB variable settings, and other management-related settings.

Management IP Address Conflict Notification

This feature validates the uniqueness of the switch's IP address, whether it is assigned manually or through DHCP. If the IP address is not unique, the switch performs actions according to the address type. See IP Addressing.

Configuration File Download and Upload

The device configuration is stored in a configuration file. The configuration file includes both system-wide and port-specific device configuration. The system can display configuration files as a collection of CLI commands that are stored and manipulated as text files.

Auto-Update of Configuration/Image File

This feature facilitates installation of new devices. When you enable the various auto-update options, the device automatically downloads a new image or configuration file when it receives its IP address from a TFTP server, and automatically reboots, using the image or configuration file it received.

For more information, see Auto-Update/Configuration Feature.

TFTP Trivial File Transfer Protocol

The device supports boot image, software, and configuration upload/download via TFTP.

For more information, see File Management.

Remote Monitoring

Remote Monitoring (RMON) is an extension to SNMP that provides comprehensive network traffic monitoring capabilities. RMON is a standard MIB that defines MAC-layer statistics and control objects, enabling real-time information to be captured across the entire network.

For more information, see RMON.

sFlow

The sFlow feature enables collecting statistics using the sFlow sampling technology, based on sFlow V5.

For more information, see sFlow.

Command Line Interface

Command Line Interface (CLI) syntax and semantics conform as much as possible to common, industry standards. CLI is composed of mandatory and optional elements. The CLI interpreter provides command and keyword completion to assist users and save typing.

SYSLOG

Syslog is a protocol that enables event notifications to be sent to a set of remote servers, where they can be stored, examined, and acted upon. The system sends notifications of significant events in real time, and keeps a record of these events for after-the-fact usage.

For more information on SYSLOG, see Logs.

SNTP

The Simple Network Time Protocol (SNTP) assures accurate network Ethernet Switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. Time sources are prioritized by strata. Strata define the distance from the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock.

For more information, see Time Synchronization.

Domain Name System

Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned, the DNS service translates the name into a numeric IP address. For example, www.ipexample.com is translated into 192.87.56.2. DNS servers maintain domain name databases containing their corresponding IP addresses.

For more information, see Domain Name.

802.1ab (LLDP-MED)

The Link Layer Discovery Protocol (LLDP) enables network managers to troubleshoot, and enhances network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing methods for network devices to advertise themselves to other systems, and to store discovered information. The multiple advertisement sets are sent in the packet **Type Length Value**

(TLV) field. LLDP devices must support chassis and port ID advertisement, as well as system name, system ID, system description, and system capability advertisements.

LLDP Media Endpoint Discovery (LLDP-MED) increases network flexibility by enabling various IP systems to co-exist on a single network LLDP. It provides detailed network topology information, emergency call service via IP phone location information, and troubleshooting information.

For more information, see LLDP.

Security Features

SSL

Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates and public and private keys.

Port-Based Authentication (Dot1x)

Port-based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the Remote Authentication Dial-In User Service (RADIUS) server using the Extensible Authentication Protocol (EAP). Dynamic VLAN Assignment (DVA) enables network administrators to automatically assign users to VLANs during the RADIUS server authentication.

For more information, see Dot1x Authentication.

Locked Port Support

Locked Port increases network security by limiting access on a specific port to users with specific MAC addresses. These addresses are either manually defined or learned on that port. When a frame is seen on a locked port, and the frame source MAC address is not tied to that port, the protection mechanism is invoked.

For more information, see Port Security.

RADIUS Client

RADIUS is a client/server-based protocol. A RADIUS server maintains a user database that contains per-user authentication information, such as user name, password, and accounting information.

RADIUS Accounting

This feature enables recording device management sessions (Telnet, serial, and WEB but not SNMP) and/or 802.1x authentication sessions.

Due to the complexity of 802.1x setup and configuration, many mistakes can be made that might cause loss of connectivity or incorrect behavior. The 802.1x Monitor mode enables applying 802.1x functionality to the switch, with all necessary RADIUS and/or domain servers active, without actually taking any action that may cause unexpected behavior. In this way, the user can test the 802.1x setup before actually applying it.

For more information, see RADIUS.

SSH

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH version 2 is currently supported. The SSH server feature enables an SSH client to establish a secure, encrypted connection with a device. This connection provides functionality that is similar to an inbound telnet connection. SSH uses RSA and DSA Public Key cryptography for device connections and authentication.

For more information, see Security Management and Password Configuration.

TACACS+

TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized, user management system, while still retaining consistency with RADIUS and other authentication processes.

For more information, see TACACS+.

Password Management

Password management provides increased network security and improved password control. Passwords for SSH, Telnet, HTTP, HTTPS, and SNMP access are assigned security features.

The switch provides the ability to demand strong passwords, meaning that they must contain both upper and lower-case letters, numbers, and punctuation marks.

For more information, see Password Management.

Access Control Lists (ACL)

Access Control Lists (ACL) enable network managers to define classification actions and rules for specific ingress ports. Packets entering an ingress port with an active ACL, are either admitted or denied entry and the ingress port is disabled. If they are denied entry, the user can disable the port.

For more information, see Password Management

Dynamic ACL/Dynamic Policy Assignment (DACL/DPA)

The network administrator can specify the user's ACL in the RADIUS server. After successful authentication, the user is assigned that ACL.

For more information, see ACLs.

DHCP Snooping

DHCP Snooping expands network security by providing firewall security between untrusted interfaces and DHCP servers. By enabling DHCP Snooping, network administrators can differentiate between trusted interfaces connected to end-users or DHCP servers and untrusted interfaces located beyond the network firewall.

For more information, see DHCP Snooping.

DHCP Relay

The device can act as a DHCP Relay agent that listens for DHCP messages, and relays them between DHCP servers and clients, which reside in different VLANs or IP subnets.

For more information, see DHCP Relay.

ARP Inspection

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

For more information, see Dynamic ARP Inspection.

Port Profile (CLI Macro)

Macros provide a convenient way to save and share a common configuration. A macro is a set of CLI commands with a unique name. When a macro is applied to a port, the CLI commands contained within it are executed and added to the Running Configuration file.

For more information, see Port Profile.

Protected Ports

The Protected Ports feature provides Layer 2 isolation between interfaces (Ethernet ports and LAGs) that share the same Broadcast domain (VLAN) with other interfaces.

For more information, see Protected Ports.

Proprietary Protocol Filtering

This feature enables user control over the filtering of packets with proprietary protocols such as CDP, VTP, DTP, UDLD, PaGP, and SSTP. The user can select any combination of the protocols to be filtered, for example: CDP and VTP.

For more information, see Proprietary Protocol Filtering.

UDLD

UDLD complements the Spanning Tree Protocol which is used to eliminate switching loops

For more information, see UDLD.

Static Routing

Static routing enables the user to define a routing table manually.

For more information, see IPv4 Routes Table (Advanced Mode).

IPv6 Router

For more information, see IPv6 Router.

3

Hardware Overview

This section describes the device hardware.

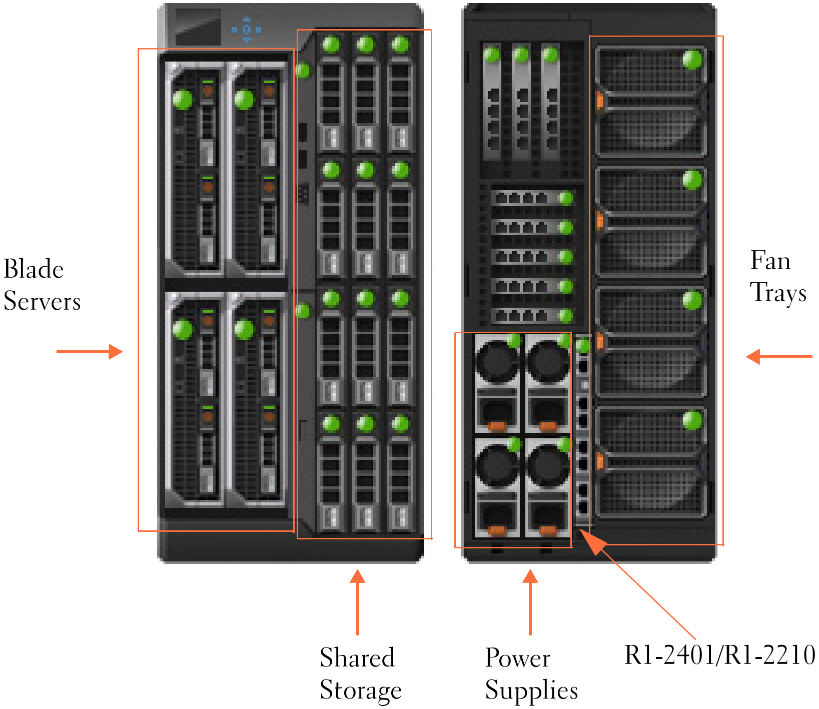
It contains the following topics:

- Switch Layout
- Ports
- Front Panel LEDs

Switch Layout

Figure 3-1 shows the R1-2401/R1-2210 devices within the chassis.

Figure 3-1. R1-2401/R1-2210



Ports

The devices have five groups of ports, numbered 0-4. Group 0 contains the external ports and groups 1-4 contain the internal ports that are connected to blade servers 1-4.

The following naming convention is used for internal and external ports:

- 1G Ethernet Ports:

  gigabitethernet *group*/*port_number* or gi *group*/*port_number*

- 10G Ethernet Ports:

  tengigabitethernet *group/port_number* or te *group/port_number*

In addition, the switch supports an Out-of-Band (OOB) port that is connected to the management network of the chassis.

Port Types

The following ports are found on the R1-2401 switch:

- **24 x 1G Ethernet Ports.** These consist of:
  - 8 **external ports**—Connected to network (visible when the switch is in the chassis)
  - **16 internal ports**—Connected to blade servers (not visible when the switch is in the chassis)
- **1 Out-of-Band port** (this port is the same as used for CMC)

The following ports are found on the R1-2210 switch:

- **20 x 10G Ethernet Ports.** These consist of:
  - **4 external ports**—Connected to network (visible when the switch is in the chassis)
  - **16 internal ports**—Connected to blade servers (not visible when the switch is in the chassis)
- **2 x 1G Ethernet Ports**
- **1 Out-of-Band port** (this port is the same as used for CMC)

Table 3-1 and Table 3-2 map the hardware network port numbers to the software interface port numbers and describe the short version of the port name in the CLI/GUI for the R1-2401 and the R1-2210, respectively:

Table 3-1. R1-2401 Port Mapping Table

Port Type and Number	Software Port Naming Convention in CLI/WEB
External 1G ports 1-8/server slot 0	gi0/1.... gi0/8
Internal 1G ports 1-4/server slot 1	gi1/1.... gi1/4
Internal 1G ports 5-8/server slot 2	gi2/1.... gi2/4
Internal 1G ports 9-12/server slot 3	gi3/1.... gi3/4

Table 3-1. R1-2401 Port Mapping Table

Port Type and Number	Software Port Naming Convention in CLI/WEB
Internal 1G ports 13-16/server slot 4	gi4/1.... gi4/4
Out-of-Band port	oob

Table 3-2. R1-2210 Port Mapping Table

Port Type and Number	Software Port Naming Convention in CLI/WEB
External 10G ports 1-4/server slot 0	te0/1.... te0/4
External 1G ports 1-2/server slot 0	gi0/1.... gi0/2
Internal 10G ports 1-4/server slot 1	te1/1.... te1/4
Internal 10G ports 5-8/server slot 2	te2/1.... te2/4
Internal 10G ports 9-12/server slot 3	te3/1.... te3/4
Internal 10G ports 13-16/server slot 4	te4/1.... te4/4
Out-of-Band port	oob

Front Panel LEDs

The front panels of both devices contain the following LEDs:

- Status and Power LEDs, described in Table 3-3.
- LEDs associated with external ports, described in Table 3-4 and Table 3-5.

Table 3-3. System LEDs on R1-2401 and R1-2210

State of Switch	Status LED	Power LED (Green)	Description
Off	Off	Off	Switch is powered-off.
Healthy/Booted	Blue	On	Switch is functionally normally.
Fault	Amber Blink 1 HZ	On — Self-diagnosed fault Off — Configuration error or other CMC-detected fault	Switch has issued a fault.

Table 3-3. System LEDs on R1-2401 and R1-2210

State of Switch	Status LED	Power LED (Green)	Description
Booting	Off	On	Boot in progress.
Identify	Blue Blink 1 HZ	On	CMC is identifying the switch

Table 3-4. R1-2401 External Port LEDs

LED	Color
Link	**Off** — No link **Solid green** — Link at 1G speed **Solid amber** — Link at 10/100M speed
Activity	**Off** — No link **Blinking green** — Traffic is being received/forward

Table 3-5. R1-2210 External Port LEDs

LED	Color
1G Link	**Off** — No link **Solid green** — Link at 1G speed **Solid amber** — Link at 10/100M speed
1G Activity	**Off** — No link **Blinking green** — Traffic is being received/forward
10G Link and Activity	**Off** — No link **Solid green** — Link is up **Blinking green** — Traffic is being received/forward

4

Initial Configuration of the Switch

This section describes how to initially configure the Dell VRTX 1Gb and 10Gb switch modules.

NOTE: Before proceeding further, read the latest documentation and release notes for this product, which can be downloaded from the Dell Support website at dell.com/support.

To logon to the switch after it is inserted into the chassis, perform the following:

1 Turn on the chassis. To display the IP address configured for the out-of-band interface, go to the CMC GUI, options: **I/O Module Overview > Setup.** See the *CMC User Guide* for further information on how to access the CMC GUI.

2 Log on to the switch in one of the following ways:

- Establish a Telnet session to the out-of-band IP address obtained in the last step, and log on with the default user/password: **root/calvin**. Continue managing the switch through the CLI (see the *Dell PowerEdge VRTX Switch Modules, R1-2401 and R1-2210 CLI Reference Guides*).
- Open a GUI session from the CMC GUI, options: **I/O Module Overview > Properties > Launch IOM GUI**. In the Login menu, select either Basic or Advanced mode and use the default user/password: **root/calvin**. Continue managing the switch through the Network Administrator.
- Connect to the IOM serial interface through the CMC. For that, use the CMC command: **connect switch**. See the *CMC Command Line Reference* from dell.com/support.

Table 4-1 describes the major switch defaults:

Table 4-1. Major System Defaults

Feature	Defaults
SNMP	Enabled. SNMP version: V3. SNMP Local Engine ID: 0000000001. SNMP Notifications: Enabled.
Login and Authentication	Telnet authentication login is from the local user data base. HTTP authentication login is from the local data base. HTTPS authentication login is from the local data base.
Authentication Servers	No RADIUS server is defined. No TACACS server is defined.
Logging	No SYSLOG server is defined.
System Time	SNTP is supported.
DHCP	DHCP server is disabled. DHCP auto configuration is enabled.
Ports	24 GE BaseT ports (for VRTX 1Gb). 20 10G copper fiber ports plus 2 GE BaseT ports (for VRTX 10Gb). Full duplex is enabled. Negotiation is enabled. Flow control is Off. No LAGs are defined.
Multicast	Multicast filtering is disabled.
IGMP Snooping	Disabled
MLD Snooping	Disabled
Spanning Tree	Enabled
VLANs	Default VLAN is enabled. Default VLAN ID is 1.

Table 4-1. Major System Defaults

Feature	Defaults
Default IP Address	DHCP enabled by default; If DHCP is disabled, the default IP address of 192.168.2.1 over the OOB interface is used.
Default system mode (for VRTX 1Gb only)	Layer 2

NOTE: CLI and/or GUI need only be used if the default configuration is not sufficient.

The switch can be configured in the following modes from the GUI:

- **Basic** — Elementary network configuration for the switch.
- **Advanced** — Full network configuration mode that enables configuration of all switch capabilities. This mode is intended for advanced network administrators.

5

Using the CLI

This section describes how to perform various configuration operations through the Command Line Interface CLI.

It includes the following topics:

- Using the CLI
- CLI Command Conventions
- Accessing the Device Through the CLI
- Retrieving an IP Address
- Security Management and Password Configuration
- Configuring Login Banners
- Startup Menu Procedures
- Software Download

Using the CLI

This section provides some general information for using the CLI.

For a complete description of CLI commands, refer to the *Dell PowerEdge VRTX Switch Module CLI Reference Guide*.

Command Mode Overview

The CLI is divided into command modes, each with a specific command set. Entering a question mark at the terminal prompt displays a list of commands available for that particular command mode.

In each mode, a specific command is used to navigate from one mode to another.

These modes are described below.

User EXEC Mode

During CLI session initialization, the CLI is in User EXEC mode. Only a limited subset of commands is available in User EXEC mode. This level is reserved for tasks that do not change the terminal configuration and is used to access configuration sub-systems.

After logging into the device, User EXEC command mode is enabled. The user-level prompt consists of the host name followed by the angle bracket (>). For example: `console>`

NOTE: The default host name is `console` unless it has been modified during initial configuration.

The User EXEC commands enable connecting to remote devices, changing terminal settings on a temporary basis, performing basic tests, and listing system information.

To list the User EXEC commands, enter a question mark at the command prompt.

To enter the next level, Privileged EXEC mode, a password is required (if configured).

Privileged EXEC Mode

Privileged EXEC mode provides access to the device global configuration.

Privileged access can be protected, to prevent unauthorized access and to secure operating parameters. Passwords are displayed on the screen, and are case-sensitive.

NOTE: The enable command is only necessary if you login with privilege level less than 15.

To access and list the Privileged EXEC mode commands:

1 At the prompt type **enable** and press **<Enter>**.

2 When a password prompt displays, enter the password and press **<Enter>**.

The Privileged EXEC mode prompt displays as the device host name followed by #. For example: `console#`

To list the Privileged EXEC commands, type a question mark at the command prompt.

To return from Privileged EXEC mode to User EXEC mode, type **disable** and press **<Enter>**.

The following example illustrates accessing privileged EXEC mode and then returning to the User EXEC mode:

```
console> enable
Enter Password: ******
console#
console# disable
console>
```

Use the **exit** command to return to a previous mode.

To configure the device, enter the next level, Global Configuration mode.

Global Configuration Mode

The Global Configuration mode manages device configuration on a global level. Global Configuration commands apply to system features, rather than a specific protocol or interface.

To access Global Configuration mode, at the Privileged EXEC Mode prompt, type **configure** and press **<Enter>**. The Global Configuration mode displays as the device host name followed by **(config)** and the pound sign **#**:

```
console# configure
console(config)#
```

To list the Global Configuration commands, enter a question mark at the command prompt.

The following example illustrates how to access Global Configuration mode and return back to the Privileged EXEC mode:

```
console#
console# configure
console(config)# exit
console#
```

Interface Configuration Mode

The Interface Configuration mode configures the device at the physical interface level (port, VLAN, or LAG). Interface commands that require subcommands have another level, called the Subinterface Configuration mode. A password is not required to access this level.

The following example places the CLI in Interface Configuration mode on port gi0/1. The **sntp** command is then applied to that port.

```
console# configure
console(config)# interface gi0/1
console(config-if)# sntp client enable
```

To run a command in a mode, which does not contain it, use "**do**" before the command, as in the following example:

```
console# configure
console(config)# interface gi0/1
console(config-if)# sntp client enable
console(config-if)# do show sntp configuration
```

CLI Command Conventions

There are certain command entry conventions that apply to all commands. The following table describes these conventions.

Table 5-1. Common GUI Elements

Button	Description
[ ]	In a command line, square brackets indicate an optional entry.
{ }	In a command line, curly brackets indicate a mandatory parameter. A selection of mandatory parameters is separated by the | (or) character. One option must be selected. For example: **flowcontrol** {**auto**|**on**|**off**} means that for the flowcontrol command either auto, on, or off must be selected.
Italic Font	Indicates a parameter value.
Bold Italic Font	Indicates a parameter key word.

Button	Description
<button-name>	Any individual key on the keyboard. For example click **<Enter>**.
Ctrl+F4	Any combination of keys clicked simultaneously, for example: **Ctrl** and **F4**.
Screen Display	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and **all** is an option, the default for the command is **all** when no parameters are defined. For example, the command **interface range port-channel** has the option of either entering a range of channels, or selecting **all**. When the command is entered without a parameter, it automatically defaults to **all**.

Accessing the Device Through the CLI

You can manage the device using CLI commands, through the CMC connected to the terminal console, or via a Telnet connection.

Through CMC

To manage the device through the CMC:

1. Insert the device into the chassis.
2. Log into the CMC console.
3. Use the command `connect switch` to gain access to the switch console.

See the *Dell Chassis Management Controller User Guide* for VRTX.

Telnet Connection

The device supports up to four simultaneous Telnet sessions. All CLI commands can be used over a Telnet session.

Retrieving an IP Address

By default, the switch receives its IP address dynamically via a DHCP server for the OOB port interface, although it can also be configured statically. If the DHCP server is not accessible, the OOB uses the default IP address 192.168.2.1. After a static or DHCP IP address is assigned on the OOB interface, the default IP address is removed. The in-band IP address can also be received from a DHCP server or configured statically. This IP address can be removed at any time.

Receiving an In-Band IP Address from a DHCP Server

When using the DHCP protocol to retrieve an IP address, the device acts as a DHCP client. When the device is reset, the DHCP command is saved in the configuration file, but the IP address is not.

To retrieve an IP address from a DHCP server, perform the following steps:

1. Select and connect any port to a DHCP server or to a subnet that has a DHCP server on it.
2. Type the following commands to use the selected port for receiving the IP address:

   a. Assigning dynamic IP Addresses on a port:

   ```
   console# configure
   console(config)# interface gi0/1
   console(config-if)# ip address dhcp
   ```

   b. Assigning a dynamic IP Addresses on a VLAN:

   ```
   console# configure
   console(config)# interface vlan 1
   console(config-if)# ip address dhcp
   ```

   The interface receives the IP address automatically.

3 Type the following to verify the IP address:

```
console# show ip interface
IP Address       I/F  I/F Status Type Directed   Precedence     Status
                      admin/oper      Broadcast
----------------------------------------------------------------------
0.0.0.0/32       oob    UP/DOWN DHCP disable    No       Not received
10.5.229.113/27 vlan 1 UP/UP   DHCP disable    No       Valid
```

When configuring/receiving IP addresses through DHCP, the configuration received from these servers includes the IP address and may include the subnet mask and default gateway.

NOTE: It is not necessary to delete the device configuration to retrieve an IP address from the DHCP server.

NOTE: When copying configuration files, avoid using a configuration file that contains an instruction to enable DHCP on an interface that connects to the same DHCP server, or to one with an identical configuration. In this instance, the device retrieves the new configuration file and boots from it. The device then enables DHCP, as instructed in the new configuration file, and the DHCP instructs it to reload the same file.

Security Management and Password Configuration

System security is handled through the Authentication, Authorization, and Accounting (AAA) mechanism that manages user access rights, privileges, and management methods. AAA uses both local and remote user databases. Data encryption is handled through the SSH mechanism.

Passwords can be configured for the following services:

- Terminal
- Telnet
- SSH
- HTTP
- HTTPS

NOTE: When creating a user name, the default priority is 1, which provides access but not configuration rights. A priority of 15 must be set to enable access and configuration rights to the device. Although user names can be assigned privilege level 15 without a password, it is recommended to always assign a password. If there is no specified password, privileged users can access the Web interface with any password.

NOTE: Passwords can be secured by using password management commands to force aging out of passwords, or expiration of passwords. For more information, see Management Security.

Password Recovery

The system is delivered with a default username/password (root/calvin). If a user-defined password is lost, there are several password recovery procedures that can be invoked. These procedures are applicable for the local terminal only and enable a single access to the device from the local terminal with no password entered.

The retention of the device user configuration after password recovery can be enabled/disabled through the CLI command: `service password-recovery.`

This affects password recovery in the following way:

- **Enabled (default):** When the password-recovery mechanism is invoked, one-time access to the device without a password is enabled and all configuration and user files are retained.
- **Disabled:** When the password-recovery mechanism is invoked, one-time access to the device without a password is stilled enabled, however all configuration files (startup and backups) are removed and the following log message is generated to the terminal after boot process completed: “All configuration and user files were removed”

Through the CMC

To perform password recovery through the CMC perform the following:

1. Login to the CMC console CLI.
2. Execute command `racadm racresetcfg -m switch-1`

The switch is now restored to the default configuration using default settings on the next boot.

NOTE: When using this option, the switch configuration will be restored to factory default configuration.

Through the Startup Menu

To enter the switch without a password through the Setup Menu, see Password Recovery Procedure [3].

Configuring Initial Passwords

Initial Telnet Password

To configure an initial Telnet password, enter the following commands:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password bob
```

Initial SSH Password

To configure an initial SSH password, enter the following commands:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line ssh
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password jones
```

Initial HTTP Password

To configure an initial HTTP password, enter the following commands:

```
console(config)# ip http authentication aaa login-authentication local
console(config)# username admin password user1 privilege 15
```

Initial HTTPS Password

To configure an initial HTTPS password, enter the following commands:

```
console(config)# ip http authentication aaa login-authentication local
console(config)# username admin password user1 privilege 15
```

Enter the following commands once when configuring use of a terminal, a Telnet, or an SSH session, for an HTTPS session.

NOTE: In the Web browser, enable SSL 2.0 or greater for the page content to be displayed..

```
console(config)# crypto certificate 1 generate key-generate
console(config)# ip http secure-server
```

NOTE: HTTP and HTTPS services require privilege level 15 and connect directly to the configuration-level access.

Configuring Login Banners

Banners can be defined for each line, such as console and telnet or for all lines. They are disabled by default.

The following types of banners can be defined:

- **Message-of-the-Day Banner (motd)** — Displayed when the user connects to the device, before login. The following defines a message-of-the-day for the console:

```
console# configure
console(config)# line console
console(config-line)# motd-banner
console(config-line)# exit
console (config)# banner motd *
Welcome*
console# do show banner motd
Banner: MOTD
Welcome
console(config)#
```

- **Login Banner** — Displayed after the Message-of-the-Day Banner, and before the user has logged in. The following defines a login banner for the console:

```
console# configure
console(config)# line console
console(config-line)# login-banner
console(config-line)# exit
console (config)# banner login *
Please log in*
console# do show banner login
Banner: Login
Please log in
console(config)#
```

- **Exec Banner** — Displayed after successful login (in all privileged levels and in all authentication methods). The following defines an exec banner for the console:

```
console# configure
console(config)# line console
console(config-line)# exec-banner
console(config-line)# exit
console (config)# banner exec *
Successfully logged in*
Would you like to enable this banner to all lines? (Y/N)[Y] Y
console# do show banner exec
Banner: Exec
Successfully logged in
console(config)#
```

Startup Menu Procedures

The **Startup** menu enables performing various tasks, such as software download, flash handling and password recovery.

You can enter the **Startup** menu when booting the device. User input must be entered immediately after the POST test.

To enter the **Startup** menu:

1. On the R1-2401, login to the CMC console CLI. On the R1-2210, connect to the external UART (console).
2. On the R1-2401, enter command `connect switch-1`. This step is not necessary for the R1-2210.
3. Login to the switch console CLI prompt.
4. Type **reload** and select **Y** to continue. The switch reloads.
5. When the prompt: `Autoboot in 2 seconds - press RETURN or ESC to abort displays`, press RETURN or ESC. The boot menu will now display.

   The following menu is displayed:

```
[1]Download Software
[2]Erase Flash File
[3]Password Recovery Procedure
[4]Set Terminal Baud-Rate
[5]Back
```

The sections below describe the available Startup menu options.

NOTE: When selecting an option from the Startup menu, take the time-out interval into account. If no selection is made within 10 seconds (default), the device times out. This default value can be changed through the CLI.

Download Software - Option`[1]`

The software download procedure is used to replace corrupted files or upgrade system software, when the device does not have IP connectivity or when both software images of the device are corrupted and therefore you cannot use the web-based management system.

NOTE: Dell recommends that before loading via xmodem, the baud rate of the device and terminal be set to 115200.

To download software through the Startup menu:

1. From the Startup menu, `press [1]`. The following prompt is displayed:

```
Downloading code using XMODEM
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

2. When using the HyperTerminal, click **Transfer** on the HyperTerminal Menu Bar and select **Send File**.
3. In the **Filename** field, enter the file path for the file to be downloaded.
4. Ensure that the Xmodem protocol is selected in the **Protocol** field.
5. Press **Send**. The software is downloaded.

NOTE: After software download, the device reboots automatically.

Erase FLASH File - Option`[2]`

In some cases, the device Startup Configuration file must be erased. If the configuration is erased, all parameters configured via CLI, web-management or SNMP must be reconfigured.

To erase the device configuration in the Startup Configuration file:

1. From the Startup menu, `select [2]`. The following message is displayed:

   `Warning! About to erase a Flash file.`

   `Are you sure (Y/N)?`

2. Press **Y**. The following message is displayed.

   `Write Flash file name (Up to 8 characters, Enter for none.):`

3. Enter **config** ("config" is the standard name for the Startup configuration file although you can use any name).

   The following is displayed:

```
File config (if present) will be erased after system initialization
======== Press Enter To Continue ========
```

The configuration is erased when the system is reset.

Password Recovery Procedure [3]

The following describe how to access the switch if a user-defined password has been lost.

To perform password recovery through the Startup menu perform the following:

1. From the Startup menu select option `[3] Password Recovery and Enter`. Selecting **Enter** causes the request for the current password to be ignored after the boot continues.
2. Select `[5] Back.`
3. The boot process continues and ignores the password prompt.
4. Update password.

NOTE: If the **service password-recovery** command is enabled, all device configuration is retained. If the **service password-recovery** command is disabled, the switch is restored to the default configuration and uses default settings on the next boot.

Set Terminal Baud-Rate - Option [4]

To set the terminal baud-rate:

1. Type `[4]` and press **<Enter>**.
2. Enter the new baud rate. The following is displayed:

```
Set new device baud-rate: 38,400
```

NOTE: After this step, your terminal will no longer respond. Adjust your terminal speed to the configured one.

Software Download

This section contains instructions for downloading device software (system and boot images) through a TFTP server. The TFTP server must be configured before downloading the software.

System Image Download

When the device boots, it decompresses the system image from the flash memory area and runs it. When a new image is downloaded, it is saved in the secondary area allocated for the alternative system image copy.

On the next boot, the device decompresses and runs the image from the currently-active system image.

A system image can be downloaded through a TFTP server.

To download the system image from a TFTP server, ensure that an IP address is configured on the device and pings can be sent to the TFTP server. In addition, ensure that the file to be downloaded is saved on that TFTP server.

To download a system image through the TFTP server:

1 Enter the **show version** command, to verify which software version is currently running on the device. The following is an example of the information that is displayed:

```
console# show version
SW version    1.0.0.17 ( date  05-Sep-2012 time  12:05:41 )
Boot version  1.0.0.2  ( date  22-Aug-2012 time  15:56:52 )
HW version
console#
```

2 Enter the **show bootvar** command, to verify which system image is currently active. The following is an example of the information that is displayed:

```
console# show bootvar
Image  Filename   Version    Date                  Status
-----  ---------  ---------  --------------------  ------
1      image-1    1.0.0.13   04-Aug-2010  08:27:30  Active*
2      image-2    1.0.0.12   29-Jul-2010  17:02:26  Not active
console#
```

3 To copy a new system image to the device:

```
copy tftp://{tftp address}/{file name} image
```

4 When the new image is downloaded, it is saved in the area allocated for the alternative copy of the system image (image-2, as shown in the example). The following is an example of the information that is displayed:

```
console# copy tftp://176.215.31.3/r2401-100048.ros image
Accessing file ‘r2401-100048’ on 176.215.31.3Ö
Loading r2401-100048 from 176.215.31.3:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Exclamation symbols indicate that a copying process is in progress. Each symbol (!) corresponds to 512 bytes transferred successfully. A period indicates that the copying process is timed out. Many periods in a row indicate that the copying process failed.

5 Select the image for the next boot by entering the **boot system** command. After this command, enter the **show bootvar** command to verify that the copy indicated as a parameter in the **boot system** command is selected for the next boot.

The following is an example of the information that is displayed:

```
console# boot system image-2
console# show bootvar
IImage  Filename   Version    Date                   Status
-----  ---------  ---------  --------------------  ------
1      image-1    1.0.0.13   04-Aug-2010  08:27:30  Active
2      image-2    1.0.0.12   29-Jul-2010  17:02:26  Not active*
"*" designates that the image was selected for the next boot
```

If the image for the next boot has not been selected by entering **boot system**, the system boots from the currently active image.

6 To load the new image, enter **reload**. The following message is displayed:

```
console# reload
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

7 Enter **Y**. The device reboots with the new image.

Boot Image Download

Loading a new boot image from the TFTP server, updates the boot image. The boot image is loaded when the device is powered on. A user has no control over the boot image copies.

To download a boot image through the TFTP server:

1 Enter the **show version** command to verify which software version is currently running on the device. The following is an example of the information that is displayed:

```
console# show version
SW version    1.0.0.17 ( date  05-Sep-2012 time  12:05:41 )
Boot version    1.0.0.2 ( date  22-Aug-2012 time  15:56:52 )
HW version
```

2 Enter the **copy** {**tftp://**}{*tftp address*}/{*file name*} **boot** command to copy the boot image to the device. The following is an example of the information that is displayed:

```
console# copy tftp://50.1.1.7/r2401-boot-1009.rfb boot
01-Oct-2006 11:57:35 %COPY-I-FILECPY: Files Copy - source URL
tftp://50.1.1.7/r2401-1009.rfb destination URL flash://boot
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
01-Sep-2010 11:57:38 %INIT-I-Startup: Cold Startup
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
01-Sep-2010 11:59:05 %COPY-N-: The copy operation was completed
successfully!
Copy: 522288 bytes copied in 00:01:30 [hh:mm:ss]
```

3 Enter the **reload** command. The following message is displayed:

```
console# reload
This command will reset the whole system and disconnect your current
session. Do you want to continue (Y/N) [N]?
```

4 Enter **Y.** The device reboots.

6

Network Administrator

This section describes how to manage the R1-2401 and R1-2210 devices using the web-based Network Administrator.

It contains the following topics:

- Starting the Application
- Understanding the Interface
- Using the Network Administrator Buttons
- Field Definitions
- Common GUI Features
- GUI Terms

Starting the Application

NOTE: Before starting the application the IP address must be defined. For more information, see Accessing the Device Through the CLI.

1. Open the CMC GUI.
2. Press the **Launch IOM GUI** button.
3. Enter a user name and password.

NOTE: Passwords are both case sensitive and alpha-numeric.

4. Click **OK**.

   The **Network Administrator** home page is displayed.

Understanding the Interface

The home page contains the following views:

- **Tree view** — Located on the left side of the home page, the tree view provides an expandable view of the features and their components. The branches in the tree view can be expanded to view all the components under a specific feature, or closed to hide the feature's components. By dragging the vertical bar to the right, the tree area can be expanded to display the full name of a component.

- **Components List** — Located in the bottom center of the home page, contains a list of the feature components. When a feature is expanded, the GUI page for that feature is displayed.
- **Information Buttons**— Located at the top of the home page, provide access to information about the device and access to Dell Support. For more information, see Information Buttons.

Device Representation

The graphic display on the home page displays port and system LEDS that specify whether a specific port is currently active.

See Ports.

To configure a port double-click on its icon.

Using the Network Administrator Buttons

This section describes the buttons found on the Network Administrator interface.

Information Buttons

Table 6-1 describes the information buttons that provide access to online support and online help, as well as information about the Network Administrator interfaces. These are displayed at the top of each page.

Table 6-1. Information Buttons

Button	Description
Mode	You are either in Basic or Advanced mode according to your user privileges. Basic mode has a subset of the features available. Advanced mode has all features available.
Support	Opens the Dell Support page at **dell.com/support**
About	Contains the version and build number and Dell copyright information.
Logout	Opens the Log Out window.

Device Management Icons

Table 6-2 describes the device management buttons.

Table 6-2. Device Management Icons

Button	Icon	Description
Apply&Save	💾	Saves changes to the Running and Startup Configuration files.
Help	?	Open online help. The online help pages are context-sensitive. For example, if the **IP Addressing** page is open, the help topic for that page is displayed when **Help** is clicked.
Print	🖨	Prints the **Network Management System** page and/or table information.
Refresh	↻	Refreshes device information from the Running Configuration file.

Field Definitions

Fields that are user-defined can contain between 1–159 characters, unless otherwise noted on the Network Administrator web page. All letters or characters can be used, except the following: "\/ : * ? < >"

Common GUI Features

Table 6-3 describes the common functions that can be performed on many GUI pages.

Table 6-3. Common GUI Elements

Button	Description
Apply	Save changes entered in GUI page to the Running Configuration file.
Back	Go to previous page.
Cancel	Cancel changes entered in GUI page.
Clear All Counters	Delete counters.
Clear Counters	Delete selected counters.
Clear Log	Delete entries from log.
Clear Statistics	Delete statistics.
Copy parameters from	Copy the parameters from a selected row to the selected target rows.
Copy parameters from port	Copy the parameters from a selected port to the selected target ports.
Details	Shows further details relevant to the current page.
Next	Go to next page.
Query	Run a query after query criteria have been entered.
Remove	Remove checked elements in the page. If **Select All** is selected, all elements are removed.
Reset All Counters	Delete all counters.
Restore Defaults	Restores parameters entered in page to default values.
Telnet	Opens a Telnet window. This only works in the Explorer 6 and Firefox browsers.

GUI Terms

Each GUI page in the tree view is described in the following sections. A brief introduction is provided along with steps specifying how to enter information in the page. The following terms are used:

- **Enter** — Indicates that information may be entered in the field. It does not imply that the field is mandatory.
- **Select** — Indicates that information may be selected from a drop-down list or from radio buttons.
- **Displays** — Indicates that the field is display only.

7

Configuring System Information

This section describes how to set system parameters, such as security features, switch software, system time, logging parameters and more.

It contains the following topics:

- General
- Time Synchronization
- Logs
- IPv4 Addressing
- IPv6 Addressing
- Domain Name
- Diagnostics
- Management Security
- SNMP
- File Management
- sFlow

General

This section describes how to view and set general switch parameters.

It contains the following topics:

- Asset Information
- System Health
- System Routing Mode

Asset Information

Use the **Asset** page to view and configure general device information, including the system name, location, contact, system MAC Address, System Object ID, date, time, and system up time.

To configure general device parameters:

1 Click **System** > **General** > **Asset** in the tree view to display the **Asset** page.

2 Enter/view the parameters:

- **System Name (0-159 Characters)** — Enter the user-defined device name.
- **System Contact (0-159 Characters)** — Enter the name of the contact person.
- **System Location (0-159 Characters)** — Enter the location where the system is currently running.
- **MAC Address** — Displays the device MAC address.
- **OOB MAC Address** — Displays the MAC address of the Out-of-Band port.
- **Sys Object ID** — Displays the vendor's authoritative identification of the network management subsystem contained in the entity.
- **Date** — Enter the current date (mandatory). This date can also be entered in the **Manual Time Settings** page. If SNTP has been defined, but the SNTP server is not available, the switch uses the date and time in this field and the **Time** field.
- **Time** — Enter the current time (mandatory). This time can also be entered in the **Manual Time Settings** page. If SNTP has been defined, but the SNTP server is not available, the switch uses the date and time in this field and the **Date** field.
- **System Up Time** — Displays the amount of time since the last device reset.
- **Service Tag** — Displays the service reference number used when servicing the device.
- **Asset Tag** — Enter the **Asset Tag (0-16 Characters)** for the device. This is the user-defined reference for the device.
- **Serial No.** — Displays the device serial number.

Entering Asset Information Using the CLI Commands

The following table summarizes the CLI commands for entering fields displayed on the **Asset** page.

Table 7-1. Asset CLI Command

CLI Command	Description
snmp-server contact *text* **no snmp-server contact**	Configures the system contact (sysContact) name. Use the **no** form of the command to remove the system contact information.
snmp-server location *text* **no snmp-server location**	Configures the system location string. Use the no form of this command to remove the location string.
hostname *name* **no hostname**	Specifies the device host name. Use the no form of the command to remove the existing host name.
clock set *hh:mm:ss {[day month] | [month day]} year*	Sets the system clock to this time.
asset-tag *tag* **no asset-tag**	Assigns the asset tag to the device. Use the **no** form of this command to remove the asset tag from the device.

The following is an example of the CLI commands

```
console (config)#        asset-tag    2365491870
```

System Health

There are five temperature sensors for monitoring the temperature of the switch and the ambient temperature.

To view the device's temperature information:

1 Click **System** > **General** > **System Health** in the tree view to display the **System Health** page.

This page displays the temperature of each sensor, as follows:

- **Ambient 1**— Temperature surrounding the switch.
  - **Current Temperature (Celsius)** — Current temperature around the switch.
  - **Target Temperature (Celsius)** — Maximum temperature allowed around the switch.
- **Switch Temperature Sensor (Only for R1-2401)**— Temperature inside the switch.
  - **Current Temperature (Celsius)** — Current temperature inside the switch.
  - **Target Temperature (Celsius)** — Maximum temperature allowed inside the switch.
- **Component 1**—Temperature inside the packet process thermal sensor (98CX8123).
  - **Current Temperature (Celsius)** — Current temperature inside the component.
  - **Target Temperature (Celsius)** — Maximum temperature allowed inside the component.
- **Component 2**—Temperature inside the CPU thermal sensor (88F6707).
  - **Current Temperature (Celsius)** — Current temperature inside the component.
  - **Target Temperature (Celsius)** — Maximum temperature allowed inside the component.
- **Component 3**—Temperature inside the PHY thermal sensor (88E1514 (U21).
  - **Current Temperature (Celsius)** — Current temperature inside the component.
  - **Target Temperature (Celsius)** — Maximum temperature allowed inside the component.

- **Component 4 (Only for R1-2210)**—Temperature inside the PHY Thermal sensor (88E1514 (U22)):
  - **Current Temperature (Celsius)** — Current temperature inside the component.
  - **Target Temperature (Celsius)** — Maximum temperature allowed inside the component.

Table 7-2. Celsius to Fahrenheit Conversion Table

Celsius	Fahrenheit
0	32
5	41
10	50
15	59
20	68
25	77
30	86
35	95
40	104

Viewing System Health Information Using the CLI Commands

The following table summarizes the CLI commands for viewing fields displayed on the **System Health** page.

Table 7-3. System Health CLI Command

CLI Command	Description
`show system sensor`	Displays sensor temperature information.

The following is an example of the output of the CLI command (on the R1-2210):

```
console# show system sensor
Temperature Sensor Type Current                  Target
                        Temperature (C)          Temperature (C)
----------------------- ---------------------- ----------------
Ambient 1                    31                       70
Component 1                  52                       95
Component 2                  27                       90
Component 3                  25                      105
Component 4                  25                      105
```

System Routing Mode

The R1-2401 device can be in either Layer 2 mode or Layer 2+ Static Routing mode. The R1-2210 device is always in Layer 2+ Static Routing mode.

To set the system mode of the R1-2401:

1. Click **System** > **General** > **System Routing Mode** in the tree view to display the **System Mode** page.
2. Select either **Layer 2** or **Layer 2+** Static Routing.
3. Click **Apply**.

Setting the System Mode Using CLI Commands

The following table summarizes the CLI commands for setting the system mode.

Table 7-4. Clock Source CLI Command

CLI	Description
set system mode {*layer-2-plus-IPv4-static-routing* **|** *layer-2-only***}**	Configures the system mode to be router (Layer 2 + Static Routing or switch (Layer 2).

The following is an example of the CLI commands:

```
console# set system mode layer-2-plus-IPv4-static-
routing
```

Time Synchronization

The system clock runs from the moment the system starts up, and keeps track of the date and time.

The date and time may be either set manually, or it may be received from an SNTP server. If an external clock source, or an SNTP time server is not defined, the manual clock setting is not persistent across boots.

This section describes how to set system time, and contains the following topics:

- Global Settings (Clock Source)
- Manual Time Settings
- System Time from an SNTP Server
  - SNTP Global Settings
  - SNTP Authentication
  - SNTP Servers
  - SNTP Interface Settings

Global Settings (Clock Source)

System time can be set manually, or it may be received from an external SNTP server. You if wish to set the system time manually, you do not to use the **Global Settings** page, because the default is manual (local) system time.

To set the clock source:

1. Click **System** > **Time Synchronization** > **Global Settings** in the tree view to display the **Global Settings** page.
2. Select the **Clock Source**. The possible options are:
   - **Local** —System time is taken from the device's internal clock. Set this as defined in Manual Time Settings.
   - **SNTP** — System time is set via an SNTP server. Set SNTP parameters as defined in System Time from an SNTP Server.

Defining the Clock Source Using CLI Commands

The following table summarizes the CLI commands for setting the clock source.

Table 7-5. Clock Source CLI Command

CLI	Description
clock source sntp **no clock source**	Configures an external time source for the system clock. Use the no form of this command to disable the external time source.
show clock [*detail*]	Displays the time and date from the system clock and its source.

The following is an example of the CLI commands:

```
console# clock source sntp
console# show clock detail
3:29:03 UTC Sep 7 2010
Time source is sntp
Time zone:
Offset is UTC+0
```

Manual Time Settings

Use the **Manual Time Settings** page to set system date/time manually (as opposed to receiving them from an external SNTP server). For more information on SNTP, see System Time from an SNTP Server.

If system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the time set here or in the **Asset** page.

In addition to setting the local clock, you can use this page to enable Daylight Savings Time (DST) on the device.

The manual clock setting is not persistent across boots.

DST Start and End Times

The following is a list of DST start and end times in various countries:

- **Albania** — Last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia - Tasmania** — From beginning of October until the end of March.
- **Armenia** — Last weekend of March until the last weekend of October.
- **Austria** — Last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with U.S. summer hours.
- **Belarus** — Last weekend of March until the last weekend of October.
- **Belgium** — Last weekend of March until the last weekend of October.
- **Brazil** — From the 3rd Sunday in October until the 3rd Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- **Chile** — Easter Island 9th March 12th October. The first Sunday in March or after 9th March.
- **China** — China does not operate Daylight Saving Time.
- **Canada** — From the first Sunday in April until the last Sunday of October. Daylight Saving Time is usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities.
- **Cuba** — From the last Sunday of March to the last Sunday of October.
- **Cyprus** — Last weekend of March until the last weekend of October.
- **Denmark** — Last weekend of March until the last weekend of October.
- **Egypt** — Last Friday in April until the last Thursday in September.
- **Estonia** — Last weekend of March until the last weekend of October.
- **Finland** — Last weekend of March until the last weekend of October.
- **France** — Last weekend of March until the last weekend of October.
- **Germany** — Last weekend of March until the last weekend of October.
- **Greece** — Last weekend of March until the last weekend of October.
- **Hungary** — Last weekend of March until the last weekend of October.

- **India** — India does not operate Daylight Saving Time.
- **Iran** — From 1st Farvardin until the 1st Mehr.
- **Iraq** — From 1st April until 1st October.
- **Ireland** — Last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.
- **Italy** — Last weekend of March until the last weekend of October.
- **Japan** — Japan does not operate Daylight Saving Time.
- **Jordan** — Last weekend of March until the last weekend of October.
- **Latvia** — Last weekend of March until the last weekend of October.
- **Lebanon** — Last weekend of March until the last weekend of October.
- **Lithuania** — Last weekend of March until the last weekend of October.
- **Luxembourg** — Last weekend of March until the last weekend of October.
- **Macedonia** — Last weekend of March until the last weekend of October.
- **Mexico** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.
- **Moldova** — Last weekend of March until the last weekend of October.
- **Montenegro** — Last weekend of March until the last weekend of October.
- **Netherlands** — Last weekend of March until the last weekend of October.
- **New Zealand** — From the first Sunday in October until the first Sunday on or after 15th March.
- **Norway** — Last weekend of March until the last weekend of October.
- **Paraguay** — From 6th April until 7th September.
- **Poland** — Last weekend of March until the last weekend of October.
- **Portugal** — Last weekend of March until the last weekend of October.
- **Romania** — Last weekend of March until the last weekend of October.
- **Russia** — From the 29th March until the 25th October.
- **Serbia** — Last weekend of March until the last weekend of October.
- **Slovak Republic** — Last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not operate Daylight Saving Time.

- **Spain** — Last weekend of March until the last weekend of October.
- **Sweden** — Last weekend of March until the last weekend of October.
- **Switzerland** — Last weekend of March until the last weekend of October.
- **Syria** — From 31st March until 30th October.
- **Taiwan** — Taiwan does not operate Daylight Saving Time.
- **Turkey** — Last weekend of March until the last weekend of October.
- **United Kingdom** — Last weekend of March until the last weekend of October.
- **United States of America** — From the second Sunday of March at 02:00 to the first Sunday of November at 02:00.

To manually set the device time:

1. Click **System** > **Time Synchronization** > **Manual Time Settings** in the tree view to display the **Manual Time Settings** page.
2. Enter the following local settings:
   - **Date** — The system date.
   - **Local Time** — The system time.
   - **Time Zone Offset** — The difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1:00, while the local time in New York is GMT –5:00.
3. To set Daylight Savings Time (DST), select the **Daylight Savings** field and select one of the possible options:
   - **USA** — The device switches to DST at 2 a.m. on the second Sunday of March, and reverts to standard time at 2 a.m. on the first Sunday of November.
   - **European** — The device switches to DST at 1:00 am on the last Sunday in March, and reverts to standard time at 1:00 am on the last Sunday in October. The **European** option applies to EU members, and other European countries using the EU standard.
   - **Other** — Specifies that you will set DST manually in the fields described below.

   If you selected **USA** or **European** you are finished. If you selected **Other**, proceed to the next step.

There are two types of DST possible when **Others** is selected. You can set a specific date in a particular year, or you can set a recurring setting, irrespective of the year. For a specific setting in a particular year, complete the **Daylight Savings** area, and for a recurring setting, complete the **Recurring** area.

If **Other** is selected, the **From** and **To** fields must be defined either in the **Non-recurring** or **Recurring** section.

4 To enter non-recurring DST parameters, enter the following fields:

   – **From** — The time that DST begins. The possible options are:

      - **DD/MMM/YY** — The date, month, and year at which DST begins.
      - **HH/MM** — The time (hour and minutes) at which DST begins.

   – **To** — The time that DST ends. The possible options are:

      - **DD/MMM/YY** — The date, month, and year at which DST ends.
      - **HH/MM** — The time (hour and minutes) at which DST ends.

5 To enter recurring DST parameters, select **Recurring** and enter the following fields:

   – **From** — The time that DST begins each year, for example, DST begins locally every second Sunday in April at 5:00 am. The possible options are:

      - **Day** — The day of the week from which DST begins every year.
      - **Week** — The week within the month from which DST begins every year.
      - **Month** — The month of the year in which DST begins every year.
      - **Time** — The time at which DST begins every year.

   – **To** — The recurring time that DST ends each year, for example, DST ends locally every fourth Friday in October at 5:00 am. The possible options are:

      - **Day** — The day of the week at which DST ends every year.
      - **Week** — The week within the month at which DST ends every year.
      - **Month** — The month of the year in which DST ends every year.

- **Time** — The time at which DST ends every year.

CLI Commands for Setting Manual Time

The following steps (in any order) must be completed before setting time manually:

- Set system time
- Define the time zone in relation to GMT.
- Configure Daylight Savings Time.

The following table summarizes the CLI commands for setting fields displayed in the **Manual Time Setting** pages when the clock source is **Local**.

Table 7-6. Manual Time Setting CLI Commands

CLI	Description
clock set *hh:mm:ss* {[*day month*]|[*month day*]} *year*	Set the system clock to this time.
clock summer-time ***zone*** **recurring** {***usa***|***eu***|{*week day month hh:mm week day month hh:mm*}}[*offset*]	Configures the system to automatically switch to summer time (according to the USA and European standards) every year on a recurring basis.
clock summer-time zone **recurring {usa | eu |** {week day month hh:mm week day month hh:mm}} [offset]	Configures the system to automatically switch to summer time (Daylight Savings Time) for a specific period - date/month/year format.
clock summer-time zone **date** day month year hh:mm date month year hh:mm [offset]	Use the no form of the command to configure the system not to switch to summer time (Daylight Savings Time).
clock summer-time zone **date** month day year hh:mm month day year hh:mm [offset]	
no clock summer-time	

Table 7-6. Manual Time Setting CLI Commands *(continued)*

CLI	Description
clock timezone *zone hours-offset* [*minutes offset*]	Sets the time zone and names it "zone" for display purposes.
no clock timezone	Use the no form of this command to set the time to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same.
show clock	Displays the time and date from the system clock.

A sample script to set system time manually is shown below.

Table 7-7. CLI Script to Set Manual System Time

CLI	Description
console# clock summer-time Ohio date apr 1 2010 09:00 aug 2 2010 09:00	Set a time range for summer time called "Ohio".
console# **clock timezone** Ohio +2	Set the time zone to GMT plus 2 hours. The name of the zone "Ohio" is purely for documentation purposes. This is not mandatory for manual time, but is recommended. It enables anyone seeing the time to know what that time is in respect to their timezone.
console# **clock summer-time** Ohio_Summer recurring usa	Set Daylight Savings Time such that it recurs every year and is based on the summer time schedule of the USA. The name of the zone "Ohio_Summer" is for documentation purposes only.
console# **show clock**	Display the system time.

System Time from an SNTP Server

This section describes how to configure SNTP servers. It contains the following topics:

- Overview
- SNTP Global Settings
- SNTP Authentication
- SNTP Servers
- SNTP Interface Settings

Overview

The switch supports the Simple Network Time Protocol (SNTP), which provides accurate network switch clock time synchronization of up to 100 milliseconds. The implementation of SNTP is based on SNTPv4 (RFC 2030).

SNTP is a simple and lighter version of NTP, and can be used when the ultimate performance of the full NTP implementation, described in RFC-1305, is not required. SNTP operates with NTP, thus an SNTP client can work with both SNTP and NTP servers.

The switch operates only as a client, and cannot provide time services to other systems.

SNTP Server Types

The switch can accept time information from the following server types:

- **Unicast**

  Polling for Unicast information is used for polling a server whose IP address is known. This is the preferred method for synchronizing device time, as it is most secure.

  Up to eight SNTP servers can be defined.

  If this method is selected, SNTP information is accepted only from SNTP servers defined in the **SNTP Servers** page.

  Time levels T1 - T4 (see the Algorithm for Selecting Designated SNTP Server section) are used to determine from which server time information is accepted.

If Unicast polling is not enabled or if no servers are defined on the device, the device accepts time information from any SNTP server of the type that is enabled, which responds.

- **Anycast**

  Polling for Anycast information is used when the SNTP server's IP address is not defined or it cannot be reached. If this method is enabled, time information can be received from any SNTP server on the network. The device time and date are synchronized when it proactively requests synchronization information.

  Anycast polling to get time information is preferable to Broadcast polling, because it is more secure.

  Time levels T3 and T4 are used to determine from which server time information is accepted.

- **Broadcast**

  Broadcast information is used if receiving Broadcast packets has been enabled, and one of the following situations occurs:

  – The SNTP server IP address has not been defined.

  – Several time-information packets are received and the Broadcast time is best according to the algorithm defined in Algorithm for Selecting Designated SNTP Server.

Broadcast is the least secure method of receiving time, because it is both unsecured and the time information was not specifically requested by the device. Anycast is also unsecured, but time-information packets are only accepted if they were requested.

Stratums

Each SNTP server is characterized by stratums, which define the accuracy of its clock. The stratum is the distance, in terms of NTP hops, from the most authoritative time server. The lower the stratum (where zero is the lowest), the more accurate the clock. The switch accepts time from stratum 1 and above.

The following provides examples of clocks from various stratums:

- **Stratum 0** — A real time clock is used as the time source, for example, a GPS system.

- **Stratum 1** — A server that is directly linked to a Stratum 0 time source is used.
- **Stratum 2** — The time source is distanced from the Stratum 1 server over a network path, for example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Algorithm for Selecting Designated SNTP Server

Messages received from SNTP servers are logged, until there are three responding servers, or the timer expires. In any event, when the third message is received, the timer expires.

A server is selected to be the “designated server” according to the following criteria:

- The stratum (the distance in terms of NTP hops from the best authoritative time servers) is considered, and the server with the best (lowest) stratum is selected.
- If there is a tie in stratums, packets from servers defined on the device are preferred to Anycast packets, which in turn are preferred to Broadcast packets.
- If multiple servers pass the above criteria, then the server that sent the first (earliest) time packet is chosen.

If a better server is discovered later, it is selected to be the “designated server” at that time.

Polling

You can configure the system to acquire time information in the following ways:

- **Enable polling** — Time information is requested every polling interval.
- **Do not enable polling** — Time information is received when the system is brought up and every time that a topological change is made to the Running Configuration file, for example when an SNTP Unicast server is added.

This is configured by the user in the **SNTP Global Settings** page.

On power up, when the switch sends a request and there is no reply, it issues another request (three retries at most) after 20 seconds of waiting.

If no SNTP server is found, the process is invoked every “poll interval” (set in the **SNTP Global Settings** page), and a management trap is triggered.

Authentication

You can require that SNTP servers be authenticated, although this is not mandatory (see the **SNTP Authentication** pages).

MD5 (Message Digest 5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash value. MD5 is a variation of MD4, and increases MD4 security.

MD5 both verifies the integrity of the communication and authenticates the origin of the communication.

SNTP Global Settings

If **SNTP** was selected as the clock source in the **Global Settings** page, you must define the mechanism of setting time from an SNTP server. This is done in the SNTP pages, described below.

To define the types of server from which the device accepts SNTP information and the polling interval:

1. Click **System > Time Synchronization > SNTP Global Settings** in the tree view to display the **SNTP Global Settings** page.
2. Enter the fields:
   - **Poll Interval (60-86400)** — Enter the interval (in seconds) at which the SNTP servers are polled.
   - **Receive Broadcast Servers Updates** — Enable/disable receiving time information from Broadcast servers.
   - **Receive Anycast Servers Updates** — Enable/disable receiving time information from Anycast SNTP servers.
   - **Receive Unicast Servers Updates** — Enable/disable receiving time information from the SNTP servers defined on the switch.
   - **Poll Unicast Requests** — Enable/disable sending SNTP Unicast server time information requests to the SNTP server.

Defining SNTP Global Settings Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **SNTP Global Settings** pages.

Table 7-8. SNTP Global Parameters CLI Commands

CLI Command	Description
sntp client poll timer *seconds* **no sntp client poll timer**	Sets the polling time for an SNTP client. Use the no form of this command to restore the default configuration.
sntp broadcast client enable **no sntp broadcast client enable**	Enables SNTP Broadcast clients. Use the **no** form of this command to disable SNTP Broadcast clients.
sntp anycast client enable **no sntp anycast client enable**	Enables SNTP Anycast clients. Use the no form of this command to disable SNTP Anycast clients.
sntp unicast client enable **no sntp unicast client enable**	Enables SNTP predefined Unicast clients. Use the no form of this command to disable SNTP Unicast clients.
show sntp configuration	Displays SNTP configuration

The following is an example of the CLI commands:

```
console(config)# sntp anycast client enable
```

SNTP Authentication

Use the **SNTP Authentication** page to enable/disable SNTP authentication between the device and an SNTP server, and to set the means by which the SNTP server is authenticated.

To configure SNTP authentication:

1 Click **System > Time Synchronization > SNTP Authentication** in the tree view to display the **SNTP Authentication: Summary** page.

The previously-defined authentication keys are displayed.

2 Enable/disable **SNTP Authentication**. This enables/disables authenticating SNTP sessions between the device and an SNTP server.

3 Multiple keys can be defined. To add a new SNTP authentication key, click **Add**, and enter the fields.

– **Encryption Key ID (1 - 4294967295)** — Enter the number used to identify this SNTP authentication key internally.

– **Authentication Key (1 - 8 Characters)** — Enter the key used for authentication. The SNTP server must send this key for the switch to use its time/date information.

– **Trusted Key** — Check to specify that the encryption key is used to authenticate the (Unicast) SNTP server. If this is not checked, the key is not used for authentication (and another key(s) is used).

Defining SNTP Authentication Settings Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **SNTP Authentication** pages.

Table 7-9. SNTP Authentication CLI Commands

CLI Command	Description

`sntp authenticate`
`no sntp authenticate`
	Defines authentication for received SNTP traffic from servers.
	Use the no form of this command to disable the feature.

`sntp trusted-key` *`key-number`*
`no sntp trusted-key` *`key-number`*
	Authenticates the identity of a system to which SNTP will synchronize.
	Use the no form of this command to disable system identity authentication.

`sntp authentication-key` *`key-number`* **`md5`** *`key-value`*
`no sntp authentication-key` *`key-number`*
	Defines an authentication key for SNTP.
	Use the no form of this command to remove the authentication key for SNTP.

The following is an example of the CLI commands:

```
console(config)# sntp authenticate
console(config)# sntp trusted-key 8
console(config)# sntp authentication-key 8 md5 Clkkey
```

SNTP Servers

To add an SNTP server or display SNTP server information:

1. Click **System > Time Synchronization > SNTP Servers** in the tree view to display the **SNTP Servers: Summary** page.

   The following is displayed for the previously-defined servers:

   - **SNTP Server** — IP address of server.
   - **Polling** — Polls the selected SNTP server for system time information, when enabled.
   - **Encryption Key ID** — Key Identification used to communicate between the SNTP server and device.
   - **Preference** — SNTP server providing SNTP system time information. The system displays on of the following options:
     - **Primary** — The server from which time was last accepted.
     - **Secondary** — All other servers from which time was received.
   - **Status** — The operating SNTP server status. The possible options are:
     - **Up** — The SNTP server is currently operating normally.
     - **Down** — An SNTP server is currently not available, for example, the SNTP server is currently not connected or is currently down.
     - **In progress** — The SNTP server is currently sending or receiving SNTP information.
     - **Unknown** — The progress of the SNTP information currently being sent is unknown, for example, the device is currently looking for an interface.
   - **Last Response** — The last time a response was received from the SNTP server.

- **Offset** — The estimated offset of the server's clock, relative to the local clock, in milliseconds. The host determines the value of this offset, using the algorithm described in RFC 2030.
- **Delay** — The estimated round-trip delay of the server's clock, relative to the local clock over the network path between them, in milliseconds. The host determines the value of this delay, using the algorithm described in RFC 2030.

2 To add an SNTP Server, click **Add**, and enter the fields:

- **Supported IP Format** — Select whether IPv4 or IPv6 format is used for the IP address of the SNTP server.
- **IPv6 Address Type** — When the server supports IPv6, this specifies the type of static address supported. Select one of the possible options:
  - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
  - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.
- **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. Select one of the possible options:
  - **VLAN** 1— The VLAN on which the IPv6 interface is configured.
  - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.
- **SNTP Server** — Enter the SNTP server's IP address.
- **Poll Interval** — Enable/disable polling the selected SNTP server for system time information, when enabled.
- **Encryption Key ID** — Check to use an encryption key, and select one of the encryption keys that was defined in the **SNTP Authentication** pages.

Defining SNTP Servers Settings Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **SNTP Server** pages.

Table 7-10. SNTP Server CLI Commands

CLI Command	Description
sntp server {*ip-address* | *hostname*} [**poll**] [**key** *keyid*] **no sntp server** {*ip-address* | *hostname*}	Configures the device to use SNTP to request and accept SNTP traffic from a server. Use the no form of this command to remove a server from the list of SNTP servers.
sntp unicast client poll **no sntp unicast client poll**	Enables polling for the SNTP predefined Unicast clients. Use the no form of this command to disable the polling for the SNTP client.
show sntp status	Displays the SNTP server statuses.

The following is an example of the CLI commands:

```
console(config)# sntp server 100.1.1.1 poll key 10
console# show sntp status
Clock is unsynchronized
Unicast servers:
Server       Status   Last Response  Offset   Delay
                                     [mSec]   [mSec]
---------- -------- ------------  ------   -----
Anycast server:
Server       Status   Last Response  Offset   Delay
                                     [mSec]   [mSec]
---------- -------- ------------  ------   -----
Broadcast:
Interface     IP Address        Last Response
----------- -------------- ----------------------
  gi0/1      00:00:00.0      Jan 1 2010
```

SNTP Interface Settings

If receiving time information from Anycast servers is enabled, you can determine through which interface the Anycast packets are sent and received. If no interface is defined, Anycast requests are not sent.

To enable receiving Anycast updates on an interface:

1 Click **System** > **Time Synchronization** > **SNTP Interface Settings** to display the **SNTP Interface Settings: Summary** page.

   The following fields are displayed for every interface for which an SNTP interface has been enabled:

   – **Interface** — The port, LAG or VLAN on which SNTP is enabled.

   – **Receive Servers Updates** — Displays whether the interface is enabled to receive updates from the SNTP server.

2 To add an interface that can receive SNTP server updates, click **Add**.

3 Select an interface and enable/disable **State** to indicate that the interface can now receive/not receive SNTP server updates.

Defining SNTP Interface Settings Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **SNTP Interface Settings** pages.

Table 7-11. SNTP Interface Settings CLI Commands

CLI Command	Description

`sntp client enable {interface-id}`
`no sntp client enable {interface-id}`
	Enables the SNTP client on an interface in Global Configuration mode for Broadcast and Anycast clients on an interface.
	Use the **no** form of this command to disable the SNTP client.

`sntp client enable`
`no sntp client enable`
	Enables SNTP client on an interface in Global Configuration or Interface Configuration mode for Broadcast and Anycast clients on an interface.
	Use the **no** form of this command to disable the SNTP client.

`show sntp configuration`	Shows the configuration of the Simple Network Time Protocol (SNTP).

The following is an example of the CLI commands:

```
console# configure
console(config)# sntp client enable gi0/1
console# exit
console# configure
console(config)# interface gi0/1
console(config-if)# sntp client enable
console# show sntp configuration
SNTP port: 123.
Polling interval: 1024 seconds.
No MD5 authentication keys.
Authentication is not required for synchronization.
No trusted keys.
Unicast Clients: Disabled
Unicast Clients Polling: Disabled
Server              Polling   Encryption Key
----------------------------- ---------- -----------
Broadcast Clients: disabled
Anycast Clients: disabled
Broadcast Interfaces: gi0/1
```

CLI Script for Receiving Time from an SNTP Server

The following is a sample script that configures receiving system time from an SNTP server.

Table 7-12. Manual Time Setting CLI Commands

CLI	Description
`console(config)#clock source sntp`	Set the source of time as an SNTP server.
`console(config)#sntp client poll timer 6`	Set polling time to 6 seconds.
`console(config)#sntp unicast client enable`	Enable accepting time from predefined Unicast clients.
`console(config)#sntp unicast client poll`	Enable polling predefined Unicast clients.
`console(config)#sntp server 10.4.1.3 poll`	Define the server that will be used as an SNTP server.

`console(config)#exit`
`console# show sntp configuration`
	Display SNTP settings.

`console# show sntp status`	Display SNTP servers.

Logs

The Logs feature enables the switch to keep several, independent logs. Each log is a set of entries that record system events.

It contains the following topics:

- Overview
- Global Parameters
- RAM Log
- Log File
- Login History
- Remote Log Server

Overview

System logs record events and report errors or informational messages. Some aspects of system logging can be configured, as described below.

Some events are automatically logged, such as hardware problems. You may enable/disable logging the following types of events:

- **Authentication Events** in the **Global Parameters** page
- **Copy File Events** in the **Global Parameters** page
- **Management Access Events** in the **Global Parameters** page
- **Login History** in the **Login History** page

Event messages have a unique format, as per the System Logs (SYSLOG) protocol recommended message format for all error reporting, for example, SYSLOG and local device reporting messages are assigned a severity code, and include a message mnemonic that identifies the source application generating the message.

Messages may be filtered, based on their urgency or relevancy.

Events may be logged to the following destinations:

- **Console**
- **Logging buffer (RAM)**— Messages are stored in a cyclical file buffer. When the maximum number of messages is reached, messages are written starting at the beginning of the buffer (overwriting the old messages).

  Logs stored on the Logging buffer are deleted when the device is reset.
- **Logging file (flash)** — Messages are stored in flash memory. When the buffer is full, messages are written starting at the beginning of the memory block (overwriting the old messages).
- **SYSLOG Server** — Messages are sent to a remote server. This is useful for central and remote management and to provide more space for storage of messages. Up-to eight SYSLOG servers can be defined in the **Remote Log Server Settings** pages.

You can select where to send logging messages according to their severity. Each of the severity level can be directed to the console, RAM log, flash log file or SYSLOG server or to any combination of these destinations.

Global Parameters

Use the **Global Parameters** page to enable/disable logging for the following logging severity levels.

- **Emergency** — If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- **Alert** — An alert log is saved if there is a serious device malfunction, for example, all device features are down.
- **Critical** — A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
- **Error** — A device error has occurred, for example, a single port is offline.
- **Warning** — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- **Notice** — Provides device information to which you might have to respond.
- **Informational** — Provides device information to which you do not have to respond.
- **Debug** — Provides debugging messages.

If you enable logging, some events are automatically logged, and in addition, you can enable/disable specific types of logging and set their destination.

To configure logging:

1. Click **System** > **Logs** > **Global Parameters** in the tree view to display the **Global Parameters** page.
2. **Enable/disable** logging in the **Logging** drop-down list. Console logs are enabled by default, and cannot be disabled.
3. If Logging is enabled, select the types of events to be logged in addition to the events that are always logged:
   - **Log Authentication Events** — Enable/disable generating logs when users are authenticated.
   - **Log Copy Files Events** — Enable/disable generating logs when files are copied.

- **Log Management Access Events** — Enable/disable generating logs when the device is accessed using a management method, for example, each time the device is accessed using SSH, a device log is generated.

4 To select the destination of logging messages, according to their severity levels, check the minimum severity level that will be associated with the console log, RAM log, Log file (Flash memory) and remote SYSLOG servers. When a severity level is selected, all severity levels above the selection are selected automatically.

Enabling Logs Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **Global Parameters** page.

Table 7-13. Global Log Parameters CLI Commands

CLI Command	Description
logging on	Enables error message logging.
no logging on	Turns off error message logging.
logging console *level* **no logging console**	Limits messages logged to the console, based on severity. Use the **no** form of this command to disable logging limiting to the console.
logging file *level* **no logging file**	Limits SYSLOG messages stored in flash memory, based on severity. Use the **no** form of this command to cancel using the buffer.
file-system logging {***copy*** | ***delete-rename***}	Enables the logging of file system events.
no file-system logging {***copy*** | ***delete-rename***}	Use the **no** form of this command to disable logging file system events

management logging {***deny***}
no management logging {***deny***}
	Enables Management Access List (ACL) deny events.
	Use the **no** form of this command to disable logging management access list events.

Table 7-13. Global Log Parameters CLI Commands ***(continued)***

CLI Command	Description

aaa logging {*login*}
no aaa logging {*login*}
	Enables logging authentication login events.
	Use the **no** form of this command to disable logging authentication login events.

The following is an example of the CLI commands:

```
console# configure
console(config)# logging on
console(config)# logging console errors
console(config)# logging file alerts
```

RAM Log

To manage the RAM log buffer:

1 Click **System** > **Logs** > **RAM Log** in the tree view to display the **RAM Log** page.

   The **Max RAM Log Entries (20-400)** line, which contains the maximum number of RAM log entries permitted, is displayed. When the log buffer is full, the oldest entries are overwritten. The **Current Setting** contains how many entries are currently permitted, and you can change this number in the **New Setting (after reset)** field.

   The following is displayed for the existing logs:

   – **Log Index** — The log number in the RAM Log table.

   – **Log Time** — The time at which the log was entered into the RAM Log table.

   – **Severity** — The log severity.

   – **Description** — The log entry text.

2 To remove all entries from the RAM log, click **Clear Log**.

Viewing and Clearing the RAM Log Table Using the CLI Commands

The following table summarizes the CLI commands for setting the size of the RAM log buffer, viewing, and clearing entries in the RAM log.

Table 7-14. RAM Log Table CLI Commands

CLI Command	Description
logging buffered *[buffer-size] [severity-level | severity-level-name]*	Sets the number of SYSLOG messages stored in the internal buffer (RAM).
no logging buffered	Use the **no** form of this command to cancel using the buffer.
show logging	Displays the RAM logging buffer.
clear logging	Clears the RAM logging buffer.

The following is an example of the CLI commands:

```
console(config)# logging buffered 300 alerts

SYSLOG-N-LOGGINGBFRSIZE: the number of syslog
messages stored in the internal buffer will be
changed to default (after reboot).
```

Log File

To view and/or clear the flash memory log file:

1 Click **System** > **Logs** > **Log File** in the tree view to display the **Log File** page.

The following is displayed for the existing logs:

- **Log Index** — The log number in the Log file.
- **Log Time** — The time at which the log was entered.
- **Severity** — The log severity.
- **Description** — The log entry text.

2 To remove all entries from the log file, click **Clear Log**.

Displaying the Log File Table Using the CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **Log File** page.

Table 7-15. Log File Table CLI Commands

CLI Command	Description
`show logging file`	Displays the logging state and the SYSLOG messages stored in the logging file.

The following is an example of the CLI commands:

```
console# show logging file

Logging Header Sending is enabled.

Logging is enabled.

Console Logging: Level info. Console Messages: 0
Dropped.

Buffer Logging: Level info. Buffer Messages: 62
Logged, 62 Displayed, 200 Max.

File Logging: Level debug. File Messages: 11 Logged,
51 Dropped.

SysLog server 1.1.1.1 Logging: info. Messages: 0
Dropped.

Application filtering control

Application   Event                           Status

----------- --------------------        ---------

AAA            Login                           Enabled

File system    Copy                            Enabled

File system    Delete-Rename                   Enabled

Management ACL Deny                            Enabled

01-Jan-2000 01:12:01: %COPY-W-TRAP: The copy
operation was completed successfully

01-Oct-2012 01:11:49: %LINK-I-Up: gi0/11

01-Oct-2012 01:11:46: %LINK-I-Up: gi0/12
```

Login History

Use the **Login History** page to monitor users, including the time a user logged in, and the protocol used to log on to the device.

To enable user history logging and view user login history:

1 Click **System** > **Logs** > **Login History** in the tree view to display the **Login History** page.

  The login history for the selected user or all users is displayed.

2 Enable/disable **Login History to File** to record login history.

3 Select a user or **All** from the **User Name** drop-down list. The login history for this user is displayed in the following fields:

  - **Login Time** — The time the selected user logged on to the device.
  - **User Name** — The user that logged on to the device.
  - **Protocol** — The means by which the user logged on to the device.
  - **Location** — The IP address of the station from which the device was accessed.

Displaying the Device Login History Using CLI Commands

The following table summarizes the CLI commands for viewing and setting fields displayed in the **Login History** page.

Table 7-16. Login History CLI Commands

CLI Command	Description

`aaa login-history file`
`no aaa login-history file`
	Enables writing to the login history file.
	Use the no form of this command to disable writing to the login history file.

`show users login-history [username` *`username`*`]`	Displays the user’s login history.

The following is an example of the CLI commands:

```
console (config)# aaa login-history file
console# show users login-history

Login Time            Username  Protocol   Location
-----------           --------  --------   ----------
01-Oct-2010 23:58:17  admin     HTTP       172.16.1.8
01-Oct-2010 07:59:23  admin     Telnet     172.16.0.8
```

Remote Log Server

Log messages can be sent to remote log servers, using the SYSLOG protocol.

To add a remote log server:

1. Click **System** > **Logs** > **Remote Log Server** in the tree view to display the **Remote Log Server: Summary** page.

   The previously-defined remote servers are displayed.

2. To add a remote log server, click **Add**, and enter the fields:

   – **Supported IP Format** — Select whether the IPv4 or IPv6 format is supported.

   – **IPv6 Address Type** — When the server supports IPv6, this specifies the type of static address supported. The possible options are:

     - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
     - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.

   – **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:

     - **VLAN 1** — The VLAN on which the IPv6 interface is configured.
     - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.

- **New Log Server IP Address** — Enter the IP address of the remote SYSLOG server.
- **UDP Port (1-65535)** — Enter the UDP port to which the logs are sent for the selected server.
- **Facility** — Select a user-defined application from which system logs are sent to the remote server. Only a single facility can be assigned to a single server. If a second facility level is assigned, the first facility level is overridden. All applications defined for a device utilize the same facility on a server.
- **Description (0-64 Characters)** — Enter a server description.
- **Severity to Include** — Check the severity levels to be logged to the remote server. The event severity levels are listed on this page in descending order from the highest severity to the lowest. When a severity level is selected to appear in a log, all higher severity events are automatically selected to appear in the log. When a security level is not selected, no lower severity events appear in the log.

Working with Remote Server Logs Using the CLI Commands

The following table summarizes the CLI command for working with remote log servers.

Table 7-17. Remote Log Server CLI Commands

CLI Command	Description
`logging host` *`{ipv4-address	ipv6-address	hostname}`* **`[port`** *`port`*`]` `[`**`severity`** *`level`*`]` `[`**`facility`** *`facility`*`]` `[`**`description`** *`text`*`]` **`no logging host`** `{`*`ipv4-address	ipv6-address	hostname`*`}`	Logs messages to a remote server with this IP address. Use the no form of this command to delete the SYSLOG server with the specified address from the list of SYSLOGs.
`show syslog-servers`	Displays list of SYSLOG servers.

The following is an example of the CLI commands:

```
console (configure) # logging host 1.1.1.1

console# show syslog-servers

Device Configuration

---------------------------------------------------
------

IP Address  Port  Facility    Severity
    Description

----------- ----- -------- -----------     ---------
--

1.1.1.1     514   local7       info

1.1.1.2     514   local7       info

1.1.1.3     514   local7       info

1.1.1.4     514   local7       info
```

Domain Name

The Domain Name feature enables configuring the usage of site names in place of IP addresses. It contains the following topics:

- Domain Name System
- Default Domain Name
- Host Name Mapping

Domain Name System

The Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned, the DNS service translates the name into a numeric IP address, for example, **www.ipexample.com** is translated into 192.87.56.2. DNS servers maintain domain name databases and their corresponding IP addresses.

To add a DNS server and specify the active DNS server:

1 Click **System** > **Domain** Name > **Domain Name System** in the tree view to display the **Domain Name System: Summary** page.

   The list of previously-defined DNS servers is displayed.

2 Enter the following fields:

   - **DNS Status**—Select **Enable** to enable mapping of host names into IP addresses through a DNS server.
   - **Domain Name Query Interval(20-3600)—** Enter how often DNS queries will be sent.

3 To activate one of the currently-defined DNS servers, enable **Active Server**.

4 To add a DNS server, click **Add**, and enter the fields:

   - **Supported IP Format** — Select whether the IPv4 or IPv6 format is supported.
   - **IPv6 Address Type** — When the server supports IPv6, this specifies the type of static address supported. The possible options are:
     - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
     - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.
   - **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:
     - **VLAN** 1 — The VLAN on which the IPv6 interface is configured.
     - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.
   - **DNS Server** — Enter the IP address of the DNS server being added.
   - **DNS Server Currently Active** — Displays the DNS server that is currently active.
   - **Set DNS Server Active** — Check to activate the selected DNS server.

Configuring DNS Servers Using the CLI Commands

The following table summarizes the CLI commands for configuring the fields in the **Domain Name System** pages.

Table 7-18. DNS CLI Commands

CLI Command	Description
ip domain lookup **no ip domain lookup**	Enables DNS system for translating host names to IP addresses. Use the no form of this command to disable DNS-based host name-to-address translation.
ip name-server {*server1-ipv4-address* | *server1-ipv6-address*} [*server-address2* …*server-address8*] **no ip name-server** [*server-address* … *server-address8*]	Sets the available name servers. Up to eight name servers can be set. The no form of the command removes a name server.
clear host {*name*|*}	Deletes entries from the host name-to-address cache.
clear host dhcp {*name*|*}	Deletes entries from the host name-to-address mapping received from DHCP.
show hosts [*name***]**	Displays the default domain name, the list of name server hosts, the static and the cached list of host names and addresses

The following is an example of the CLI commands:

```
console (config)# ip domain lookup
console(config)# ip name-server 176.16.1.18
```

Default Domain Name

A default domain name is used when an IP address cannot be mapped to a known domain name. This domain name is applied to all unqualified host names.

To define the default domain name:

1. Click **System** > **Domain Name** > **Default Domain Name** to display the **Default Domain Name** page.

   If there is a currently-defined default domain name, it is displayed.

2. Enter the **Default Domain Name (1 - 158 Characters).**

   Its **Type** is displayed, and has one of the following options:

   – **Dynamic** — The IP address was created dynamically.

   – **Static** — The IP address is a static IP address.

Defining Default Domain Names Using the CLI Commands

The following table summarizes the CLI commands for configuring the default domain name:

Table 7-19. Default Domain Name CLI Commands

CLI Command	Description

`ip domain name` *`name`*
`no ip domain name`
	Defines a default domain name that the software uses to complete unqualified host names.
	The no form of the command disables the use of the Domain Name System (DNS).

The following is an example of the CLI commands:

```
console(config)# ip domain name dell.com
```

Host Name Mapping

Host names can be dynamically mapped to IP addresses through the **Domain Name System** pages, or statically through the **Host Name Mapping** page.

To assign IP addresses to static host names.

1. Click **System** > **Domain Name** > **Host Name Mapping** in the tree view to display the **Host Name Mapping: Summary** page.

   The currently-defined host names are displayed.

2. Click **Add** to add a new host name. Up to four IP addresses can be added.

3 For each IP address, enter the fields:

- **Supported IP Format** — Select whether the IPv4 or IPv6 format is supported.
- **IPv6 Address Type** — When the server supports IPv6, this specifies the type of static address supported. The possible options are:
  - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
  - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.
- **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:
  - **VLAN1**— The VLAN on which the IPv6 interface is configured.
  - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.
- **Host Name (1-158 Characters)** — Enter the host name to be associated with the IP address entered below.
- **IP Address** — Enter the IP address of the domain. Four addresses can be entered.

Mapping IP Addresses to Domain Host Names Using the CLI Commands

The following table summarizes the CLI commands for mapping domain host names to IP addresses.

Table 7-20. Domain Host Name CLI Commands

CLI Command	Description
ip host *name address* [*address2 address3 address4*]	Defines the static host name-to-address mapping in the host cache
no ip host *name*	Removes the name-to-address mapping.
clear host {*name***|*}**	Deletes entries from the host name-to-address cache.
show hosts [*name*]	Displays the default domain name, list of name server hosts, the static and the cached list of host names and addresses.

The following is an example of the CLI commands:

```
console(config)# ip host accounting.abc.com 176.10.23.1
```

Diagnostics

This section describes how to perform hardware tests on the device. It contains the following topics:

- Integrated Cable Test
- Optical Transceiver Diagnostics

Integrated Cable Test

NOTE: This feature is supported on the R1-2401 (all ports) and on the R1-2210 on external ports gi0/1-2.

Time Domain Reflectometry (TDR) technology is used to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables can only be tested when the ports are in the down state, with the exception of Approximated Cable Length test.

The Approximated Cable Length test can only be performed when the port is up and operating at 1 Gbps.

To perform a cable test and view the results:

1. Click **System** > **Diagnostics** > **Integrated Cable Test: Summary** in the tree view to display the **Integrated Cable Test: Summary** page.
2. Ensure that both ends of the copper cable are connected, one end to tested port and one end to device. Go to the **Test** tab.
3. Click **Test**. The copper cable and Approximate Cable Length tests are performed, and the following test results are displayed:
   - **External Port**— Select the port to be reported.
   - **Test Result** — Displays the cable test results. The possible options are:
     - **No Cable** — There is no cable connected to the port.
     - **Open Cable** — The cable is connected on only one side.
     - **Short Cable** — A short has occurred in the cable.
     - **OK** — The cable passed the test.
     - **Unknown Test Result** — Test results are not known.

- **Cable Fault Distance** — Displays the distance from the port where the cable error occurred.
- **Last Update** — Displays the last time the port was tested.
- **Approximate Cable Length** — Displays the approximate cable length.

Performing Integrated Cable Tests Using CLI Commands

The following table contains the CLI commands for performing integrated cable tests.

Table 7-21. Integrated Cable Test CLI Commands

CLI Command	Description
test cable-diagnostics tdr interface *interface-id*	Performs VCT tests.
show cable-diagnostics tdr [interface *interface-id* | **detailed**]	Shows results of last VCT tests on ports.
show cable-diagnostics cable-length [interface *interface-id* | **detailed**]	Displays the estimated copper cable length attached to a port.

The following is an example of the CLI commands:

```
console> enable
console# test cable-diagnostics tdr gi2/4
Cable is open at 100 meters.
console# show cable-diagnostics cable-length
interface gi2/4
Port      Length [meters]
-------   ----------------
gi2/4    < 50
```

Optical Transceiver Diagnostics

NOTE: This feature is only supported on the R1-2210 on external ports 1-4.

The Optical Transceiver Diagnostics page displays the operating conditions reported by the SFP (Small Form-factor Pluggable) transceiver. Some information might not be available for SFPs that do not support the digital diagnostic monitoring standard SFF-8472.

This test can only be performed on external 10G ports.

The following GE SFP (1000Mbps) transceivers are supported:

- 1000BASE-BX-20U SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 40 km.
- 1000BASE-LH SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 40 km.
- 1000BASE-LX SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 10 km.
- 1000BASE-SX SFP transceiver, for multimode fiber, 850 nm wavelength, supports up to 550 m.
- 1000BASE-T SFP transceiver for category 5 copper wire, supports up to 100 m.

NOTE: For specific part numbers, consult with your Dell representative.

To view the results of optical tests, click **System > Diagnostics > Optical Transceiver Diagnostics**.

This page displays the following fields:

- Port—Port number and description on which the SFP is connected.
- Temperature—Temperature (Celsius) at which the SFP is operating.
- Voltage—SFP's operating voltage.
- Current—SFP's current consumption.
- Output Power—Transmitted optical power.
- Input Power—Received optical power.
- Transmitter Fault—Remote SFP reports signal loss. Values are True, False, and No Signal (N/S).
- Loss of Signal—Local SFP reports signal loss. Values are True and False.
- Data Ready—SFP is operational. Values are True and False.

Performing Optical Transceiver Diagnostics Using CLI Commands

The following table contains the CLI commands for performing Optical Transceiver Diagnostics tests.

Table 7-22. Integrated Cable Test CLI Commands

CLI Command	Description
show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics.

The following is an example of the CLI commands:

```
console> enable
console# show fiber-ports optical-transceiver
Port Temp Voltage Current Output Input LOS
[C] [Volt] [mA] Power Power
[mWatt] [mWatt]
----------- ------ ------- ------- ------- ------- -
gi0/1 Copper
gi0/6 Copper
gi0/7 28 3.32 7.26 3.53 3.68 No
gi0/8 29 3.33 6.50 3.53 3.71 No
Temp - Internally measured transceiver temperature
Voltage - Internally measured supply voltage
Current - Measured TX bias current
Output Power - Measured TX output power in
milliWatts
Input Power - Measured RX received power in
milliWatts
LOS - Loss of signal
N/A - Not Available, N/S - Not Supported, W -
Warning, E - Error
```

Management Security

This section describes the pages used to manage device security.

It contains the following topics:

- Access Profiles
- Profile Rules
- Authentication Profiles
- Select Authentication
- Password Management
- Active Users
- Local User Database
- Line Password
- Enable Password
- TACACS+
- RADIUS

Access Profiles

Access to management functions can be limited to users identified by:

- Ingress interface (Port, LAG, or VLAN)
- Source IP address
- Source IP subnet

Management access may be separately defined for the following types of management access methods:

- Telnet (CLI over Telnet sessions)
- Secure Telnet
- Web (HTTP)
- Secure Web (HTTPS, Using SSL)
- SNMP

This means, for example, that the set of managers allowed via Telnet may be different than the set of Web-based managers which is, in turn, may be different than the set of secure-web based managers, and so on.

A specific management access method may be completely disabled by denying all user access to it (e.g. denying all users access to CLI/Telnet management effectively disables CLI/Telnet as an available management interface to the system).

By default, management access to the system, through all methods, is enabled over all interfaces.

NOTE: If you enable management access through a physical port, all VLANs and IP interfaces on this port will be acceptable management traffic sources. If you enable management access through a VLAN, all ports and IP interfaces on that VLAN will be acceptable. If specific IP address(es) are specified, only traffic from these specified IP addresses on the appropriate ports will be accepted.

Access Profiles Rules (Advanced Mode)

Each management access profile is composed of at least one rule, which acts as a filter, and defines the device management method, interface type, source IP address, network mask, and the device management access action.

Users can be blocked or permitted management access.

Rule priority sets the order in which the rules are implemented. Assigning an access profile to an interface denies access via other interfaces. If an access profile is not assigned to any interface, the device can be accessed by all interfaces.

A total of 256 rules can be defined for all Management Access profiles.

To add rules to existing access profiles, see Profile Rules.

Creating an Access Profile

To define an access profile with a single rule:

1 Click **System** > **Management Security** > **Access Profiles** in the tree view to display the **Access Profiles: Summary** page.

The currently-defined access profiles are displayed.

2 To activate an access profile, select it in the **Active Access Profile** field.

If you select **Console Only**, active management of the device can only be performed using the console connection. This profile cannot be removed.

3 To add a new profile, click **Add**, and enter the fields:

- **Access Profile Name (1-32 Characters)** — Enter a name for the access profile.
- **Rule Priority (1-65535)** — Enter the rule priority. Rules are applied to packets according to their priority. These can be viewed in the **Profile Rules: Summary** page.
- **Management Method** — Select the management method to which the access profile is applied. Users using this management method are authenticated using this access profile. The possible options are:
  - **All** — The access profile is applied to all management methods.
  - **Telnet** — The access profile is applied to Telnet users.
  - **Secure Telnet (SSH)** — The access profile is applied to SSH users.
  - **HTTP** — The access profile is applied to HTTP users.
  - **Secure HTTP (HTTPS)** — The access profile is applied to HTTPS users.
  - **SNMP** — The access profile is applied to SNMP users.
- **Interface** — Check the fields and select the interface type to which the rule applies.
- **Enable Source IP Address** — Check this parameter to restrict access, based on the source IP address. When this field is not selected, the source IP address cannot be entered into a configured rule.
- **Supported IP Format** — Select whether the IPv4 or IPv6 format is supported for the source IP addresses.
- **Source IP Address** — Enter the interface source IP address for which the rule applies. This is an optional field and indicates that the rule is valid for a subnetwork.
- **Network Mask** — Enter the IP subnetwork mask if **Supported IP Format** is IPv4.
- **Prefix Length** — Enter the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Select whether to permit or deny management access to the defined interface. The possible options are:

- **Permit** — Permits access to the device.
- **Deny** — Denies access to the device.

Defining Access Profiles Using CLI Commands

The following table contains the CLI command for defining an access profile, without its rules. The CLI commands for defining the rules are described in Defining Access Profile Rules Using CLI Commands.

Table 7-23. Access Profile CLI Commands

CLI Command	Description
management access-list *name* **no management access-list** *name*	Defines an access-list for management. Use the no form of this command to delete an access list.

The following is an example of the CLI commands:

```
console(config)# management access-list mlist
console(config-macl)#
```

Profile Rules

If an access profile already exists, meaning that a single rule has been defined on it, use the **Profile Rules** pages to add additional rules to it.

To add a rule to a management access profiles:

1. Click **System** > **Management Security** > **Profile Rules** in the tree view to display the **Profile Rules: Summary** page.
2. Select an access profile name. Its rules are displayed in the order that they will be implemented.
3. To add a rule to the selected access profile, click **Add**.
4. Select an access profile from the Access Profile Name list.
5. Complete the fields that are defined in the **Access Profiles** section above.

Defining Access Profile Rules Using CLI Commands

The following table summarizes the CLI commands for adding rules to access profiles.

Table 7-24. Access Profiles CLI Commands

CLI Command	Description
permit [*interface-id*] [***service*** *service*]	Sets port permit conditions for the management access list.
permit ip-source {*ipv4-address* | *ipv6-address/prefix-length*} [***mask*** {*mask* | *prefix-length*}] [*interface-id*] [***service*** *service*]	Sets port permitting conditions for the management access list, and the selected management method.
deny [*interface-id*] [***service*** *service*]	Sets port denying conditions for the management access list, and the selected management method.
deny ip-source {*ipv4-address* | *ipv6-address/prefix-length*} [***mask*** {*mask* | *prefix-length*}] [*interface-id*] [***service*** *service*]	Sets port denying conditions for the management access list, and the selected management method.
management access-class {**console-only** | *name*}	Defines which access-list is used as the active management connections.
no management access-class	Use the no form of this command to disable management connection restrictions.
show management access-list [*name*]	Displays the active management access-lists.
show management access-class	Displays information about management access-class.

The following is an example of the CLI commands:

```
console(config)# management access-list mlist
console(config-macl)# permit gi0/1
console(config-macl)# permit gi0/2
console(config-macl)# deny gi0/3
console(config-macl)# deny gi0/4
console(config-macl)# exit
console(config)# management access-class mlist
console(config)# exit
console# show management access-list
mlist
-----
permit gi0/1
permit gi0/2
deny gi0/3
deny gi0/4
! (Note: all other access implicitly denied)
console# show management access-class
Management access-class is enabled, using access
list mlist
```

Authentication Profiles

In addition to access profiles, you can configure authentication for management access methods, such as SSH, console, Telnet, HTTP, and HTTPS.

User authentication can occur:

- Locally
- Via an external server, such as a TACACS+ or a RADIUS server

User authentication occurs in the order that the methods are selected, for example, if both the **Local** and **RADIUS** options are selected, the user is authenticated first locally. If the local user database is empty, the user is authenticated via the RADIUS server.

If an error occurs during the authentication, the next selected method is used.

If an authentication method fails, or the user has an insufficient privilege level, the user is denied access to the switch. The switch then stops, does not continue, and does not attempt to use the next authentication method.

If a privilege level is redefined, the user must also be re-defined.

User authentication can also be set to **None**, in which case no authentication is performed.

The process of configuring authentication for management access methods is divided into the following stages:

- Create an authentication profile, as described below
- Assign an authentication profile to a management method, as described in Select Authentication

To create an authentication profile:

1 Click **System** > **Management Security** > **Authentication Profiles** in the tree view to display the **Authentication Profiles: Summary** page.

   All currently-defined authentication profiles are displayed.

2 Click **Add** to add a new authentication profile, and enter the fields:

   – **Profile Name (1-12 Characters)** — Enter the name of the new authentication profile. Profile names cannot include blank spaces.

   – **Authentication Method: Optional Methods** — Select a user authentication methods that can be assigned to this authentication profile. The possible options are:

      - **Line** — The line password is used for user authentication (defined in Line Password).
      - **Enable** — The enable (encrypted) password is used for authentication (defined in Enable Password).
      - **Local** — The user authentication is performed by the device, which checks the user name and password for authentication.

- **RADIUS** — The user authentication is performed by the RADIUS server. For more information, see RADIUS.
- **TACACS+** — The user authentication is performed by the TACACS+ server. For more information, see TACACS+.
- **None** — No user authentication occurs.

Select a method by highlighting it in the **Optional Methods** list, and clicking on the right arrow to move it to the **Selected Methods** list.

Configuring an Authentication Profile Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **Authentication Profiles** pages.

Table 7-25. Authentication Profile CLI Commands

CLI Command	Description
aaa authentication login {***default*** | *list-name*} *method1* [*method2...*] **no aaa authentication login** {**default** | *list-name*}	Configures login authentication. Use the no form of the command to remove a login authentication profile.

The following is an example of the CLI commands:

```
console(config)# aaa authentication login default
radius local enable none
```

Select Authentication

After Authentication Profiles are defined, the Authentication Profiles can be assigned to Management Access methods, for example, console users can be authenticated by Authentication Profile 1, while Telnet users can be authenticated by Authentication Profile 2.

To assign an authentication profile to a management access method:

1. Click **System > Management Security > Select Authentication** in the tree view to display the **Select Authentication** page.
2. For the **Console**, **Telnet** and **Secure Telnet (SSH)** types of users, select either the default authentication profile or one of the previously-defined authentication profiles.

3 For **Secure HTTP** and **HTTP** types of users, select one or all of the **Optional Methods** and click the right-arrow to move them to the **Selected Methods**. The options are:

- **Local** — Authentication occurs locally.
- **None** — No authentication method is used for access.
- **RADIUS** — Authentication occurs at the RADIUS server.
- **TACACS+** — Authentication occurs at the TACACS+ server.

Assigning Access Authentication Profiles Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **Select Authentication** page.

Table 7-26. Select Authentication CLI Commands

CLI Command	Description
aaa authentication enable {**default** | *list-name*} *method* [*method2* ...]} **no aaa authentication enable** {***default*** | *list-name*}	Indicates the authentication method list when accessing a higher privilege level from a remote Telnet, Console or SSH.
enable authentication [***default*** | *list-name*] **no enable authentication**	Specifies the authentication method for accessing a higher privilege level from a remote Telnet or console. Use the no form of this command to restore the default authentication method.
login authentication [***default*** | *list-name*] no login authentication	Indicates the login authentication method list for a remote Telnet, Console or SSH. Use the no form of this command to restore the default authentication method.
ip http authentication aaa login-authentication *method1* [*method2...*] **no ip http authentication aaa login-authentication**	Indicates authentication methods for HTTP or HTTPS servers.

Table 7-26. Select Authentication CLI Commands *(continued)*

CLI Command	Description
show authentication methods	Displays information about the authentication methods.

The following is an example of the CLI commands that sets authentication for the console using the default method list that was previously-defined:

```
console(config)#line console
console(config-line)# enable authentication default
console(config-line)# login authentication default
console(config-line)# exit
```

The following is an example of the CLI commands that creates an authentication method list for http server access (RADIUS and local):

```
console(config)# ip http authentication aaa login-
authentication radius local
console(config)# exit
```

Active Users

To view active users on the device:

- Click **System** > **Management Security** > **Active Users** in the tree view to display the **Active Users** page.

  The following fields are displayed for all active users:

  - **Name** — Active users logged into the device.
  - **Protocol** — The management method by which the user is connected to the device.
  - **Location** — The user’s IP address.

Displaying Active Users Using CLI Commands

The following table summarizes the CLI commands for viewing active users connected to the device.

Table 7-27. Active Users CLI Commands

CLI Command	Description
show users	Displays information about active users.

The following example shows an example of the CLI command:

```
console> show users
Username     Protocol       Location
--------     --------       ---------
Bob           Serial
John          SSH           172.16.0.1
Robert        HTTP          172.16.0.8
Betty         Telnet        172.16.1.7
```

Local User Database

Use the **Local User Database** pages to define users, passwords and access levels.

To add a new user:

1. Click **System** > **Management Security** > **Local User Database** in the tree view to display the **Local User Database: Summary** page.

   All users are displayed even if they have been suspended.

   If a user has been suspended, it can be restored here by selecting the **Reactivate Suspended User** field.

2. To add a user, click **Add**, and enter the fields:

   – **User Name (1-20 characters)** — Enter the username of the user.

- **Access Level** — Select a user access level. The lowest user access level is 1 and 15 is the highest user access level. Users with access level 15 are Privileged Users, and only they can access and use the switch administrator.
- **Password (8-64 characters)** — Enter the password of the user.
- **Confirm Password** — Confirm the password of the user.

  The following fields are displayed:

  - **Expiry Date** — The expiration date of the user-defined password.
  - **Lockout Status** — Specifies whether the user currently has access (status *Usable*), or whether the user is locked out due to too many failed authentication attempts since the user last logged in successfully (status *Locked*).
  - **Reactivate Suspended User** — Check to reactivate the specified user's access rights. Access rights can be suspended after unsuccessfully attempting to login.

Configuring Local Users Using CLI Commands

The following table summarizes the CLI commands for configuring local users.

Table 7-28. Local User CLI Commands

CLI Command	Description
username *name* {**nopassword** | **password** *password* | **privilege** *privilege-level* | *unencrypted-password* | **encrypted** *encrypted-password*} **username** *name* **no username** *name*	Establishes a username-based authentication system. Use the no form to remove a user name.
set username *name* **active**	Reactivates a suspended user's access rights.
show user accounts	Displays users information.

The following is an example of the CLI commands:

```
console(config)# username bob password lee privilege
15
console# set username bob active
```

Line Password

To add a line password for Console, Telnet, and Secure-Telnet users:

1 Click **System** > **Management Security** > **Line Passwords** in the tree view to display the **Line Password** page.

2 Enter the fields for each type of user, separately:

- **Password (0 - 80 Characters)** — Enter the line password for accessing the device.
- **Confirm Password** — Confirm the line password.
- **Expiry Date** — Displays the expiration date of the line password.
- **Lockout Status** — Displays whether the user currently has access (status **Usable**), or whether the user is locked out due to too many failed authentication attempts since the user last logged in successfully (status **Locked**).
- **Reactivate Locked Line** — Check to reactivate the line password for a Console/Telnet/Secure Telnet session. Access rights can be suspended after a number of unsuccessful attempts to log in.

Assigning Line Passwords Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **Line Password** page.

Table 7-29. Line Password CLI Commands

CLI Command	Description
line {*console* | *telnet* | *ssh*}	Identifies a specific line for configuration and enters the Line Configuration command mode.
password *password* [***encrypted***] **no password**	Sets a password on a line. Use the no form of this command to remove the password.

The following is an example of the CLI commands:

```
console(config)# line console
console(config-line)# password dell
```

Enable Password

To set a local password to control access to Normal and Privilege levels activities.

1. Click **System > Management Security > Enable Password** in the tree view to display the **Enable Password** page.
2. **Enter the fields:**
   - **Select Enable Access Level** — Select the access level to associate with the enable password. The lowest user access level is **1** and **15** is the highest user access level. Users with access level 15 are Privileged Users, and only they can access and use the Network Administrator.
   - **Password (0-159 characters)** — Enter the enable password.
   - **Confirm Password** — Confirm the password.
   - **Expiry Date** — If Aging is selected, displays the expiration date of the enable password.
   - **Lockout Status** — Displays the number of failed authentication attempts since the user last logged in successfully (if the **Enable Login Attempts** checkbox is selected in the **Password Management** page.) Specifies **LOCKOUT**, when the user account is locked.
   - **Reactivate Suspended User** — Check to reactivate the specified user's access rights. Access rights can be suspended after unsuccessfully attempting to login.

Assigning Enable Passwords Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **Enable Password** page.

Table 7-30. Enable Password CLI Commands

CLI Command	Description
enable password [**level** *privilege-level*] {*unencrypted-password* | ***encrypted*** *encrypted-password*} **no enable password** [***level*** *level*]	Sets a local password to control access to user and privilege levels. Use the no form of this command to remove the password requirement.

The following is an example of the CLI commands:

```
console(config)# enable password level 15 secret
```

Password Management

Password management provides increased network security and improved password control. This feature is optional and must be enabled in the **Password Management** page.

Passwords for SSH, Telnet, HTTP, HTTPS, and SNMP access can be assigned security features that include:

- Minimum password lengths
- Password expiration dates (password aging)
- Prevention of frequent password reuse
- Lockout of users after failed login attempts
- Number of repeated characters allowed
- Number of different character classes required in the password. Numeric, alphabetic, and special characters are all character classes.

Password aging starts immediately after password management is enabled. However it is only effective if system time on the device is taken from an SNTP server. Passwords expire according to the user-defined expiration date/time. Ten days prior to password expiration, the device displays a password expiration warning message.

After the password has expired, users can log in a few additional times. During the remaining logins, an additional warning message displays informing the user that the password must be changed. If the password is not changed, users are locked out of the system, and can only log in using the console. Password warnings are logged in the SYSLOG file.

NOTE: Password aging is enabled only after setting the switch to use SNTP for setting time.

To define password management parameters:

1 Click **System > Management Security > Password Management** in the tree view to display the **Password Management** page.

2 Check the required fields and enter their values:

- **Enable Strong Passwords** — Check to enable this feature.
- **Number of Classes** — Select a number of character classes. The character classes are: upper case characters, lower case characters, digits and punctuation. The number of character classes selected indicates how many different types of characters must be in the password.
- **Repeated Characters** — Select the number of permissible repeated characters in the password.
- **Password Minimum Length (8-64 characters)** — When checked, specifies the minimum password length. Enter the minimum password length.
- **Enable Login Attempts** — When checked, enables locking a user out of the device when a faulty password is used more than the number of times entered. Select the maximum number of login attempts.
- **Global Password Aging (1-365)** — When checked, specifies that the password will expire in the number of days entered. Enter the number of days. This is only enabled after setting the switch to use SNTP for setting time
- **Consecutive Passwords Before Reuse (1-10)** — When checked, indicates the number of times a password must be changed, before the password can be reused. Select the number of times.
- **Password History Hold Time (1-365)** — When checked, the password history will be deleted after the number of days entered. Enter the number of days.

Password Management Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **Password Management** page.

Table 7-31. Password Management CLI Commands

CLI Command	Description
passwords strength-check enable **no passwords strength-check enable**	Enforces password strength checks. Use the no form of this command to disable enforcing password strength checks.
passwords strength *max-limit repeated characters* *number* **no passwords strength *max-limit repeated characters***	Defines the maximum number of characters in the new password that can be repeated consecutively. Use the no form of this command to disable enforcing limits of repeated characters and character classes.
passwords strength minimum character-classes *number* **no passwords strength minimum character-classes**	Defines the minimal classes required for passwords. Use the no form of this command to remove the requirement.
passwords min-length *length* **no passwords min-length**	Defines the minimum password length. Use the no form of this command to remove the restriction.
passwords aging *days* **no passwords aging**	Enforces password aging. Use the no form of this command to return to default.
passwords history *number* **no passwords history**	Defines the amount of times a password is changed, before the password can be reused.

Table 7-31. Password Management CLI Commands *(continued)*

CLI Command	Description
passwords history hold-time *days* **no passwords history hold-time**	Configures the duration that a password is relevant for tracking passwords history. Use the no form of this command to return to the default configuration.
passwords lockout *number* **no passwords lockout**	Defines the number of times a faulty password is entered before the user is locked out of the device. Use the no form of this command to disable the lockout feature.
show password configuration	Displays password management information.

The following is a sample script that sets password strength rules and creates a user with a valid password.

Table 7-32. CLI Script to Configure Strong Password

CLI Command	Description
console#**configure** console(conf)# **passwords strength-check enable**	Enable strong passwords.
console(config)# **passwords strength minimum character-classes** 3	Enable that passwords must contain at least three character classes.
password min-length 8	Enable that passwords must contain at least eight characters.
console(config)# **username** admin **privilege** 15 **password** FGH123!@#	Create a user named "admin" with privilege level 15 and password that fits the strength rules.

TACACS+

The device can act as a Terminal Access Controller Access Control System (TACACS+) client. TACACS+ provides centralized validation of users accessing the device, while still retaining consistency with RADIUS and other authentication processes.

TACACS+ provides the following services:

- **Authentication** — Provides authentication during login and via user names and user-defined passwords.
- **Authorization** — Performed at login after authentication. The TACACS+ server checks the privileges of the authenticated user.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the device and TACACS+ server.

To configure TACACS+ servers:

1. Click **System > Management Security > TACACS+** in the tree view to display the **TACACS+: Summary** page.

   The list of currently-defined TACACS+ servers is displayed. The parameters for each server is displayed, along with its connection status.

2. Enter the default parameters for TACACS+ servers. These values are used unless values are added in the **TACACS+ Add** or **Edit** pages.

   – **Key String (0-128 Characters)** — The authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. This key must match the encryption key sent by the TACACS+ server. This key is encrypted.

   – **Timeout for Reply (1-30)** — The amount of time that passes before the connection between the device and the TACACS+ server times out.

   – **Source IPv4** —(In Layer 2+ Static Routing mode only) Select the device IPv4 source interface to be used in messages for communication with the RADIUS server.

   – **Source IPv6** —(In Layer 2+ Static Routing mode only) Select the device IPv6 source interface to be used in messages for communication with the RADIUS server.

NOTE: The Auto option, which is the default option for the Source IPv4 and Source IPv6 fields, causes the system to take the source IP address from the IP address defined on the outgoing interface.

3 To add a TACACS+ server, click **Add**, and enter the fields on the page. The fields below are those that were not described on the **TACACS+: Summary** page.

- **Supported IP Format** — Select whether the **IPv4** or **IPv6** format is supported for the TACACS+ server IP address.
- **IPv6 Address Type** — Select whether the **Link-Local** or **Global** format of the **IPv6 Address** is supported for the TACACS+ server IP address.
- **Link Local Interface** — Select whether the link local address is the default VLAN or an ISATAP tunnel.
- **Host IP Address** — Enter the TACACS+ server IP address.
- **Priority (0-65535)** — Enter the order in which the TACACS+ servers are used if several are defined.
- **Key String (0-128 Characters)** — Enter the key of the TACACS+ server.
- **Authentication Port (0-65535)** — Enter the port number through which the TACACS+ session occurs.
- **Timeout for Reply (1-30)** — Enter the amount of time that passes before the connection between the device and the TACACS+ server times out.
- **Single Connection** — Check to maintain a single open connection between the device and the TACACS+ server.

Wherever available, check **Use Default** to use a value that was entered in the **TACACS+: Summary** page.

Defining TACACS+ Settings Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **TACACS+ Settings** pages.

Table 7-33. TACACS+ CLI Commands

CLI Command	Description
tacacs-server host {*ip-address* | *hostname*} [***single-connection***] [***port*** *port-number*] [***timeout*** *timeout*] [***key*** *key-string*] [***source*** *{source-ip}*] [***priority*** *priority*] **no tacacs-server host** {*ip-address* | *hostname*}	Configures a TACACS+ host. Use the no form of this command to delete the specified TACACS+ host.
tacacs-server key *key-string* **no tacacs-server key**	Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. Use the no form of this command to disable the key.
tacacs-server timeout *timeout* **no tacacs-server timeout**	Specifies the timeout value in seconds.
show tacacs [*ip-address*]	Displays configuration and statistics for a TACACS+ server.

The following is an example of the CLI commands:

```
console(config)# tacacs-server source-ip 172.16.8.1
console# show tacacs
Device Configuration
----------------------------
IP Address  Status  Port     Single      TimeOut  Source IP  Priority
                             Connection
---------- ------   ------   ----------  -------- ---------- --------
1.1.1.11   Not        49      No           Global   Global      10
           Connected
1.1.1.21   Not        49      No           Global   Global      19
           Connected
1.1.1.31   Not        49      No           Global   Global      18
           Connected
1.1.1.41   Not        49      No           Global   Global      17
           Connected
Global values
--------------
TimeOut : 5
-----------------------------
Source IP : 0.0.0.0
```

RADIUS

Remote Authentication Dial-In User Service (RADIUS) servers provide additional security for networks. Up to four RADIUS servers can be defined.

RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Secure Shell Access
- Web Access
- Console Access

To add a RADIUS server:

1 Click **System** > **Management Security** > **RADIUS** in the tree view to display the **RADIUS: Summary** page.

  The RADIUS default parameters and previously-defined RADIUS servers are displayed.

2 Enter the default parameters to be used when these parameters are not entered for a specific server.

  – **Default Retries (1-10)** — The default number of transmitted requests sent to RADIUS server before a failure occurs.

  – **Default Timeout for Reply (1-30)** — The default amount of the time (in seconds) that the device waits for an answer from the RADIUS server before timing out.

  – **Default Dead time (0-2000)** — The default amount of time (in minutes) that a RADIUS server is bypassed for service requests.

  – **Default Key String (0-128 Characters)** — The Default Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key is used for encryption.

  – **Source IPv4** —(In Layer 2+ Static Routing system mode only) Select the device IPv4 source interface to be used in messages for communication with the RADIUS server.

  – **Source IPv6** —(In Layer 2+ Static Routing system mode only) Select the device IPv6 source interface to be used in messages for communication with the RADIUS server.

NOTE: The Auto option, which is the default option for the Source IPv4 and Source IPv6 fields, causes the system to take the source IP address from the IP address defined on the outgoing interface.

3 To add a RADIUS server, click **Add**, and enter the fields:

  – **Supported IP Format** — Select whether the **IPv4** or **IPv6** format is supported.

  – **IPv6 Address Type** — Select whether the **Link-Local** or **Global** format of the **IPv6 Address** is supported.

- **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:
  - **VLAN 1**— The VLAN on which the IPv6 interface is configured.
  - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.
- **IP Address** — Enter the RADIUS server IP address.
- **Priority (0-65535)** — Enter the priority of the RADIUS server being added. 0 is the highest value. This is used to configure the order in which servers are queried.
- **Authentication Port (0-65535)** — Enter the authentication port used to verify the RADIUS server authentication. Enter 0 if you do not want this server to be used for authentication purposes.
- **Accounting Port (0-65535)** — Enter the accounting port, which is the UDP port number of the RADUS server used for accounting requests. Enter 0 if you do not want this server to be used for accounting purposes.
- **Usage Type** — Enter the RADIUS server usage. The possible options are:
  - **Login** — Used for login authentication and/or accounting.
  - **802.1x** — Used for 802.1x authentication and/or accounting.
  - **All** — Used for all types of authentication and/or accounting.

4. Enter the following fields if you do not want to use the default values entered in the **RADIUS: Summary** page. If you do want to use the default values, check **Use Default** for these fields.
   - **Number of Retries (1-10)** — Enter the number of requests sent to the RADIUS server before a failure occurs.
   - **Timeout for Reply (1-30)** — The amount of the time in seconds that the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server.
   - **Dead Time (0-2000)** — The amount of time (in minutes) that a RADIUS server is bypassed for service requests.

– **Key String (0-128 Characters)** — The key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server.

Defining RADIUS Servers Using CLI Commands

The following table summarizes the CLI commands for defining fields displayed on the **RADIUS** pages.

Table 7-34. RADIUS Server CLI Commands

CLI Command	Description
radius-server host {*ipv4-address* | *ipv6-address* | *ipv6z-address* | *hostname*} [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**source** {*source-ip*}] [**priority** *priority*] [**usage** {**login** | **802.1x** | **all**}] **no radius-server host** {*ip-address* | *hostname*}	Specifies a RADIUS server host. Use the no form of the command to delete the specified RADIUS server host.
radius-server timeout *timeout-seconds* **no radius-server timeout**	Sets the interval for which a device waits for a server host to reply. Use the no form of this command to restore the default configuration.
radius-server retransmit *retries* **no radius-server retransmit**	Specifies the number of times the software searches the list of RADIUS server hosts. Use the no form of this command to restore the default configuration.
radius-server deadtime *deadtime* **no radius-server deadtime**	Configures unavailable servers to be skipped. Use the no form of this command to restore the default configuration.

Table 7-34. RADIUS Server CLI Commands *(continued)*

CLI Command	Description
radius-server key [*key-string*] **no radius-server key**	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. Use the no form of this command to restore the default configuration.
show radius-servers	Displays the RADIUS server settings.

The following is an example of CLI commands:

```
console(config)# radius-server host 192.168.10.1
auth-port 20 timeout 20

console(config)# radius-server key enterprise-server

console# show radius-servers

  IP address    Port  Port  Time-   Ret-  Dead-    Source IP    Prio. Usage

                Auth  Acct  Out     rans  Time
-------------- ----- ----- ------ ------ ------ -------------- ----- ---
   1.1.1.11     1812  1813  Global Global Global     Global       10    all
   1.1.1.21     1812  1813  Global Global Global     Global       19    all
   1.1.1.31     1812  1813  Global Global Global     Global       18    all
   1.1.1.41     1812  1813  Global Global Global     Global       17    all
   1.1.1.51     1812  1813  Global Global Global     Global       16    all
Global values
--------------
TimeOut : 3
Retransmit : 3
Deadtime : 0
Source IP : 0.0.0.0
Source IPv6 : ::
```

SNMP

This section describes the Simple Network Management Protocol (SNMP) for managing network devices.

It contains the following topics:

- SNMP Overview
- Global Parameters
- View Settings
- Access Control
- User Security Model
- Communities
- Notification Filter
- Notification Recipients

SNMP Overview

The switch supports the SNMPv1, SNMPv2 and SNMPv3.

SNMP v1 and v2

The SNMP agent maintains a list of variables that are used to manage the switch. These variables are stored in the Management Information Base (MIB) from which they may be presented. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

SNMPv1 and v2 are enabled by default.

SNMP v3

In addition to the features provided by SNMPv1 and SNMPv2, SNMPv3 applies access control and a new trap mechanism to SNMPv1 and SNMPv2 PDUs. In addition, a User Security Model (USM) can be defined, which includes:

- **Authentication** — Provides data integrity and data origin authentication.

- **Privacy** — Protects against disclosure of message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication alone can be enabled on an SNMP message, or both authentication and privacy can be enabled on an SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management** — Defines key generation, updates, and use.

The switch supports SNMP notification filters, based on Object IDs (OIDs), which are used by the system to manage switch features.

Authentication or Privacy Keys are modified in the **User Security Model (USM)**.

SNMPv3 can only be enabled if the Local Engine ID is enabled.

SNMP Access Rights

Access rights in SNMP are managed in the following ways:

- **SNMPv1 and SNMPv2** — Communities

  The community name is a password sent by the SNMP management station to the device for authentication purposes.

  A community string is transmitted along with the SNMPv1,v2 frames, but neither the frames nor the community string are encrypted. Since SNMPv1 and SNMPv2 are not encrypted, they are not secure.

  Communities can be associated with views or groups, and they are defined in the **Community** pages.

- **SNMPv3** — Users and Groups

  SNMP v3 works with users instead of communities. The users belong to groups that have access rights assigned to them. Users are defined in the **User Security Model** pages

  SNMPv3 provides two security mechanisms:

  - **Authentication** — The switch checks that the SNMP user is an authorized system administrator. This is done for each and every frame.

- **Privacy** — SNMP frames can carry encrypted data.

These mechanisms can be combined to provide three levels of security:

- No security
- Authentication
- Authentication and Privacy. Note that for both authentication and privacy to be enabled, two groups with the same name, one with authentication and one with privacy, must be created.

A group is a label for a combination of attributes that determines whether members have read, write, and/or notify privileges. Users can be associated with a group. A group is operational only when it is associated with an SNMP user.

Global Parameters

The Engine ID is used by SNMPv3 entities to uniquely identify themselves. Both a remote and local Engine ID can be specified.

An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set), and sends trap messages to a manager. The agent's local information is encapsulated in fields in the message.

Each SNMP agent maintains local information that is used in SNMPv3 message exchanges (not relevant for SNMPv1 or SNMPv2). The default SNMP Engine ID is comprised of the enterprise number and the default MAC address. The SNMP engine ID must be unique for the administrative domain, so that no two devices in a network have the same engine ID.

The local information is stored in four read-only MIB variables: snmpEngineId, snmpEngineBoots, snmpEngineTime, and snmpEngineMaxMessageSize.

To configure SNMP:

1. Click **System > SNMP > Global Parameters** in the tree view to display the **Global Parameters** page.

   The global parameters are displayed.

2. Enter the fields:

   – **Local Engine ID (10-64 Hex Characters)** — Check and enter the local device engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled.

   – **Use Default** — Check to use the device-generated Engine ID. The default Engine ID is based on the device MAC address, and is defined per standard as:

     - **First 4 octets** — First bit = 1, the rest is IANA Enterprise number = 674.
     - **Fifth octet** — Set to 3 to indicate the MAC address that follows.
     - **Last 6 octets** — MAC address of the device.

   – **SNMP Notifications** — Enable/disable the switch sending SNMP notifications.

   – **Authentication Notifications** — Enable/disable the switch sending SNMP traps when authentication fails.

3. To add a remote Engine ID, click **Add**.

4. Enter the following fields:

   – **Supported IP Format**— Select either IPv4 or IPv6.

   – **IPv6 Address Type** — This can be either a Link Local or Global IPv6 address.

   – **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:

     - **VLAN 1**— The VLAN on which the IPv6 interface is configured.
     - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.

- **IP Address** — Enter the IP address.
- **Engine ID**— Enter the remote Engine ID.

Setting SNMP Global Parameters Using CLI Commands

The following table summarizes the CLI commands for setting fields in the **Global Parameters** page.

Table 7-35. SNMP Global Parameters Commands

CLI Command	Description
snmp-server engineID local {*engineid-string* | ***default***} **no snmp-server engineID local**	Specifies the local device engine ID. The field values is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. The Engine ID must be defined before SNMPv3 is enabled. Use the no form of this command to remove the configured engine ID.
snmp-server engineID remote *{ip-address} engineid-string* **no snmp-server engineID remote {***ip-address***}**	Specifies the remote device engine ID. The field values is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. The Engine ID must be defined before SNMPv3 is enabled. Use the no form of this command to remove the configured engine ID.
snmp-server enable traps **no snmp-server enable traps**	Enables the router to send Simple Network Management Protocol traps. Use the no form of the command to disable SNMP traps.
snmp-server trap authentication **no snmp-server trap authentication**	Enables the router to send Simple Network Management Protocol traps when authentication fails. Use the no form of this command to disable SNMP failed authentication traps.

Table 7-35. SNMP Global Parameters Commands *(continued)*

CLI Command	Description
`show snmp`	Checks the status of SNMP communications.

The following is an example of the CLI commands:

```
console(config)# snmp-server enable traps

console(config)# snmp-server trap authentication

console(config)# snmp-server engineid local default

The engine-id must be unique within your
administrative domain.

Do you wish to continue? [Y/N]y

The SNMPv3 database will be erased. Do you wish to
continue? [Y/N]y
```

View Settings

An SNMP view, which is a collection of MIB subtrees, provides or blocks access to device features.

Each subtree is defined by the Object ID (OID) of the root of its subtrees. In extreme cases this subtree can be a leaf. Well-known names can be used to specify the root of the desired subtree, or an OID can be entered (see Global Parameters).

Each subtree is either included in or excluded from the view being defined.

Views can be attached to groups in the **Access Control** pages.

To create an SNMP view:

1. Click **System** > **SNMP** > **View Settings** in the tree view to display the **View Settings: Summary** page.
2. Select a view name. Its subtrees are displayed.
3. To remove a subtree from an SNMP view, click **Remove**. The subtrees of the default views (Default, DefaultSuper) cannot be changed.
4. To add a new view, click **Add**, and enter a new **View Name (1-30 Characters)**.

5 To complete the definition of the view, click **Edit**, and select a **View Name** to modify. Enter the fields:

   – **New Object ID Subtree** — Check to specify the device feature OID included or excluded in the selected SNMP view.

      - **Select from List** — Select the device feature OID by using the **Up** and **Down** buttons to scroll through a list of all device OIDs.

     Or:

      - **Insert** — Specify the device feature OID.

   – **View Type** — Specify if the defined OID branch will be included or excluded in the selected SNMP view.

Defining SNMP Views Using CLI Commands

The following table summarizes the CLI commands for defining fields displayed in the **View Settings** pages.

Table 7-36. SNMP View CLI Commands

CLI Command	Description
`snmp-server view` *`view-name oid-tree`* `{`**`included`** `|` **`excluded`**`}`	Creates or updates a SNMP server view entry.
`no snmp-server view` *`view-name`* `[`*`oid-tree`*`]`	Use the no form of this command to remove an SNMP server view entry.
`show snmp views` `[`*`viewname`*`]`	Displays the configuration of a view or all views.

The following is an example of CLI commands:

```
console(config)# snmp-server view user1 1 included

console(config)# end

console# show snmp views
Name          OID Tree          Type
-----------   --------------    --------
user1         system            included
Default       iso               included
Default       snmpVacmMIB       excluded
Default       usmUser           excluded
Default       rndCommunityTab   excluded
              le
DefaultSuper  iso               included
```

Access Control

For ease of use, users may be assigned to groups. In this way, it is possible to assign feature access rights to an entire group, instead of assigning them individually to users. Users are created in the **User Security Model** pages.

Groups can be defined in any version of SNMP, but only SNMPv3 groups can be assigned authentication methods.

To add an SNMP group, and assign it access control privileges:

1 Click **System** > **SNMP** > **Access Control** in the tree view to display the **Access Control: Summary** page.

  Previously-defined groups are displayed.

2 To add a new group, click **Add**, and enter the fields:

  – **Group Name (1-30 Characters)** — Enter a group name.

  – **Security Model** — Select the SNMP version of the group.

  – **Security Level** — Select the security level attached to the group. Security levels apply to SNMPv3 only. The possible options are:

    • **No Authentication** — Neither authentication nor the privacy security levels are assigned to the group.

    - **Authentication** — Authenticates SNMP messages, and ensures that the origin of the SNMP message is authenticated.
    - **Privacy** — Encrypts SNMP message.
  - **Operation** — Select the group access rights. The possible options are:
    - **Read** — The management access is restricted to read-only, and changes cannot be made to the assigned SNMP view. If desired, select a view from the drop-down list.
    - **Write** — The management access is read-write and changes can be made to the assigned SNMP view. If desired, select a view from the drop-down list.
    - **Notify** — Sends traps for the assigned SNMP view. If desired, select a view from the drop-down list.

Defining SNMP Access Control Using CLI Commands

The following table summarizes the CLI commands for defining fields displayed in the **Access Control** pages.

Table 7-37. SNMP Access Control CLI Commands

CLI Command	Description
snmp-server group *groupname* {**v1** **|** **v2** **|** **v3** {***noauth*** | ***auth*** | ***priv***} [***notify*** *notifyview*]} [**read** *readview*] [**write** *writeview*]	Configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views.
no snmp-server group *groupname* {***v1*** | ***v2*** | ***v3*** [***noauth*** | ***auth*** | ***priv***]}	Use the no form of this command to remove a specified SNMP group.
show snmp groups [*groupname*]	Displays the configuration of groups

The following is an example of the CLI commands:

```
console (config)# snmp-server group user-group v3
priv read user-view

console# show snmp groups

Name      Security                Views

      Model    Level     Read     Write     Notify

----- -----    -------   -------  -------   --------
--

1     V1     noauth     -         -          -

2     V1     noauth     -         -          -

3     V1     noauth     -         -          -

4     V1     noauth     -         -          -

5     V1     noauth     -         -          -
```

User Security Model

An SNMP user is defined by the following:

- Login credentials (username, password, and authentication method)
- Context and scope in which the user operates
- Association with a group
- Engine ID

SNMP user login credentials are verified using a local database.

After a user is authenticated, it takes on the attributes of its group, and can then access the views permitted to this group. A user can only be a member of a single group.

Before you create an SNMPv3 user, create an SNMPv3 group in the **Access Control** pages.

When the configuration file is saved, SNMP communities/users are not saved. This means that if you configure another device with this configuration file, you must define the SNMP communities/users on that device.

To create an SNMP V3 user, and assign it to a group and view:

1 Click **System** > **SNMP** > **User Security Model** in the tree view to display the **User Security Model: Summary** page.

   The currently-defined users and their groups are displayed.

2 To add a user, click **Add**, and enter the fields:

   – **User Name** (1-30 Characters) — Enter a new user name.

   – **Engine ID** — Specifies the local or remote SNMP entity, to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database. Select either **Local** or **Remote**. If **Remote** is selected, enter the remote engine ID.

   – **Group Name** — Select from a list of user-defined SNMP groups. SNMP groups are defined in the **Access Control Group** pages.

   – **Authentication Method** — Select an authentication method used to authenticate users. The possible options are:

     - **None** — No user authentication is used.
     - **MD5** Key — Users are authenticated using the HMAC-MD5 algorithm.
     - **SHA** Key — Users are authenticated using the HMAC-SHA-96 authentication level.

   – **Authentication Password (1-32 Characters)** — If the MD5 Key or SHA Key authentication method was selected, enter the user-defined password for a group.

   – **Privacy Method** — If the MD5 Key or SHA Key authentication method was selected, enable the DES privacy method or None.

   – **Privacy Password** (16 Hex Characters) — If the DES privacy method is selected, enter the user-defined password.

Defining SNMPv3 Users Using CLI Commands

The following table summarizes the CLI commands for defining fields displayed in the **User Security Model** pages.

Table 7-38. SNMP Users CLI Commands

CLI Command	Description
snmp-server user *username groupname* {***v1*** | ***v2c*** | [**remote** *host*] ***v3*** [***auth*** {***md5*** | ***sha***} *auth-password* [**priv** *priv-password*]]} **no snmp-server user** *username* [*remote-host*]	Configures a new SNMP V3 user. Use the no form of the command to remove a user.
show snmp users [*username*]	Displays the configuration of users.

The following is an example of the CLI commands:

```
console(config)# snmp-server user tom acbd v1

console(config)# snmp-server user tom acbd v2c

console(config)# snmp-server user tom acbd v3
```

Communities

When using SNMP v1,2, communities strings (passwords) are used to provide access rights in the following ways:

- **Basic Table** — The access rights of a community can be read-only, read-write, or SNMP Admin. In addition, you can restrict access to the community to only certain MIB objects using a **view**. Views are defined in the **Views Setting** pages.
- **Advanced Table** — Access rights to a community are assigned to a group that consists of users. A group can have Read, Write, and Notify access to views. Groups are defined in the **Access Control** pages.

To define an SNMP community:

1. Click **System > SNMP > Communities** in the tree view to display the **Communities: Summary** page.

   The Basic and Advanced tables are displayed.

2. To add a new community, click **Add**.
3. Define the SNMP management station by entering its IP address information:
   - **Supported IP Format** — Select whether the IPv4 or IPv6 format is being used.
   - **IPv6 Address Type** — When the community supports IPv6, this specifies the type of static address supported. The possible options are:
     - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
     - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.
   - **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:
     - **VLAN 1** — The VLAN on which the IPv6 interface is configured.
     - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.
   - **SNMP Management Station** — Enter the management station IP address for which the SNMP community is defined, or choose **All** to be able to receive SNMP messages from anywhere.
   - **Community String (1-20 Characters)** — Enter the community string, which functions as a password, and is used to authenticate the management station to the device.
4. To associate access mode and views directly with the community, enter the fields:
   - **Basic** — Check to enable SNMP Basic mode for a selected community.
   - **Access Mode** — If Basic is selected, specify the access rights of the community. The possible options are:
     - **Read-Only** — Management access is restricted to read-only, and changes cannot be made to the community.
     - **Read-Write** — Management access is read-write and changes can be made to the device configuration, but not to the community.

    - **SNMP Admin** — User has access to all device configuration options, as well as permissions to modify the community.
  - **View Name** — Select a view from a list of user-defined SNMP views. The view determines other characteristics associated with the community.

5 To use Advanced mode, enter the fields:

  - **Advanced** — When SNMP Advanced mode is selected, you can select an SNMP group to specify the SNMP access control rules for the selected community. The SNMP Advanced mode is defined only with SNMPv3.
  - **Group Name** — Select the group to be associated with the community.

Configuring Communities Using CLI Commands

The following table summarizes the CLI commands for setting fields in the **Community** pages.

Table 7-39. SNMP Community CLI Commands

CLI Command	Description
snmp-server community *community-string* [**ro** | **rw** | **su**] [ipv4-address | ipv6-address] [**mask** *mask* | **prefix** *prefix-length*] [**view** view-name] **no snmp-server community** *community-string* [*ip-address*]	Sets up the community access string to permit access to the SNMP protocol. Use the no form of this command to remove the specified community string
snmp-server community-group *community-string group-name* [ipv4-address | ipv6-address] [**mask** *mask* | **prefix** *prefix-length*]	Sets up community access string to permit limited access to the SNMP protocol, based on group access rights.
show snmp	Displays the current SNMP device configuration.

The following is an example of the CLI commands:

```
console (config)# snmp-server community dell ro
10.1.1.1
```

Notification Filter

Notification filters determine the type of SNMP notifications that are sent to the management station, based on the OID of the notification to be sent. Each OID is linked to a device feature or a feature aspect.

SNMP notification filters provide the following services:

- Identification of management trap targets
- Trap filtering
- Selection of trap generation parameters
- Access control checks

After creating a notification filter, attach it to a notification recipient in the **SNMPv1,2 Notification Recipients** pages.

To add a notification filter:

1 Click **System > SNMP > Notification Filter** in the tree view to display the **Notification Filter: Summary** page.

2 The OIDs of the selected filter are displayed.

3 If required, the notification filter type can be changed by selecting one of the following options:

   – **Excluded** — OID traps or informs will not be sent.

   – **Included** — OID traps or informs will be sent.

4 To add a new notification filter, click **Add**.

5 In addition to the fields described in the **Summary** page, enter the fields:

   – **Filter Name (1-30 Characters)** — Enter the notification filter name.

   – **New Object Identifier Tree** — Check to specify the device feature OID included or excluded in the selected SNMP view.

      - **Select from List** — Select the device feature OID by using the **Up** and **Down** buttons to scroll through a list of all device OIDs.

or:

- **Object ID** — Specify the device feature OID.

– **Filter Type** — Select whether the defined OID branch will be **Included** or **Excluded** in the selected SNMP view.

Configuring Notification Filters Using CLI Commands

The following table summarizes CLI commands for defining fields displayed in the **Notification Filter** pages.

Table 7-40. SNMP Notification Filter CLI Commands

CLI Command	Description
snmp-server filter *filter-name oid-tree* {**included** | **excluded**}	Creates or updates an SNMP notification filter.
no snmp-server filter *filter-name* [*oid-tree*]	Use the no form of this command to remove the specified SNMP server filter entry.
show snmp filters [*filter-name*]	Displays the configuration of SNMP notification filters

The following is an example of CLI commands:

```
console (config)# snmp-server filter user1 iso
included
console(config)# end
console # show snmp filters

Name          OID Tree       Type
-----------   -------------  --------
user1         iso            Included
```

Notification Recipients

An SNMP notification is a trap message, sent from the switch to the SNMP management station, indicating that a certain event has occurred, such as a link up or down.

Trap receivers, also known as notification recipients, are network nodes to which trap messages are sent by the switch.

A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that will be included in the trap message. When an event arises that requires a trap message to be sent, it is sent to every node listed in the trap receiver list.

Some messages are of an informational nature and are called "informs" instead of traps.

To add notification recipients, and attach them to notification filters:

1. Click **System > SNMP > Notification Recipients** in the tree view to display the **Notification Recipients: Summary** page.

   The previously-defined notification recipients are displayed.

2. To add a new notification recipient, click **Add**, and enter the fields:
   - **Supported IP Format** — Select whether the IPv4 or IPv6 format is supported.
   - **IPv6 Address Type** — When the recipient supports IPv6, this specifies the type of static address supported. The possible options are:
     - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
     - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.
   - **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:
     - **VLAN 1**— The IPv6 interface is configured on this VLAN.
     - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.
   - **Recipient IP** — The IP address to whom the traps are sent.
   - **Notification Type** — The notification sent. The possible options are:
     - **Traps** — Traps are sent.
     - **Informs** — Informs are sent.

If SNMP versions 1 and 2 are enabled for the selected recipient, enter the fields:

- **Community String** — The community string of the trap manager.
- **Notification Version** — The message trap SNMP version (v1 or v2).

If SNMPv3 is used to send and receive traps, enter the fields:

- **User Name** — The user to whom SNMP notifications are sent.
- **Security Level** — The means by which the packet is authenticated. The possible options are:
  - **No Authentication** — The packet is neither authenticated nor encrypted.
  - **Authentication** — The packet is authenticated.
  - **Privacy** — The packet is both authenticated and encrypted.

3. Enter the fields for all versions of SNMP:
   - **UDP Port (1-65535)** — The UDP port used to send notifications. The default is 162.
   - **Filter Name** — Select an SNMP filter from a list of previously-defined SNMP filters.
   - **Timeout (1-300)** — The amount of time (seconds) the device waits before resending informs.
   - **Retries (1-255)** — The amount of times the device resends an inform request.

Configuring SNMP Notification Recipients Using CLI Commands

The following table summarizes the CLI commands for setting fields in the **Notification Recipients** pages.

Table 7-41. SNMP Notification CLI Commands

CLI Command	Description
snmp-server host {*host-ip* | *hostname*} [***traps*** | ***informs***] [**version** {*1* |*2c* | *3* [***auth*** | ***noauth*** | ***priv***]}] *community-string* [***udp-port*** *port*] [***filter*** filtername] [***timeout*** seconds] [**retries** retries]	Creates or updates a notification recipient receiving notifications in SNMP version 1, 2 or 3. Use the no form of this command to remove the specified host.
no snmp-server host {*ip-address* | *hostname*} [***traps*** | ***informs***] [*version* {*1* | *2c* | *3*}]	
show snmp	Shows the current SNMP configuration.

The following is an example of the CLI commands:

```
console(config)# snmp-server host 172.16.1.1 private

console(config)# end

console# show snmp

Community-     Community-    View Name  IP Address
String         Access

-------------  ------------  ---------  ----------

public         read only     user-view  All

private        read write    default    172.16.1.1

private        su            DefaultSu  172.17.1.1
                             per
```

File Management

This section describes how to manage device firmware (image files) and configuration files. It contains the following topics:

- File Management Overview
- Auto-Update/Configuration Feature
- File Download
- File Upload
- Active Images
- Copy Files
- File System

File Management Overview

This section describes the system files found in the system and how they can be updated (downloaded) and backed up (uploaded).

System Files

The following system files are maintained on the system:

- **Startup Configuration File** — Files with extension **.text**. These files contain the commands required to configure the device at startup or after reboot. The Startup Configuration file is created from the Running Configuration file, or can be created from another file.
- **Running Configuration File** — Files with extension **.text**. These files contain all Startup Configuration file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost.

  During the startup process, all commands in the Startup Configuration file are copied to the Running Configuration file, and applied to the device.

  During the session, new configuration commands are added to the Running Configuration file. To update the Startup Configuration file with these configuration commands, the Running Configuration file must first be copied to the Startup Configuration file before powering down the device. This can be done manually in the Copy Files page or see Auto-

Update/Configuration Feature for more information about how to perform this automatically.

- **Image Files**—Files with extension **.ros**. System file images are saved in two flash files called Image 1 and Image 2. The active image contains the active copy, while the other image contains a backup copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the software upgrade process.

Downloading/Uploading System Files

System files can be manually loaded from (downloaded) or copied to (uploaded) a TFTP server. This can be done in one of the following ways:

- **Manually**—System files can be downloaded using the *File Download* page and uploaded using the *File Upload* page.
- **Automatically (Auto Update/Configuration)**—System files can be downloaded automatically, as follows:
  - **Auto-Configuration**—If the Auto-Configure feature is enabled (in the Auto Update of Configuration/Image File page), the Startup Configuration file (in various conditions described below) might be automatically updated after reboot.
  - **Auto-Update**—If the Firmware Auto-Update feature is enabled in the Auto Update of Configuration/Image File page, the image file is might be automatically updated (in various conditions described below).

Auto-Update/Configuration Feature

The Auto-Update/Configuration feature enables initial configuration of the device and upgrading of the firmware through an automatic process, which enables the administrator to ensure that the configuration/firmware of all the devices in the network is up-to-date.

The required configuration files/images are stored on a TFTP server, and these are downloaded to all the devices in the network when the device boots up instead of booting from a local startup configuration file.

Auto-Update/Configuration also enables quick installation of new devices on the network, since an out-of-box device can be configured to retrieve its configuration file from the network, allowing instant access to it from the administrator's management station and up-to-date configuration on the device.

Triggering the Auto Update of Configuration/Image File Process

When the Auto-Update/Configuration feature is enabled (in the Auto Update of Configuration/Image File page), the device automatically attempts to download a new image or configuration file (under certain circumstances) using one of the following processes:

- The Auto-Update from a TFTP server is triggered if the following conditions are fulfilled:
  - An IP address of a TFTP server is received from a DHCP server.
  - A file name is received from DHCP server.
- The Auto-Configuration from a TFTP server is triggered if the following conditions are fulfilled:
  - The switch as DHCP client received a configuration file name or a TFTP URL.
  - Force Configuration Download at Next Startup enabled by the boot host dhcp command, or, the Startup Configuration file is empty.

  See Preparations for Using Auto Configuration from a TFTP Server.

Automatic DHCP IP Interface Assignment

The user can manually define a DHCP interface in the DHCP IPv4 page.

If the user does not do this, the switch automatically creates a DHCP interface on the VLAN with the lowest VLAN ID that does not have an IP address defined on it after boot if both of the following conditions are fulfilled:

- There is no DHCP IP interface.
- There is a VLAN without an IP address.

Preparations for Using Auto Configuration from a TFTP Server

The **Auto-Update/Configuration** feature enables configuring the device from a configuration file found on the TFTP server.

Two methods may be used:

- One-file Read, described in Auto Configuration (One File Read Method). This method is used if a configuration file is found on the TFTP server.
- Multi-file Read, described in Auto Configuration (Multi File Read Method). This method is used if a configuration file name is not found on the DHCP server, or the configuration file is not found on the TFTP server.

Auto Configuration (One File Read Method)

This method requires the following preparations on the DHCP and TFTP servers:

- **TFTP Server**

  Place a configuration file, for example **config.txt** in the main directory. This file can be created by copying a configuration file from a device. When the device is booted this becomes the Running configuration file.

- **DHCP Server**
  - Configure the DHCP server with option 67 and the name of the configuration file on the TFTP server (for example, **config.txt**).
  - Configure the DHCP server with option -20 or 66. This is the IP address of the TFTP server.
- **Device -** On the device, one of the following cases may exist:
  - If **Configuration Auto-Config** is selected, the device is configured with the configuration file on the TFTP server only if the Startup configuration file is empty.
  - If **Force Configuration Download at Next Startup** is selected, the device is configured with the configuration file on the TFTP server whether the Startup configuration file is not empty or not.

Auto Configuration (Multi File Read Method)

If the one-file method has failed and the TFTP Server IP address has been provided by the DHCP Server, the switch applies the multi-file method to download the configuration file. The following steps are performed by the switch:

- The switch gets the hostname, as described below.
  - If the hostname was provided by the DHCP server, this hostname is used.
  - If the hostname has not been provided by a DHCP server, and if the user has configured the **sysName** variable, its value is used as a hostname.
  - If neither of the above occurred, the switch uses the **fp-net.cfg** Filename List on the TFTP server. Each file in this list is a text file containing commands, each of which:
    - Occupies one line.
    - Has the following format: **ip host** *hostname ip-addr*. Each line maps an IP address to a hostname. When the switch identifies its own IP address in this list, the hostname associated with it is used.
- The switch tries to download a configuration file with the following names:
  - **hostname-config**
  - **hostname.cfg** if the previous file does not exist
  - **host.cfg** if the previous files do not exist

Preparations for Firmware Image Download from TFTP

When an image file is downloaded from TFTP, the following steps are performed:

- The switch downloads the Indirect Image File and extracts from it the name of the image file.

NOTE: If the size of the image name bigger than 160 octets only the first 160 octets will be used.

- If the image file version differs from the current image file version, then the image file is loaded and the switch is rebooted.

Using DHCP and TFTP servers require the following preparations:

- **TFTP Server**
  - Create a sub directory in the main directory. Place a software image file in it.
  - Create an indirect file that contains a path and the name of the software version (for example indirect-VRTX.txt that contains VRTX\VRTX-version.ros).
  - Copy this file to the TFTP server's main directory
- **DHCP Server**
  - Configure the DHCP server with option -20 or 66. This is the IP address of the TFTP server.
  - Configure the DHCP server with option 125. Enter the following information:
    - A2-02-00-00 — Enterprise Number 674 (Dell PowerEdge VRTX value). It should be written from right to left. 674=02 a2
    - 15 — Data Length
    - 01 — Sub option code 1 (Dell PowerEdge VRTX value)
    - 13 — Sub option length
    - Conversion of the file name (in the above example: conversion of **indirect-VRTX.txt** from ASCII to HEX - 69-6E-64-69-72-65-63-74-2D-63-6F-6E-74-61-78-2E-74-78-74

Auto Update of Configuration/Image File

To set the auto update and configuration parameters:

NOTE: For the automatic options in this page to work the following must be implemented:

- Since Auto-Config depends on retrieving information from a DHCP server, the startup configuration needs to include a DHCP IP interface. The device is defined as a DHCP client, as described in IPv6 Interface or IPv4 Interface. After reboot, this command is not saved in the Startup configuration.
- Preparations described above must be completed on the DHCP server and TFTP servers.

1 Click **System > File Management > Auto Update of Configuration/Image File** in the tree view to display the **Auto Update of Configuration/Image File** page.

The auto-update-configuration options are displayed.

2 Modify the auto-update configuration parameters as required:

– **Configuration Auto-Config (boot host auto-config)**— Enable/disable automatic download of the configuration parameters to the Running Configuration file. By default, this occurs only if the Startup Configuration file is empty.

– **Firmware Auto-Update (boot host auto-update)**— Enable/disable automatic download of the image file.

– **Force Configuration Download at Next Startup (boot host dhcp)** — Enable/disable the **Configuration Auto Update** option to work even if the Startup Configuration file is not empty.

– **Auto-Copy Running Configuration to Startup Configuration After Download (boot host auto-save)**— Enable/disable the Running Configuration file to be automatically copied to the Startup Configuration file after downloading the Running Configuration file.

Auto Update Configuration Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **Auto Update of Configuration/Image File** page.

Table 7-42. Auto Update of Configuration/Image File CLI Commands

CLI Command	Description

`boot host auto-config`
`no boot host auto-config`
	Enables the support of auto-configuration via DHCP.
	Use the no form of this command to disable DHCP auto configuration.

`boot host auto-update`
`no boot host auto-update`
	Enables the support of auto-update via DHCP.
	Use the no form of this command to disable DHCP auto configuration

Table 7-42. Auto Update of Configuration/Image File CLI Commands *(continued)*

CLI Command	Description
boot host dhcp **no boot host dhcp**	Forces the mechanism used to download a configuration file at the next system startup. Use the no form of this command to restore the host configuration file to the default.
boot host auto-save **no boot host auto-save**	Enables automatic saving of Running configuration in Startup configuration after download. Use the no form of this command restore default behavior
show boot	Shows the status of the IP DHCP Auto Config process.

The following is an example of the CLI command to view the Auto-Update status:

```
console# show boot

Auto Config

-----------

Config Download via DHCP: enabled

Next Boot Config Download via DHCP: force

Auto Update

-----------

Image Download via DHCP: enabled
```

The following is an example of the CLI command to configure auto-update on the switch:

```
console# configure

console(config)# boot host auto-save

console(config)# interface vlan 1

console(config-if)# ip address dhcp

console(config-if)# 01-Oct-2006 15:19:51 %BOOTP_DHCP_CL-W-
DHCPIPCANDIDATE: The device is waiting for IP address
verification on interface Vlan 1 , IP 10.5.225.47, mask
255.255.255.224, DHCP server 10.5.224.25

01-Oct-2006 15:20:03 %BOOTP_DHCP_CL-I-DHCPCONFIGURED: The
device has been configured on interface Vlan 1 , IP
10.5.225.47, mask 255.255.255.224, DHCP server 10.5.224.25

01-Oct-2006 15:20:03 %COPY-I-FILECPY: Files Copy - source
URL tftp://10.5.224.4/33.txt destination URL running-
config

01-Oct-2006 15:20:03 %COPY-N-TRAP: The copy operation was
completed successfully

01-Oct-2006 15:20:03 %COPY-I-FILECPY: Files Copy - source
URL running-config destination URL flash://startup-config

01-Oct-2006 15:20:10 %COPY-N-TRAP: The copy operation was
completed successfully
```

File Download

Software and configuration files can be downloaded from an external device to the switch in the following ways:

- To download when management computer uses HTTP
- To download files using TFTP

To download when management computer uses HTTP

1 Click **System** > **File Management** > **File Download** in the tree view to display the **File Download** page.

2 For HTTP, enter the **IP Format** fields for the HTTP server IP address.

   – **Supported IP Format** — Select whether IPv4 or IPv6 format is supported.

   – **IPv6 Address Type** — When the server supports IPv6, this specifies the type of static address supported. The possible options are:

      - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
      - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.

   – **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:

      - **VLAN**— The VLAN on which the IPv6 interface is configured.
      - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.

3 Select a **Firmware/Configuration** option. The possible options are:

   – **Firmware Download** — A firmware file is downloaded.

   – **Configuration Download** — A configuration file is downloaded.

4 Select **Download via HTTP** to download a firmware or configuration file when the management computer is using HTTP in **Download Protocol**.

5 If the **Firmware Download** option was selected, enter the following:

   – **Source File Name (1-64 characters)** — The file to be downloaded.

   – **Destination File Type** — The destination file type to which the file is downloaded. The possible options are:

      - **Software Image** — Downloads the Image file. The image file overwrites the non-active image. It is recommended to designate that the non-active image becomes the active image after reset, and then to reset the device following the download. During the Image file download a dialog box opens that displays the download progress, and browsing is disabled.

- **Boot Code** — Downloads the Boot file.

6 If the **Configuration Download** option was selected, enter the following:

  – **Source File Name (1-64 Characters)** — Enter the source file name.

  – **Destination File Name** — Select the destination file to which the configuration file is downloaded. The possible options are:

    - **Running Configuration** — Check to download commands into the Running Configuration file. The current file is overwritten.
    - **Startup Configuration —** Check to download commands into the Startup Configuration file. The current file is overwritten.
    - **My Backup** —Name of backup file.
    - **New File Name (1-64 Characters)** — Check to copy commands into a file in flash memory. Enter the filename.

7 Click **Activate** to start the download process.

To download files using TFTP

1 Click **System** > **File Management** > **File Download** in the tree view to display the **File Download** page.

2 Enter the **IP Format** fields for the TFTP server IP address.

  – **Supported IP Format** — Select whether IPv4 or IPv6 format is supported.

  – **IPv6 Address Type** — When the server supports IPv6, this specifies the type of static address supported. The possible options are:

    - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
    - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.

  – **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:

    - **VLAN** 1— The VLAN on which the IPv6 interface is configured.
    - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.

3. Select a **Firmware/Configuration** option. The possible options are:
   - **Firmware Download** — A firmware file is downloaded.
   - **Configuration Download** — A configuration file is downloaded.
4. Select **Download via TFTP** to download firmware or a configuration file via a TFTP server in **Download Protocol**.
5. If the **Firmware Download** option was selected, enter the following:
   - **Server IP Address** — The TFTP server IP address from which the configuration files are downloaded.
   - **Source File Name (1-64 characters)** — The file to be downloaded.
   - **Destination File Type** — The destination file type to which the file is downloaded. The possible options are:
     - **Software Image** — Downloads the Image file. The image file overwrites the non-active image. It is recommended to designate that the non-active image becomes the active image after reset, and then to reset the device following the download. During the Image file download a dialog box opens that displays the download progress. The window closes automatically when the download is complete.
     - **Boot Code** — Downloads the Boot file.
6. If the **Configuration Download** option was selected, enter the following:
   - **Server IP Address** — The TFTP server IP address from which the configuration files are downloaded.
   - **Source File Name (1-64 characters)** — The configuration file to be downloaded.
   - **Destination File Name** — The destination file to which the configuration file is downloaded. The possible options are:
     - **Running Configuration** — Check to download commands into the Running Configuration file. The current file is overwritten.
     - **Startup Configuration —** Check to download commands into the Startup Configuration file. The current file is overwritten.
     - **New File Name (1-64 characters)** — Check to download commands into a configuration backup file. Enter the filename.
7. Click **Activate** to start the download process.

Downloading Files Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **File Download** page.

Table 7-43. File Download CLI Commands

CLI Command	Description
copy *source-url destination-url*	Copies files from a source to a destination.

The following is an example of the CLI command:

```
console# copy tftp://10.6.6.64/pp.txt startup-config

....!

Copy: 575 bytes copied in 00:00:06 [hh:mm:ss]

01-Jan-2000 06:41:55 %COPY-W-TRAP:
The copy operation was completed successfully
```

NOTE: Each exclamation mark (!) indicates that ten packets were successfully transferred.

File Upload

Software and configuration files can be uploaded to an external device using HTTP or TFTP.

To upload a configuration file:

1 Click **System** > **File Management** > **File Upload** in the tree view to display the **File Upload** page.

2 Enter the **IP Format** fields for the server IP address.

- **Supported IP Format** — Select whether IPv4 or IPv6 format is supported.
- **IPv6 Address Type** — When the server supports IPv6, this specifies the type of static address supported. The possible options are:
  - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.

    - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.
  - **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:
    - **VLAN1**— The VLAN on which the IPv6 interface is configured.
    - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.

To upload a configuration file using HTTP:

3. Select **Upload via HTTP** to upload a configuration file.
4. Enter the fields:
   - **Transfer File Name** — The configuration file being uploaded. The possible options are:
     - **Running Configuration** — Uploads the Running Configuration file.
     - **Startup Configuration** — Uploads the Startup Configuration file.
5. Click **Activate** to start the upload process. A message will be displayed asking where for the path of the destination file.

To upload a configuration file using TFTP:

6. Select one of the options:
   - **Firmware Upload** — A firmware file is uploaded.
   - **Configuration Upload** — A configuration file is uploaded.
7. Select **Upload via TFTP** to upload firmware or a configuration file via a TFTP server.
8. If **Firmware Upload** was selected, enter:
   - **TFTP Server IP Address** — The TFTP server IP address to which the software image is uploaded.
   - **Destination File Name (1-64 Characters)** — The file name to which the file is uploaded.
9. If **Configuration Upload** was selected, enter:
   - **TFTP Server IP Address** — The TFTP server IP address to which the configuration file is uploaded.

  - **Destination File Name (1-64 Characters)** — The configuration file name/path to which the file is uploaded.
  - **Transfer File Name** — The configuration file that is uploaded. The possible options are:
    - **Running Configuration** — Uploads the Running Configuration file.
    - **Startup Configuration** — Uploads the Startup Configuration file.

10 Click **Activate** to start the upload process.

Uploading Files Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **File Upload** page.

Table 7-44. File Upload CLI Commands

CLI Command	Description
copy *source-url destination-url*	Copies any file from a source to a destination.

The following is an example of the CLI commands:

```
console# copy image tftp://10.6.6.64/uploaded.ros

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy: 4234656 bytes copied in 00:00:33 [hh:mm:ss]

01-Jan-2000 07:30:42 %COPY-W-TRAP:
The copy operation was completed successfully
```

Active Images

There are two firmware images, Image1 and Image2, stored on the switch. One of these images is identified as the active image, and the other is identified as the inactive image. The switch boots from the active image.

You can switch the inactive image to the active image, and then reboot the switch.

To select the image file to be used after reset:

1. Click **System** > **File Management** > **Active Images** in the tree view to display the **Active Images** page.

   The following fields are displayed:

   – **Active Image** — The version of the image file that is currently active on the device.

   – **After Reset** — Select one of the possible versions of the image to be active after reset.

2. Click **Apply** to select the image file to be used after reset in **After Reset**.

Working with the Active Image File Using CLI Commands

The following table summarizes the CLI commands for viewing fields displayed in the **Active Images**.

Table 7-45. Active Image CLI Commands

CLI Command	Description
boot system {*image-1* | *image-2*}	Sets the system image that the device loads at startup.
show version [md5]	Displays version information for the system

The following is an example of the CLI commands:

```
console# boot system image-1 all
```

Copy Files

Use the **Copy Files** page to perform the following:

- Copy the firmware on the device to another, specified file.
- Copy the master Running Configuration file to the Startup Configuration file, or vice versa.
- Copy the master Startup Configuration file to a backup file on the Flash file system.

- Copy a configuration file to the Running Configuration file. It is important to be aware that copying a file to the Running Configuration file actually executes these commands, so some of the configuration commands might fail (for example when trying to create a VLAN that is already defined on the system).
- Restore configuration factory defaults.

To copy files or restore factory defaults:

1. Click **System** > **File Management** > **Copy Files** in the tree view to display the **Copy Files** page.
2. To copy the Running Configuration file of the device to the Startup Configuration file of the device or vice versa, select **Copy Configuration Firmware** and enter the options:
   - **Source** — Select either the Running Configuration or the Startup Configuration file.
   - **Destination** — Select either the Running Configuration, Startup Configuration file or user-created flash files, depending on the source configuration file.

   or

   - **New File Name (1-64 characters)** — To copy the source file to a user-named file, enter the name of a file.
3. Select **Restore Configuration Factory Defaults** to replace the current configuration settings by the factory configuration default settings.
4. Click **Activate** to initiate the selected process.

Copying Files Using CLI Commands

The following table summarizes the CLI commands for performing actions provided by the **Copy Files** page.

Table 7-46. Copy Files CLI Commands

CLI Command	Description
copy *source-url destination-url*	Copies any file from a source to a destination.
delete startup-config	Deletes the startup-config file.

Table 7-46. Copy Files CLI Commands *(continued)*

CLI Command	Description
delete *url*	Deletes a file from the FLASH memory device.

The following is an example of the CLI commands:

```
console# delete startup-config

Delete startup-config [y/n]? y

console# 01-Oct-2006 16:10:51 %FILE-I-DELETE: File
Delete - file URL flash://startup-config

console# copy running-config startup-config

Overwrite file [startup-config] ?[Yes/press any key
for no]....01-Oct-2006 16:11

:47 %COPY-I-FILECPY: Files Copy - source URL running-
config destination URL flash://startup-config

01-Oct-2006 16:12:01 %COPY-N-TRAP:
The copy operation was completed successfully

Copy succeeded
```

File System

Use the **File System** page to view information about files currently stored on the system, including file names, file sizes, files modifications, and file permissions. The files system permits managing up to two user-defined backup configuration files.

To view information about files:

1 Click **System** > **File Management** > **File System** in the tree view to display the **File System** page.

   The following information is displayed for all files in the system:

   – **File Name** — The name of the file currently stored in the file management system.

   – **Size** — The file size.

- **Modified** — The date the file was last modified.
- **Permission** — The permission type assigned to the file.

2 To rename a file, click its **Rename** button. Change the **File Name**.

Managing Files Using CLI Commands

The following table summarizes the CLI command for viewing system files.

Table 7-47. File Management CLI Command

CLI Command	Description
dir [***flash***://]	Display list of files on a flash file system
rename *url new-url*	Renames a file
delete *url*	Deletes a file

The following is an example of the CLI commands:

```
console# dir flash://
Directory of flash:
File Name      Permission Flash Size Data Size    Modified
-------------- ---------- ---------- ---------    -----------------------
1.cfg          rw         524160     14065        05-Oct-2006 21:20:36
2.cfg          rw         524160     14065        7-Oct-2006 09:11:07
aaafile.prv    --         65520       --          03-Oct-2006 15:45:41
dhcpdb.sys     r-         65520       --          01-Oct-2006 19:22:49
Total size of flash: 16121856 bytes
Free size of flash: 524768 bytes
```

sFlow

This section describes sFlow monitoring of traffic.

NOTE: This feature is only supported on the R1-2210.

It contains the following topics:

- Overview
- sFlow Receiver Settings
- sFlow Interface Settings
- sFlow Statistics

Overview

The sFlow feature enables collecting statistics using the sFlow sampling technology, based on sFlow V5.

This sampling technology is embedded within switches and routers. It provides the ability to continuously monitor traffic flows on some or all the interfaces, simultaneously.

The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a stand alone probe) and a central data collector, known as the sFlow receiver.

The sFlow agent uses sampling technology to capture traffic and statistics from the device it is monitoring. sFlow datagrams are used to forward the sampled traffic and statistics to an sFlow receiver for analysis.

sFlow V5 defines:

- How traffic is monitored.
- The sFlow MIB that controls the sFlow agent.
- The format of the sample data used by the sFlow agent when forwarding data to a central data collector. The device provides support for two types of sFlow sampling: flow sampling and counters sampling. The following counters sampling is performed according to sFlow V5 (if supported by the interface):
  - Generic interface counters (RFC 2233)
  - Ethernet interface counters (RFC 2358)

Workflow

By default, flow and counter sampling are disabled.

To enable sFlow sampling:

1. Set the IP address of a receiver (also known as a collector) for sFlow statistics. Use the **sFlow Receivers Settings** page for this.
2. Enable flow and/or counter sampling, direct the samples to a receiving interface, and configure the average sampling rate. Use the **sFlow Interface Settings** pages for this.
3. View and clear the sFlow statistics counters. Use the **sFlow Statistics** page for this.

sFlow Receiver Settings

To set the sFlow receiver parameters:

1. Click **System > sFlow > sFlow Receivers Settings** in the tree view to display the **sFlow Receivers Settings: Summary** page.

   The sflow parameters are displayed.

2. To add a receiver (sflow analyzer), click **Add** and select one of the pre-defined sampling definition indices in **Index**.
3. Enter the receiver's address fields:
   - **Supported IP Format** — Select whether IPv4 or IPv6 format is supported.
   - **IPv6 Address Type** — When the server supports IPv6, this specifies the type of static address supported. The possible options are:
     - **Link Local** — A Link Local address that is non-routable and used for communication on the same network only.
     - **Global** — A globally unique IPv6 address; visible and reachable from different subnets.
   - **Link Local Interface** — When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:
     - **VLAN 1**— The VLAN on which the IPv6 interface is configured.
     - **ISATAP** — The IPv6 interface is configured on an ISATAP tunnel.

- **IP Address** — Enter the receiver's IP address.

4 Enter the fields:

- **UDP Port** — Port to which SYSLOG message are sent.
- **Maximum Datagram Size (Bytes)** — Maximum number of bytes that can be sent to the receiver in a single sample datagram (frame).

Adding an sFlow Receiver Using the CLI Commands

The following table summarizes the CLI commands for adding an sFlow receiver.

Table 7-48. sflow Receiver CLI Commands

CLI Command	Description
sflow receiver *index* {*ipv4-address*|*ipv6-address*|*hostname*} [**port** port] [***max-datagram-siz***e bytes]	Defines an sFlow receiver. Use the no form of this command to remove the definition of the receiver.
no sflow receiver *index*	
show sflow configuration [*port_id*]	Displays the sFlow configuration for ports that are enabled for Flow sampling or Counters sampling.

The following is an example of the CLI commands:

```
console(config)# sflow receiver 2 1.1.1.1 port 6343
console# show sflow configuration
Receivers
Index      IP Address        Port   Max Datagram Size
----- -------------------- -------- ----------------
  1         0.0.0.0          6343         1400
  2         172.16.1.2       6343         1400
  3         0.0.0.0          6343         1400
  4         0.0.0.0          6343         1400
  5         0.0.0.0          6343         1400
  6         0.0.0.0          6343         1400
  7         0.0.0.0          6343         1400
  8         0.0.0.0          6343         1400
Interfaces
Interface Flow      Counters          Max Header    Collector  Index
          Sampling  Sampling Interval Size          Sampling   Counters
--------- --------- ----------------- ----------- ---------- ---------
te0/1   1/2048    60 sec           128           1         1
te0/2   1/4096    Disabled         128           0         2
```

sFlow Interface Settings

To sample datagrams or counters from a port, the port must be associated with a receiver. sFlow port settings can be configured only after a receiver has been defined in the **sFlow Receiver Settings** pages.

To enable sampling and configure the port from which to collect the sFlow information:

1 Click **System > sFlow > sFlow Interface Settings** in the tree view to display the **sFlow Interface Settings: Summary** page.

The sflow interface settings are displayed.

2 To associate an sFlow receiver with a port, click **Add**, and enter the fields:

– **Interface** — Select the unit/port from which information is collected.

- **Flow Sampling** — Enable/disable flow sampling. Flow sampling cannot be disabled if **Counters Sampling** is disabled.
- **Flow Sampling Average Sampling Rate**(1024–1073741823) — If x is entered, a flow sample will be taken for each x frames.
- **Flow Sampling Receiver Index** — Select one of the indices that was defined in the **sFlow Receivers Settings** pages.
- **Flow Sampling Maximum Header Size** (20–256) — Maximum number of bytes that should be copied from a sampled packet.
- **Counters Sampling** — Enable/disable counters sampling. Flow sampling cannot be disabled if **Flow Sampling** is disabled
- **Counters Sampling Interval** (15–86400) — If x is entered, this specifies that a counter sample will be taken for each x seconds.
- **Counters Sampling Receiver Index** — Select one of the indices that was defined in the **sFlow Receivers Settings** pages.

Configuring sFlow Interfaces Using the CLI Commands

The following table summarizes the CLI commands for configuring sFlow interfaces.

Table 7-49. sflow Interface CLI Commands

CLI Command	Description
`sflow flow-sampling` *`rate receiver-index`* [*`max-header-size bytes`*]	Enables sFlow Flow sampling and configure the average sampling rate of a specific port.
`no sflow flow-sampling`	Use the no form of this command to disable Flow sampling.

`sflow counters-sampling` *`interval receiver-index`*
`no sflow counters-sampling`
	Enable sFlow counters sampling and to configure the maximum interval of a specific port.
	Use the no form of this command to disable sFlow Counters sampling.

The following is an example of the CLI commands:

```
console(config)# interface te1/1
console(config-if)#sflow flow-sampling 1024 1
```

sFlow Statistics

To view sFlow statistics:

1 Click **System** > **sFlow** > **sFlow Statistics** in the tree view to display the **sFlow Statistics** page.

  The following sflow statistics per interface are displayed:

  – **Interface** — Port for which sample was collected.

  – **Packets Sampled** — Number of packets sampled.

  – **Datagrams Sent to Receiver** — Number of sFlow sampling packets sent.

2 Click **Clear Statistics** to clear the counters.

Viewing sFlow Statistics Using the CLI

The following table summarizes the CLI commands for viewing sFlow statistics:

Table 7-50. sFlow Statistics CLI Command

CLI Command	Description
show sflow statistics [*port-id*]	Displays sFlow statistics for ports that are enabled for Flow sampling or Counters sampling.
clear sflow statistics [*port-id*]	Clears sFlow statistics for ports that are enabled for Flow sampling or Counters sampling.

The following is an example of the CLI commands:

```
console # show sflow statistics
Total sFlow datagrams sent to collectors: 100
Interface Packets Sampled Datagrams Sent to Collector
--------- ------- ------------------------------------
te0/1   30      50
te0/2   10      10
te1/1   0       10
te1/2   0       0
```

8

IP Addressing

This section describes how to configure IP addressing on the switch.

It contains the following topics:

- Overview
- IPv4 Addressing
- IPv6 Addressing

Overview

The device functions as an IPv6-compliant host, as well as an IPv4-host (also known as dual stack). This enables device operation in a pure-IPv6 network, as well as in a combined IPv4/IPv6 network.

Difference Between IPv4 and IPv6 Addressing

The primary difference between IPv4 to IPv6 is the length of network addresses. IPv6 addresses are 128 bits, whereas IPv4 addresses are 32 bits. Thus, IPv6 addresses enable the use of many more unique addresses.

The 128-bit IPv6 address format is divided into eight groups of four hexadecimal digits. Abbreviation of this format by replacing a group of zeros with double colons (::) is acceptable. IPv6 address representation can be further simplified by suppressing the leading zeros.

All IPv6 address formats are acceptable, yet for display purposes, the system displays the most abbreviated form, which replaces groups of zeros with double colons and removes the leading zeros.

IPv6 Prefixes

While Unicast IPv6 addresses written with their prefix lengths are permitted, in practice their prefix lengths are always 64 bits, and therefore are not required to be expressed. Any prefix that is less than 64 bits is a route or address range that summarizes a portion of the IPv6 address space.

For every assignment of an IP address to an interface, the system runs the Duplicate Address Detection (DAD) algorithm to ensure uniqueness.

An intermediary transition mechanism is required for IPv6-only nodes to communicate with IPv6 nodes over an IPv4 infrastructure. The tunneling mechanism implemented is the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). This protocol treats the IPv4 network as a virtual IPv6 local-link, with each IPv4 address mapped to a Link Local IPv6 address.

IPv4 Interface Assignment

An IPv4 interface can be assigned on the following types of interfaces:

- **OOB**

  By default, a switch has a single IP interface assigned on the OOB port. This IP interface cannot be removed.

- **In-Band on the R1-2401**

  Additional IP interfaces can be assigned depending on the switch's operational system mode: Layer 2 or Layer 2 + Static Routing mode.

  - In Layer 2 mode, only one additional IP interface can be assigned on any of the in-band interfaces (port, LAG or VLAN).
  - In Layer 2 + Static Routing mode, up to 32 IP interfaces can be assigned on one or more in-band interfaces.

- **In-Band on the R1-2210**

  Up to 32 IP interfaces can be assigned on one or more in-band interfaces (port, LAG or VLAN).

IPv4 Address Assignment

IPv4 addresses can be assigned to OOB and in-band interfaces. They can be assigned either statically or dynamically (by a DHCP server).

By default, the IPv4 address of the OOB is assigned dynamically from a DHCP server. If the DHCP server is not accessible, the OOB uses the default IP address 192.168.2.1. After a static or DHCP valid IP address is assigned on the OOB interface, the default IP address is removed.

NOTE: The user cannot assign the default subnet statically on an in-band interface, since it is reserved for default connectivity on the OOB in case the DHCP server is not accessible.

Dynamic Assignment

Dynamic assignment of an IPv4 address can be configured in the IPv4 Interface page.

It can also be performed using CMC management by requesting dynamic assignment of an IP address from the CMC management.

NOTE: When a static address is removed from the OOB port, the DHCP client is enabled on this port. The user cannot delete IP DHCP configuration from the OOB port without defining a new static address.

Static Assignment

The static IPv4 address on an IP interface can be assigned in the IPv4 Interface page.

Number of In-Band IP Addresses

Only a single IP address can be assigned on the OOB port.

The number of IP addresses that can be assigned on in-band ports vary according to the system mode:

- In Layer 2 mode in R1-2401, a single IP address can be assigned, either statically or by a DHCP server.
- In Layer 2 + Static Routing mode on R1-2401 devices and (always) on R1-2210 devices, multiple IP addresses can be assigned, either statically or by a DHCP server.

NOTE: The IPv4 address assigned to the OOB interface is not accessible through in-band interfaces and vice-versa.

IPv4 Default Gateway

A default gateway can be assigned on any IPv4 interface in the system (OOB, Port, LAG or VLAN).

The IPv4 default gateway can be assigned statically or received by a DHCP server according to the configuration in the IPv4 Interface page. When you enable DHCP dynamic assignment of IP addresses, the default gateway is also received from the DHCP server. DHCP assignment is the default.

An IPv4 default gateway can be defined on an OOB interface (either assigned statically or by a DHCP server) and also on in-band ports.

If multiple default gateways are assigned, only one active default gateway is used. The active default gateway is selected according to the following criteria:

- A static default gateway is preferred (not a dynamic default gateway).
- If multiple static default gateways are assigned, the static default gateway on the OOB interface is selected.
- If multiple dynamic default gateways are assigned, the DHCP default gateway assigned on the OOB interface is selected.
- See IPv4 Default Gateway for a description of how the metrics of the routes determine which default route is chosen.

IPv4 Addressing

This section describes the following sections:

- IPv4 Global Parameters
- IPv4 Interface
- IPv4 Routes Table (Advanced Mode)
- ARP
- UDP Relay

IPv4 Global Parameters

NOTE: This page is only supported on the R1-2210.

To define IPv4 global parameters:

1. Click **System** > **IPv4 Addressing** > **IPv4 Global Parameters**.
2. Select **Enable/Disable** to enable/disable IPv4 Routing.

Defining IPv4 Global Parameters Using CLI Commands

The following table summarizes the CLI commands to enable IPv4 global parameters:

Table 8-1. IPv4 Global Parameters CLI Commands

CLI Command	Description
`ip routing`	Enables IPv4 routing.

The following is a sample script to define IPv4 global parameters using CLI:

Table 8-2. Sample CLI Script to Enable IPv4 Routing

CLI Command	Description
`console(config)#`**`ip routing`**	Enables IPv4 routing.

IPv4 Interface

You can assign IPv4 addresses to an interface in the following ways:

- **Static Assignment**
- **DHCP Assignment**

  When the interface is configured as a DHCP client, it requests an IP address from the DHCP server, until it receives an answer. It then sends Address Resolution Protocol (ARP) packets to confirm the uniqueness of the IP address. If the ARP response shows that the IP address is in use, the switch sends a DHCPDECLINE message to the DHCP server, and sends another DHCPDISCOVER packet that restarts the process.

When an IP address is assigned, it is checked for uniqueness in the following way:

- A gratuitous ARP request is sent three times every three seconds.
- If after (3+1)*3 = 12 seconds the switch has not received the ARP response, the IP address is considered to be unique.
- During the procedure the switch has to reply to gratuitous ARP and probe ARP requests with the validated IP address.

The IP address is assigned even if the above validation procedure concludes that the IP address in question is not unique, but a SYSLOG message is generated.

In addition to the above validation procedure every time a switch receives an ARP request with a sender IP address that is equal to its IP address defined on the input interface it sends a SYSLOG message informing of IP duplication, containing the sender IP and MAC addresses, from the received ARP message.

To configure the default route, go to the IPv4 Routing Table page.

To assign an IP address to the OOB interface or an IPv4 Interface, and to define subnets to which traffic can be routed:

1 Click **System** > **IPv4 Addressing** > **IPv4 Interface** in the tree view to display the **IPv4 Interface: Summary** page.

The previously-assigned IP addresses are displayed along with the following field:

– **Type**—Displays the type of IPv4 interface:

- **Static**—Defined manually.
- **DHCP**—Received from DHCP server.

2 To change the interface IP address, click **Edit**, and enter the fields:

– **Interface** — Select the interface on which IPv4 routing is enabled.

– **DHCP IPv4 Interface** — Select to acquire the IP address dynamically from a DHCP server.

– **IP Address** — Enter the IP address assigned to the OOB interface manually (only if the DHCP IPv4 Interface option was not selected).

– **Network Mask** — Select the subnetwork mask to which traffic can be routed.

– **Prefix Length** — Enter the number of bits that comprise the IP address prefix of the subnetwork.

– **Default Gateway**— Enter the IP address of the default gateway if you did not enable DHCP.-If DHCP is enabled, the default gateway is received from the DHCP server.

Defining IPv4 Interfaces Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **IPv4 Interfaces Parameters** page.

Table 8-3. IPv4 Interface Parameters CLI Commands

CLI Command	Description
ip address *ip-address* {*mask* | *prefix-length*}	Sets an IP address and the default gateway on an interface.
ip address *ip-address* {*mask* | */prefix-length*} [**default-gateway** *ip-address*]	Use the no form of the command to remove an IP address and default gateway.
no ip address [*ip-address*]	

Table 8-3. IPv4 Interface Parameters CLI Commands *(continued)*

CLI Command	Description
show ip interface [*interface-id*]	Displays the usability status of interfaces configured for IP.
ip address dhcp **no ip address dhcp**	Acquires an IP address from a DHCP server). Use the no form of this command to release an acquired IP address.

The following are sample procedures to configure a static IPv4 address on an interface using CLI and then to remove it:

Table 8-4. Sample CLI Script to Configure IPv4 Statically on a VLAN

CLI Command	Description
`console#`**`config`**	Enter Global Configuration mode.
`console(config)#` **`interface vlan`** `1`	Enter Interface mode for VLAN 1.
`console(config-if)#` **`ip address`** `10.5.225.40 /27`	Set the routing interface with prefix length of 27.
`console(config-if)#` **`ip default-gateway`** `10.5.225.33`	Set the address of the default gateway
`console(config-if)#` **`no ip address`**	Remove the address (if required).

Table 8-5. Sample CLI Script to Configure IPv4 Statically on a Port

CLI Command	Description
`console#`**`config`**	Enter Global Configuration mode.
`console(config)#` **`interface`** `gi0/1`	Enter Interface mode for port 1.
`console(config-if)#` **`no switchport`**	Enable the port to work as an IP interface (Layer 3 mode).

Table 8-5. Sample CLI Script to Configure IPv4 Statically on a Port

CLI Command	Description
`console(config-if)# ip address 10.5.225.40 /27`	Configure an IP address with prefix length of 27.
`console(config-if)# ip default-gateway 10.5.225.33`	Set the address of the default gateway
`console(config-if)# no ip address`	Remove the address (if required).

Table 8-6. Sample CLI Script to Configure IPv4 Dynamically on a VLAN

CLI Command	Description
`console#config`	Enter Global Configuration mode.
`console(config)# interface vlan 1`	Enter VLAN mode for VLAN 1.
`console(config-if)# no switchport`	Enable the port to work as an IP interface (Layer 3 mode).
`console(config-if)# ip address dhcp`	Use the DHCP protocol to acquire the IP address.
`console(config-if)# no ip address dhcp`	Remove the address (if required).

Table 8-7. Sample CLI Script to Configure IPv4 Dynamically on a Port

CLI Command	Description
`console#config`	Enter Global Configuration mode.
`console(config)# interface vlan 1`	Enter VLAN mode for VLAN 1.
`console(config-if)# ip address dhcp`	Use the DHCP protocol to acquire the IP address.
`console(config-if)# no switchport`	Enable the port to work as an IP interface (Layer 3 mode).

Table 8-7. Sample CLI Script to Configure IPv4 Dynamically on a Port

CLI Command	Description
`console(config-if)# no ip address dhcp`	Remove the address (if required).

IPv4 Routes Table (Advanced Mode)

NOTE: This feature is only applicable for Layer 2 + Static Routing mode for all devices.

IPv4 static routes can be configured for IP addresses that are not on directly connected networks. These are defined in the **IPv4 Routing Table** pages.

Static route configuration is allowed only on the in-band interfaces. The maximum metric value is 255 and the default metric value is 1.

When routing traffic, the next hop is determined according to the longest prefix match (LPM algorithm). A destination IPv4 address may match multiple routes in the IPv4 Static Route table. The switch uses the matched route with the longest prefix match.

NOTE: The system does not support forwarding IP traffic between In-band and OOB interfaces.

For R1-2210 devices and R1-2401 devices in Layer 2 + Static Routing system mode

To add an IPv4 static route:

1 Click **System** > **IPv4 Addressing** > **IPv4 Routes Table** in the tree view to display the **IPv4 Routes Table: Summary** page.

The following fields are displayed:

- **Destination IPv4 Prefix** — Destination IPv4 prefix. If all zeros are entered, this represents a default route.
- **Network Mask** — Destination IPv4 mask.
- **Prefix Length** — Length of the destination IPv4 address prefix.
- **Next Hop** — IP address to which the packet is forwarded on the route to the destination address. This is typically the address of a neighboring switch.

- **Route Type** — The possible options are:
  - **Reject** — Rejects the route and stops routing to the destination network via all gateways. This ensures that if a frame arrives with the destination IP of this route, it is dropped.
  - **Remote** — The route is a remote path.
- **Route Owner** — Displays one of the following:
  - **Connected**— Directly-connected route.
  - **Static** — Manually-added route.
  - **DHCP** — DHCP-supplied route.
- **Metric** (1-255) — Cost of the destination.

2 Click **Add** and enter the required fields (that are described above).

For R1-2401 devices in Layer 2 + Static Routing

To add an IPv4 static route:

1 Click **System > IPv4 Addressing > IPv4 Routing Table** in the tree view to display the **IPv4 Routing Table: Summary** page.

The following fields are displayed:

- **IP Address**— Destination IPv4 prefix. If all zeros are entered, this represents a default route.
- **Prefix Length** — Length of the destination IPv4 address prefix.
- **Interface** — Interface on which route is defined.
- **Default Gateway**— Gateway for this interface.
- **Type** — The possible options are:
  - **Static** — User defined the IP address of the default gateway.
  - **DHCP** — The IP address of the default gateway is received from the DHCP server.

2 Click **Add** and enter the required fields (that are described above).

Adding an Entry to the IPv4 Routing Table Using CLI Commands

The following table summarizes the CLI commands for adding an entry to the IPv4 Routing table.

Table 8-8. IPv4 Static Routing CLI Commands for R1-2210 and R1-2401 in Layer 2 + Static Routing Mode

CLI Command	Description
ip route *prefix* {*mask*|*prefix-length*} *ip-address-next-hop* [***metric*** *distance*] [**reject-route**] **no ip route prefix** {*mask*|*prefix-length*} [*ip-address-next-hop*]	Configures static routes. Use the no form of this command to remove static routes.
show ip route	Displays the current routing table state.

The following is an example of the CLI command:

```
Example 1: Configuring a static route with a metric value of
10
console(config)# ip route 3.3.3.3/24 192.12.12.10 metric 10
Example 2: Configuring a static route without specifying a
metric value. The default metric is 1.
console(config)# ip route 4.4.4.4/24 192.12.12.11
```

Table 8-9. IPv4 Static Routing CLI Commands for R1-2401 in Layer 2

CLI Command	Description
ip address *ip-address* {*mask* | */prefix-length*} [**default-gateway** *ip-address*	Configures IPv4 routing on an IPv4 interface.
ip address dhcp	Renews an IP address that was acquired from a DHCP server for a specific interface

Table 8-9. IPv4 Static Routing CLI Commands for R1-2401 in Layer 2

CLI Command	Description
renew dhcp *interface-id* [force-autoconfig]	Configures acquiring an IP address for an Ethernet interface from the DHCP server. Use the no form of this command to return to entering the IP address manually.
ip default-gateway *ip-address*	Defines a default gateway.
no ip default-gateway	Use the no form of this command to restore the default gateway.
show ip interface	Displays the current IPv4 interfaces.

The following is an example of the CLI commands:

```
config)# interface vlan 1
(config-if)# ip address 131.108.1.27 255.255.255.0
(config-if)# ip address dhcp
(config)# ip default-gateway 192.168.1.1
# show ip interface
IP Address      I/F    I/F Status Type Status admin/oper
------------- ------ ---------- ------- ------
10.5.234.232/24 vlan 1 UP/UP      Static      Valid
Default Gateway: 10.5.234.254, Static
```

Configuring Two IP Networks on Two Different VLANS Using CLI

The following shows how to configure two IP networks on two different VLANS using CLI:

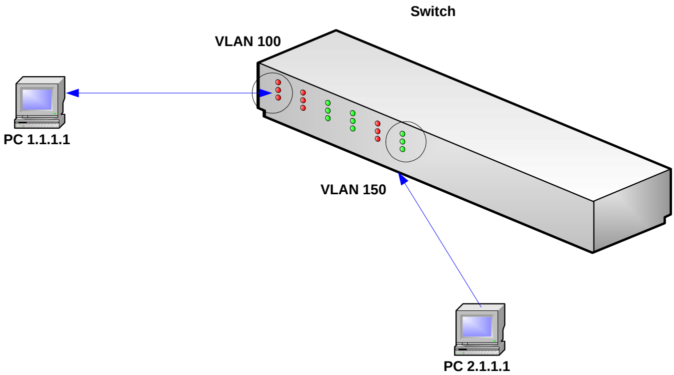
Table 8-10. Sample CLI Script to Configure Two IP Networks on Two Different VLANSs

CLI Command	Description
`console#`**`config`**	Enter Global Configuration mode.
`console(config)# `**`vlan database`**	Enter VLAN mode.
`console(config-vlan)# `**`vlan`**` 100-150`	Create VLANs number 100 to 150.
`console(config-vlan)# `**`exit`**	Exit VLAN mode.
`console(config)#`**`interface`**` te1/1`	Enter Interface mode for port 1.
`console(config-if)# `**`switchport access vlan`**` 100`	Make port a member of VLAN 100.
`console(config-if)# `**`ip address`**` 1.1.1.1 255.255.255.0`	Set the IP address with mask.
`console(config-vlan)# `**`exit`**	Exit Interface mode for port.
`console(config)#`**`interface`**` te1/2`	Enter Interface mode for port 2.
`console(config-if)# `**`switchport access vlan`**` 150`	Make port a member of VLAN 150.
`console(config-if)# `**`ip address`**` 2.1.1.1 255.255.255.0`	Set the IP address with mask.
`console(config-vlan)# `**`exit`**	Exit Interface mode for port.

To test the setup described in Figure 8-1:

1. Connect a host whose address is 1.1.1.2 to interface te1/1 (default route 1.1.1.1)
2. Connect a host whose address 2.1.1.2 to interface te1/2(default route 2.1.1.1)
3. Ping from 1.1.1.2 to 2.1.1.2 to verify the configuration

Figure 8-1. IP Routing Setup



IPv4 Default Metric for Default Routes for Layer 2 + Static Routing

An IPv4 default route can be assigned on in-band interfaces statically or by a DHCP server. The following behavior is supported:

- The default metric for static assignment is 1
- The default metric for DHCP assignment is 253

The maximum metric value is 255.

NOTE: The same metric values are used for an IP default gateway on an OOB interface.

If both an IPv4 default gateway on an OOB interface and a default route on an in-band interface are both assigned, the selection for the active default gateway / route is performed according to the following criteria:

- The lower metric is preferred regardless of the default gateway / route assignment method (static or DHCP assignment).
- If two entries have the same metric, the IPv4 default gateway assigned to an OOB interface is preferred

ARP

The Address Resolution Protocol (ARP) converts IP addresses into physical MAC addresses. ARP enables a host to communicate with other hosts when their IP addresses are known.

To configure ARP and add an IP/MAC address mapping:

1 Click **System** > **IPv4 Addressing** > **ARP** in the tree view to display the **ARP: Summary** page.

  The entries in the table are displayed.

2 Enter the parameters:

  - **ARP Entry Age Out (1 - 40000000)** — Enter the amount of time in seconds that can pass between ARP requests for this address. After this period, the entry is deleted from the table.
  - **Clear ARP Table Entries** — Select the type of ARP entries that are cleared on all devices. The possible options are:
    - **None** — ARP entries are not cleared.
    - **All** — All ARP entries are cleared.
    - **Dynamic** — Only learned ARP entries are cleared.
    - **Static** — Only static ARP entries are cleared.

3 To add a mapping, click **Add**, and enter the fields:

  – **Interface** — Select an interface to be associated with the addresses.

  – **IP Address** — Enter the station IP address that is associated with the MAC address filled in below.

  – **MAC Address** — Enter the station MAC address that is associated in the ARP table with the IP address.

4 To change the status of a mapping from static to dynamic or vice versa, click **Edit** and enter the field:

  – **Status** — Select the entry's status. The possible options are:

    - **Static** — The entry was statically entered.
    - **Dynamic** — The entry was dynamically learned.

Configuring ARP Using the CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the ARP pages.

Table 8-11. ARP CLI Commands

CLI Command	Description
arp *ip_addr mac_addr* [*interface-id*]	Adds a permanent entry in the ARP cache.
no arp *ip-address*	Removes an ARP entry from the ARP Table.
arp timeout *seconds* **no arp timeout**	Configures how long an entry remains in the ARP cache. This command can be used in Global Configuration mode for all interfaces, or in Interface Configuration mode for a specific interface. Use the no form of this command restore the default value.
clear arp-cache	Deletes all dynamic entries from the ARP cache
show arp [*ip-address* *ip-address***] [*mac-address*** *mac-address***] [***interface-id***]**	Displays entries in the ARP Table.
show arp configuration	Displays the global and interface configuration of the ARP protocol

The following is an example of the CLI commands:

```
console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

console(config)# arp timeout 12000

console(config)# exit

console# show arp

ARP timeout: 12000 Seconds
Interface     IP Address    HW Address        Status
---------     ----------    ----------        ------
gi0/11        10.7.1.102    00:10:B5:04:DB:   dynamic
                            4B
gi0/12        10.7.1.135    00:50:22:00:2A:   static
                            A4
```

UDP Relay

Switches do not typically route IP Broadcast packets between IP subnets. However, if configured, the switch can relay specific UDP Broadcast packets received from its IPv4 interfaces to specific destination IP addresses.

To configure the relaying of UDP packets received from a specific IPv4 interface with a destination UDP port:

1. Click **System** > **IPv4 Addressing** > **UDP Relay** in the tree view to display the **UDP Relay: Summary** page.

   The UDP relays are displayed.

2. To add a UDP relay, click **Add**, and enter the fields:

   – **Source IP Address** — Select the source IP address to where the switch is to relay UDP Broadcast packets, based on a configured UDP destination port. The interface must be one of the IPv4 interfaces configured on the switch. Select **All** for all addresses.

   – **UDP Port (1 - 65535)** — Check **Default Services** to select all of the following default ports:

     - IEN-116 Name Service (port 42)
     - DNS (port 53)

- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

If **Default Services** are not selected, check the text box and enter a UDP port.

– **Destination IP Address** — Enter the IP address that receives the UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.

Configuring UDP Relay Using the CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **UDP Relay** pages.

Table 8-12. UDP Relay CLI Commands

CLI Command	Description
ip helper-address {*ip-interface*|***all***} *address* [*udp-port-list*] **no ip helper-address** {*ip-interface*|***all***} *address*	Enables the forwarding of User Datagram Protocol (UDP) broadcast packets received on an interface to a specific (helper) address. Use the no form of this command to disable the forwarding of broadcast packets to a specific (helper) address.

The following is an example of the CLI commands:

```
console (config)# ip helper-address all 172.16.9.9 49 53
console (config)# do show ip helper-address
Interface    Helper Address   UDP Ports
---------- --------------   -------------------------
All         172.16.9.9        49,53
```

IPv6 Addressing

This section describes the following sections:

- IPv6 Global Parameters
- IPv6 Interface
- IPv6 Routes Table
- IPv6 Default Gateway
- ISATAP Tunnel
- IPv6 Neighbors
- IPv6 Router

IPv6 Global Parameters

To define IPv6 global parameters:

Click **System** > **IPv6 Addressing** > **IPv6 Global Parameters**.

Enter values for the following fields:

- **IPv6 Routing (for R1-2210)**—Select to enable IPv6 routing. If this is not enabled, the device acts as a host (not a router) and can receive management packets, but cannot forward packets. If routing is enabled, the device can forward the IPv6 packets.
- **ICMP Error Rate Limit Interval (0-2147483647)** — Enter how often the ICMPv6 error messages are generated in milliseconds. The value of this parameter together with the Bucket Size parameter (below) determines how many ICMP error messages may be sent per time interval, for example, a rate-limit interval of 100 ms and a bucket size of 10 messages translates to 100 ICMP error messages per second.
- **ICMP Error Rate Limit Bucket Size (1-200)** — Enter the maximum number of ICMP error messages that can be sent by the device per interval. The value of this parameter together with the **ICMP Error Rate Limit Interval** parameter determines how many ICMP error messages may be sent per time interval, for example, a rate-limit interval of 100 ms and a bucket size of 10 messages translates to 100 ICMP error messages per second.

- **IPv6 Hop Limit (for R1-2210)**—Enter the maximum number of intermediate routers on its way to the final destination to which a packet can pass. Each time a packet is forwarded to another router, the hop limit is reduced. When the hop limit becomes zero, the packet is discarded. This prevents packets from being transferred endlessly.
- **IPv6 Link Local Default Zone Interface (for R1-2210)**— Select an interface to egress a link local packet without a specified interface or with the default zone 0.

Defining IPv6 Global Parameters Using CLI Commands

The following table summarizes the CLI commands for defining IPv6 global parameters:

Table 8-13. IPv6 Global Parameters CLI Commands

CLI Command	Description
`ipv6 routing`	(For R1-2210) Enables IPv6 routing
`ipv6 icmp error-interval` ***`milliseconds`*** **`[`*`bucketsize`*`]`**	Configures the interval and bucket size for IPv6 ICMP error messages
`no ipv6 icmp error-interval`	Use the no form to return to the default values.

`ipv6 hop-limit` ***`value`***
`no ipv6 hop-limit`
	(For R1-2210)Configures the maximum number of hops used in all IPv6 packets that are originated by the router.
	Use the no form to return to the default value.

`ipv6 link-local default zone` ***`interface-id`***
`no ipv6 link-local default zone`
	(For R1-2210)Configures an interface to egress a link local packet without a specified interface or with the default zone 0.
	Use the no form of this command to return the default link local interface to the default value.

The following is a sample script to define IPv6 global parameters using CLI:

Table 8-14. Sample CLI Script to Set IPv6 Global Parameters

CLI Command	Description
`console (config) ip routing`	Enables IPv6 routing.
`console(config)#ipv6 hop-limit 15`	Configures the maximum number of hops used in all IPv6 packets that are originated by the router to 15.
`console(config)#ipv6 icmp error-interval 50 20`	Configures the interval and bucket size for IPv6 ICMP error messages to 50 and 20, respectively.
`console(config)#ipv6 hop-limit 15`	Configures the maximum number of hops used in all IPv6 packets that are originated by the router to 15.
`console(config)#ipv6 link-local default zone vlan1`	Configures VLAN1 to egress a link local packet without a specified interface.

IPv6 Interface

The system supports IPv6-addressable hosts.

To define IPv6 interfaces:

1 Click **System > IPv6 Addressing > IPv6 Interface** in the tree view to open the **IPv6 Interface: Summary** page.

   The following fields are displayed for each currently-defined IPv6 address on the selected interface:

   – **IPv6 Address** —Address of the IPv6 interface.

   – **Prefix** —Prefix of the IPv6 interface

   – **IPv6 Address Type** — Link local or Multicast.

   – **IPv6 Address Origin Type** — The options are:

   - **Autoconfig**—Learned.
   - **Manual**—Manually-entered.

- **DAD Status** —New addresses remain in a Tentative status while duplicate address detection is performed. After it is performed successfully, the DAD status is Active.

2 Enter the following fields to modify these parameters on a currently-defined IPv6 interface:

   - **Interface** — Select a non-tunnel IPv6 interface to be configured.
   - **Removed** —Select to disable IPv6 support on this interface.
   - **Duplicate Address Detection Attempts** — Number of consecutive neighbor solicitation messages that are sent on an interface while Duplicate Address Detection (DAD) is performed on Unicast IPv6 addresses on this interface. New addresses remain in a tentative state while duplicate address detection is performed. A field value of 0, disables duplicate address detection processing on the specified interface. A field value of 1, indicates a single transmission without follow up transmissions.

NOTE: A field value of 0, disables duplicate address detection processing on the specified interface. A field value of 1, indicates a single transmission without follow up transmissions.

   - **Autoconfiguration** — Enable/disable stateless auto configuration of IPv6 address assignment. When enabled, the router solicitation ND procedure is initiated. This discovers a router in order to assign an IP address to the interface, based on prefixes received with RA messages. When auto configuration is disabled, no automatic assignment of IPv6 global Unicast addresses is performed, and existing, automatically-assigned IPv6 global Unicast addresses are removed from the interface.
   - **Send ICMP Unreachable** — Enable/disable transmission of ICMPv6 address Unreachable messages. When enabled, unreachable messages are generated for any packet arriving on the interface with unassigned TCP/UDP port.
   - **IPv6 Redirects** (for R1-2210)— Enable the sending of ICMP IPv6 redirect messages to re-send a packet through the same interface on which the packet was received.

3 To configure the interface as a DHCPv6 client, meaning to enable the interface to receive information from the DHCPv6 server, such as: SNTP configuration and DNS information, enter the DHCPv6 Client fields:

- **Stateless**—Select to enable the interface to receive configuration information from a DHCP server.
- **Minimum Information Refresh Time (600-4294967294)** —This value is used to put a floor on the refresh time value. If the server sends a refresh time option that is less than this value, this value is used instead. Select either **Infinite** (no refresh unless the server sends this option) or **User Defined** to set a value.
- **Information Refresh Time (86400-4294967294)**—This value indicates how often the device will refresh information received from the DHCPv6 server. If this option is not received from the server, the value entered here is used. Select either **Infinite** (no refresh unless the server sends this option) or **User Defined** to set a value

4 To enable IPv6 support on this interface, click **Add IPv6 Interface**, and enter the fields as described above:

5 To add an address to an IPv6 interface, click **Add IPv6 Address**, and enter the fields for the selected interface:

- **IPv6 Address Type** — Check the means by which the IP address was added to the interface. The possible options are:
  - **Link Local** — The IP address is link local; non-routable and can be used for communication on the same network only. A Link Local address has a prefix of 'FE80'.
  - **Global Unicast** — The IP address is a globally unique IPv6 Unicast address; visible and reachable from different subnets.
  - **Global Anycast** — The IP address is a globally unique IPv6 Anycast address; visible and reachable from different subnets.
- **IPv6 Address** — Enter the IPv6 address assigned to the interface. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons. An example of an IPv6 address is 2031:0:130F:0:0:9C0:876A:130D and the compressed version is represented as 2031:0:130F::9C0:876A:130D. Up to five IPv6 addresses (not including Link Local addresses) can be set per interface, with the limitation of up to128 addresses per system.

- **Prefix Length** — For global Unicast or Anycast, enter the length of the IPv6 prefix. The length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). The Prefix field is applicable only on a static IPv6 address defined as a *Global IPv6* address.
- **EUI-64** — For global Unicast or Anycast, check to use the EUI-64 option.

Defining IPv6 Interfaces Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **IPv6 Interface** pages.

Table 8-15. IPv6 Interfaces CLI Commands

CLI Command	Description

`ipv6 enable`
`no ipv6 enable`
	Enables the IPv6 addressing mode on an interface.
	Use the no form of this command to disable the IPv6 addressing mode on an interface

`ipv6 address autoconfig`
`no ipv6 address autoconfig`
	Enables automatic configuration of IPv6 addresses, using stateless auto configuration on an interface. Addresses are configured depending on the prefixes received in Router Advertisement messages.
	Use the no form of this command to disable address auto configuration on the interface.

`ipv6 icmp error-interval` *`milliseconds`* `[`*`bucketsize`*`]`
`no ipv6 icmp error-interval`
	Configures the rate limit interval and bucket size parameters for IPv6 Internet Control Message Protocol (ICMP) error messages.
	Use the no form of this command to return the interval to its default setting.

Table 8-15. IPv6 Interfaces CLI Commands *(continued)*

CLI Command	Description
ipv6 address *ipv6-address/prefix-length* [***eui-64***] [***anycast***] **no ipv6 address** [*ipv6-address/prefix-length*] [**link-local**] [***eui-64***]	Configures an IPv6 address for an interface. Use the no form of this command to remove the address from the interface.
ipv6 address *[ipv6-address* **link-local]** **no ipv6 address** *[ipv6-address* **link-local]**	Configures an IPv6 link-local address for an interface. Use the no form of this command to return to the default link local address on the interface.
ipv6 unreachables **no ipv6 unreachables**	Enables the generation of ICMP for IPv6 (ICMPv6) unreachable messages for packets arriving on a specified interface. Use the no form of this command to prevent the generation of unreachable messages.
ipv6 nd dad attempts *attempt*	Configures the number of consecutive neighbor solicitation messages that are sent on an interface while Duplicate Address Detection (DAD) is performed on the unicast IPv6 addresses of the interface.
ipv6 redirect **no ipv6 redirect**	(Applicable for R1-2210) Enables the sending of ICMP IPv6 redirect messages to re-send a packet through the same interface on which the packet was received.
show ipv6 interface [inter*face-id*]	Displays the usability status of interfaces configured for IPv6.
show ipv6 icmp error-interval	Displays the IPv6 ICMP error interval.

The following is a sample script to configure IPv6 using CLI:

Table 8-16. Sample CLI Script to Configure IPv6 on a Port

CLI Command	Description
`console#`**`config`**	Enter Global Configuration mode.
`console(config)#` **`interface vlan`** `1`	Enter VLAN mode for VLAN 1.
`console(config-if)#` **`ipv6 enable`**	Enable IPv6 (dynamic).
`console(config-if)#` **`ipv6 address`** `5::1/64`	Set the IPv6 address (static)
`console(config-if)#` **`ipv6 redirect`**	Enables the sending of IPv6 ICMP redirect messages.

IPv6 Routes Table

The IPv6 Routes Table contains the various routes that have been configured. One of these routes is a default route (IPv6 address:0) that uses the default router selected from the IPv6 Default Router List to send packets to destination devices that are not in the same IPv6 subnet as the device. In addition to the default route, the table also contains dynamic routes that are ICMP redirect routes received from IPv6 routers by using ICMP redirect messages. This could happen when the default router the device uses is not the router for traffic to which the IPv6 subnets that the device wants to communicate.

The routing table is used to determine the next-hop address and the interface used for forwarding.

Each dynamic entry also has an associated invalidation timer value (extracted from Router Advertisements). This timer is used to delete entries that are no longer advertised.

To view the IPv6 Routes Table:

- Click **System > IPv6 Addressing > IPv6 Routes Table** in the tree view to display the **IPv6 Routes Table** page.

  The following is displayed for each IP address:

  – **IPv6 Prefix** — The destination IPv6 address prefix.

- **Prefix Length** — The length of the IPv6 prefix. This field is applicable only when the destination address is defined as a global IPv6 address.
- **Interface** — The interface that is used to forward the packet. Interface refers to any Port, LAG or VLAN.
- **Next Hop** — The address to which the packet is forwarded on the route to the Destination address (typically the address of a neighboring router). This can be either a Link Local or Global IPv6 address.
- **Metric** — The cost value used for comparing this route to other routes with the same destination in the IPv6 route table.
- **Life-Time** — The timeout interval of the route if no activity takes place. **Infinite** means the address is never deleted.
- **Route Type** — Specifies whether the destination is directly-attached and the means by which the entry was learned. The possible options are:
  - **Local** — A directly-connected route entry.
  - **Static** — Manually configured route, supported only for default gateway, learned through the Neighbor Discover (ND) process.
  - **ICMP** — The route was learned through ICMP Redirect messages, sent by the router.
  - **ND** — Route was learned by the ND protocol from Router Advertisement messages.

Viewing IPv6 Routes Table Parameters Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **IPv6 Router** page.

Table 8-17. IPv6 Routes Table CLI Commands

CLI Command	Description
`show ipv6 route [{Connected | Static | ICMP | ND}]`	Displays the current state of the ipv6 routing table.

The following is an example of the CLI commands:

```
console> show ipv6 route
Codes: L - Local, S - Static, I - ICMP, ND - Router
Advertisement
The number in the brackets is the metric.
S::/0 via fe80::77 [0] VLAN 1 Lifetime Infinite
ND::/0 via fe80::200:cff:fe4a:dfa8 [0] VLAN 1 Lifetime
1784 sec
L 2001::/64 is directly connected, g2 Lifetime Infinite
L 2002:1:1:1::/64 is directly connected, VLAN 1 Lifetime
2147467 sec
L 3001::/64 is directly connected, VLAN 1 Lifetime
Infinite
L 4004::/64 is directly connected, VLAN 1 Lifetime
Infinite
L 6001::/64 is directly connected, g2 Lifetime Infinite
```

IPv6 Default Gateway

Use the **IPv6 Default Gateway** pages to configure and view the default IPv6 router addresses. This list contains routers that are candidates to become the switch default router for non-local traffic. The switch randomly selects a router from the list. The switch supports one static IPv6 default router. Dynamic default routers are routers that have sent router advertisements to the switch IPv6 interface.

When adding or deleting IP addresses, the following events occur:

- When removing an IP interface, all of its default gateway IP addresses are removed.
- Dynamic IP addresses cannot be removed.
- An alert message is displayed after a user attempts to insert more than one IP address.
- An alert message is displayed when attempting to insert a non-Link Local type address.

To configure a router:

1 Click **System** > **IPv6 Addressing** > **IPv6 Default Gateway** in the tree view to display the **IPv6 Default Gateway: Summary** page.

  The previously-defined routers are displayed with the following fields:

  – **Default Gateway IPv6 Address** — The router's address.

  – **Interface** — The interface on which the router is accessed.

  – **Type** — The means by which the default gateway was configured. The possible options are:

    - **Static** — The default gateway is user-defined.
    - **Dynamic** — The default gateway is dynamically configured through router advertisement.

  – **State** (for R1-2401)— The router's status. The possible options are:

    - **Incomplete** — Address resolution is in progress and the link-layer address of the default gateway has not yet been determined.
    - **Reachable** — The default gateway is known to have been reachable recently (within tens of seconds ago).
    - **State** — (for R1-2401)The default gateway is no longer known to be reachable but until traffic is sent to the default gateway, no attempt is made to verify its reachability.
    - **Delay**-— The default gateway is no longer known to be reachable, and traffic has recently been sent to the default gateway. Rather than probe the default gateway immediately, however, there is a delay sending probes for a short while in order to give upper-layer protocols a chance to provide reachability confirmation.
    - **Probe** — The default gateway is no longer known to be reachable, and Unicast Neighbor Solicitation probes are being sent to verify reachability.
    - **Unreachable** — No reachability confirmation was received.

- **Metric** — (for R1-2210)Cost of this hop.

2 To add an IPv6 default gateway, click **Add,** and enter the fields:

- **IPv6 Address Type** — Displays that the IP address was added to the interface through a link local address.
- **Link Local Interface** — Displays the outgoing interface through which the default gateway can be reached.
- **Default Gateway IPv6 Address** — Enter the Link Local IPv6 address of the default gateway.
- **Metric** (For R1-2210)— Enter the cost of this hop.

NOTE: When defining a default gateway interface, ensure that the interface is in Layer 3 mode. This can be done via the radio button in **Switching > VLAN > Port Setting.**

Defining IPv6 Default Gateway Parameters Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **IPv6 Default Gateway** pages.

Table 8-18. IPv6 Default Gateway CLI Commands

CLI Command	Description

`ipv6 default-gateway` *`ipv6-address`*
`no ipv6 default-gateway`
	Defines an IPv6 default gateway.
	Use the no form of this command to remove the default gateway.

`show ipv6 route`	Displays the current state of the IPv6 routing table.

The following are examples of these CLI command:

```
console(config)# ipv6 default-gateway fe80::abcd
console(config-if)# do show ipv6 route
Codes: L - Local, S - Static, I - ICMP, ND - Router
Advertisement
The number in the brackets is the metric.
L 3000::/64 is directly connected, VLAN 20 Lifetime Infinite
L 4003::/64 is directly connected, VLAN 20 Lifetime Infinite
L 5003::/64 is directly connected, VLAN 20 Lifetime Infinite
L 6003::/64 is directly connected, VLAN 20 Lifetime Infinite
```

ISATAP Tunnel

To deliver IPv6 addresses in an IPv4 network, a tunneling process must be defined that encapsulates IPv6 packets in IPv4 packets.

The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an IPv6 transition mechanism that is used to transmit IPv6 packets between dual-stack nodes (nodes that can accept both IPv4 and IPv6 addresses) on top of an IPv4 network.

When enabling ISATAP on a tunnel interface, an explicit IPv4 address is configured as the tunnel source, or an automatic mode exists, where the lowest IPv4 address is assigned to an IP interface. This source IPv4 address is used for setting the tunnel interface identifier according to ISATAP addressing conventions. When a tunnel interface is enabled for ISATAP, the tunnel source must be set for the interface in order for the interface to become active.

An ISATAP address is represented using the [64-bit prefix]:0:5EFE:w.x.y.z, where 5EFE is the ISATAP identifier and w.x.y.z is a public or private IPv4 address. Thus, a Link Local address will be represented as FE80::5EFE:w.x.y.z

After the last IPv4 address is removed from the interface, the ISATAP IP interface state becomes inactive and is represented as Down, however the Admin state remains Enabled.

When defining tunneling, note the following:

- An IPv6 Link Local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, and the interface state becomes **Active**.
- If an ISATAP interface is active, the ISATAP router IPv4 address is resolved via DNS by using ISATAP-to-IPv4 mapping. If the ISATAP DNS record is not resolved, the ISATAP host name-to-address mapping is searched in the host name cache.
- When an ISATAP router IPv4 address is not resolved via the DNS process, the status of the ISATAP IP interface remains Active. The system does not have a default gateway for ISATAP traffic until the DNS procedure is resolved.
- In order for an ISATAP Tunnel to work properly over an IPv4 network, an ISATAP router is must be set up.

To define an IPv6 ISATAP tunnel:

1. Click **System** > **IPv6 Addressing** > **ISATAP Tunnel** in the tree view to display the **ISATAP Tunnel** page.
2. Enter the fields:
   - **ISATAP Status** — Enable/disable the status of ISATAP on the device.
   - **IPv4 Address Type**— Select the type of the tunnel source IPv4 address used by the tunnel. The options are:
     - **Auto** — Use the dynamic address.
     - **None** — Disable the ISATAP tunnel
     - **Manual** — Use the manual address assigned.
   - **IPv4 Address** — Enter the local (source) IPv4 address of a tunnel interface.
   - **Tunnel Router's Domain Name** — Enter a specific automatic tunnel router domain name.
   - **ISATAP Router Solicitation Interval (10 - 3600)** — Enter the interval between router solicitations messages when there is no active router.
   - **ISATAP Robustness (1 - 20)** — Enter the number of Query/Router Solicitation refresh messages that the device sends per second.

   Select the **Use Default** option to use the default setting of a field.

Defining ISATAP Tunnel Parameters Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **ISATAP Tunnel** pages.

Table 8-19. ISATAP Tunnel CLI Commands

CLI Command	Description
interface tunnel *number*	Enters tunnel interface configuration mode.
tunnel mode ipv6ip {*isatap*} **no tunnel mode ipv6ip**	Configures an IPv6 transition mechanism global support mode. Use the no form of this command to remove an IPv6 transition mechanism.
tunnel isatap router *router-name* **no tunnel isatap router**	Configures a global string that represents a specific automatic tunnel router domain name. Use the no form of this command to remove the string associated with the router domain name and restore the default configuration.
tunnel source {*auto* | *ipv4-address* *ipv4-address***}** **no tunnel source**	Sets the local (source) IPv4 address of a tunnel interface. Use the no form of the command to delete the tunnel local address.
tunnel isatap solicitation-interval *seconds* **no tunnel isatap solicitation-interval**	Configures the interval between ISATAP router solicitations messages (when there is no active ISATAP router). Use the no form of this command to restore the default configuration.
tunnel isatap robustness *number* **no tunnel isatap robustness**	Configures the number of DNS Query/Router Solicitation refresh messages that the device sends. Use the no form of this command to restore the default configuration.
show ipv6 tunnel	Displays information on the ISATAP tunnel.

The following is an example of a CLI script to create a tunnel:

Table 8-20. ISATAP Tunnel CLI Script

CLI Command	Description
`console#config`	Enter Global Configuration mode.
`console(config)# interface vlan 1`	Enter Interface mode for VLAN 1.
`console(config-if)# ip address 10.5.225.40 /27`	Configure an IP address with prefix length of 27.

`console(config-if)# ip default-gateway 10.5.225.33`
`console(config-if)#exit`
	Set the address of the default gateway and exit Interface mode.

`console (config)# ip domain lookup`	Enable DNS lookup
`console(config)# ip name-server 176.16.1.18`	Define DNS server
`console(config)# interface tunnel 1`	Enter tunnel mode
`console(config-tunnel)#tunnel mode ipv6ip isatap`	Enable tunnel.
`console(config-tunnel)#tunnel source auto`	The system minimum IPv4 address will be used as the source address for packets sent on the tunnel interface.
`console(config-tunnel)# do show ipv6 tunnel`	Display tunnel configuration

IPv6 Neighbors

The IPv6 Neighbors feature is similar in functionality to the IPv4 Address Resolution Protocol (ARP) feature. It enables detecting Link Local addresses within the same subnet, and includes a database for maintaining reachability information about active neighbors.

The device supports a total of up to 64 neighbors, obtained statically or dynamically.

When removing an IPv6 interface, all neighbors entered statically or learned dynamically, are removed.

To add an IPv6 neighbor:

1. Click **System** > **IPv6 Addressing** > **IPv6 Neighbors** in the tree view to display the **IPv6 Neighbors: Summary** page.

   The following fields are displayed for previously-defined neighbors:

   - **Interface**—Interface connected to the neighbor.
   - **IPv6 Address**—IPv6 address of the neighbor.
   - **MAC Address**—MAC address of the neighbor.
   - **Type**—Neighbor discovery cache information entry type (static or dynamic).
   - **State** (for R1-2210)—The possible states are:
     - **Incomplete** — An address resolution is in progress, and the link-layer address of the neighbor has not yet been determined.
     - **Reachable** — The neighbor is known to have been reachable recently (within tens of seconds).
     - **State** — The neighbor is no longer known to be reachable, but until traffic is sent to the neighbor, no attempt is made to verify its reachability.
     - **Delay** — The neighbor is no longer known to be reachable, and traffic has recently been sent to the neighbor. Rather than probe the neighbor immediately, however, there is a delay sending probes for a short while, in order to give upper-layer protocols a chance to provide reachability confirmation.
     - **Probe** — The neighbor is no longer known to be reachable, and Unicast Neighbor Solicitation probes are being sent to verify reachability.
   - **Router**—Whether the neighbor is a router (Yes or NA).

2. To clear the Neighbors table, select one of the following options:

   - **None** — Does not clear any entries.
   - **Static Only** — Clears the static entries.
   - **Dynamic Only** — Clears the dynamic entries.
   - **All Dynamic and Static** — Clears the static and dynamic address entries.

3 To add a new IPv6 neighbor, click **Add,** and enter the fields:

- **IPv6 Interface** — Displays the interface on which the IPv6 address is defined.
- **IPv6 Address** — Enter the neighbor IPv6 address.
- **MAC Address** — Enter the MAC address assigned to the interface.

4 To modify or remove an IPv6 neighbor, click **Edit**, and enter the fields described on the **Add** page.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache, as learned through the IPv6 neighbor discovery process, you can convert the entry to a static entry. To do this, select **Static** in the **Type** field.

Defining IPv6 Neighbors Using CLI Commands

The following table summarizes the CLI commands for setting fields displayed in the **IPv6 Neighbors** pages.

Table 8-21. IPv6 Neighbors CLI Commands

CLI Command	Description
ipv6 neighbor *ipv6-address interface-id mac-address* **no ipv6 neighbor** [[*ipv6-address*] *interface-id*]	Configures a static entry in the IPv6 neighbor discovery cache. Use the no form of this command to remove a static IPv6 entry from the IPv6 neighbor discovery cache.
show ipv6 neighbors {*static* | *dynamic*}[***ipv6-address*** *ipv6-address*] [***mac-address*** *mac-address*] [*interface-id*]	Displays IPv6 neighbor discovery cache information.
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache.

The following is an example of the CLI commands:

```
console# config

console(config)# ipv6 neighbor 3000::a31b vlan 1
001b.3f9c.84ea

console# show ipv6 neighbors dynamic

Interface IPv6 Address HW Address      State     Router

--------- ----------- ----------      -----     -----

VLAN 1    3000::a31b   0001b.3f9c.84ea Reachable Yes
```

IPv6 Router

NOTE: This feature is supported in R1-2210 only.

This section describe how to configure the device as an IPv6 router. It contains the following topics:

- Router Advertisement
- IPv6 Prefixes

Router Advertisement

IPv6 routers are able to advertise their prefixes to neighboring devices. This feature can be enabled or suppressed per interface, as follows:

1. Click **System** > **IPv6 Addressing** > **IPv6 Router** > **Router Advertisement**.
2. To configure an interface listed in the Router Advertisement Table, select it and click **Edit**.
3. Enter the following fields:
   - **Suppress Router Advertisement**—Select Yes to suppress IPv6 router advertisement transmissions on the interface. If this feature is not suppressed, enter the following fields.
   - **Router Preference**—Select either Low, Medium or High preference for the router. Router advertisement messages are sent with the preference configured in this field. If no preference is configured, they are sent with a medium preference.

Associating a preference with a router is useful when, for example, two routers on a link provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

- **Include Advertisement Interval Option**—Select to indicate that an advertisement option will be used by the system. This option indicates to a visiting mobile node the interval at which that node may expect to receive router advertisements. The node may use this information in its movement detection algorithm.
- **Hop Limit (1-255)**—This is the value that the router advertises. If it is not zero, it is used as the hop limit by the host.
- **Managed Address Configuration Flag**—Select this flag to indicate to attached hosts that they should use stateful auto configuration to obtain addresses. Hosts may use stateful and stateless address auto configuration simultaneously.
- **Other Stateful Configuration Flag**—Select this flag to indicate to attached hosts that they should use stateful auto configuration to obtain other (non address) information.

NOTE: If the Managed Address Configuration flag is set, an attached host can use stateful auto configuration to obtain the other (non address) information regardless of the setting of this flag.

- **Neighbor Solicitation Retransmissions Interval (1000-3600000)**—Set the interval to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.
- **Maximum Router Advertisement Interval(4-1800)**—Enter the maximum amount of time that can pass between router advertisements.

  The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using this command. To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum and maximum values.

- **Minimum Router Advertisement Interval(3-1350)**—Enter the minimum amount of time that can pass between router advertisements (**User Defined**) or select **Use Default** to user the system default.
- The minimum RA interval may never be more than 75% of the maximum RA interval and never less than 3 seconds.
- **Router Advertisement Lifetime(0-65535)**—Enter the remaining length of time, in seconds, that this router will continue to be useful as a default router. A value of zero indicates that it is no longer useful as a default router.
- **Reachable Time (0 - 4294967295)**—Enter the amount of time that a remote IPv6 node is considered reachable (in milliseconds) (**User Defined**) or select the **Use Default** option to use the system default.

4 Click **Apply** to save the configuration to the Running Configuration file.

Configuring Router Advertisements Using the CLI Commands

The following table summarizes the CLI commands for router advertisements.

Table 8-22. Router Advertisements CLI Commands

CLI Command	Description

`ipv6 nd advertisement-interval`
`no ipv6 nd advertisement-interval`
	Enables the advertisement interval option in router advertisements (RAs).
	Use the no form of this command to disable the interval option.

`ipv6 nd dad attempts` *value* **`no ipv6 nd dad attempts`**	Configures the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the Unicast IPv6 addresses of the interface. Use the no form of this command to return the number of messages to 1.

Table 8-22. Router Advertisements CLI Commands *(continued)*

CLI Command	Description
ipv6 nd managed-config-flag **no ipv6 nd managed-config-flag**	Sets the "managed address configuration flag" in IPv6 router advertisements. Use the no form to clear the flag.
ipv6 nd ns-interval *milliseconds* **no ipv6 nd ns-interval**	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface. Use the no form of this command to return to the default value.
ipv6 nd prefix {*ipv6-prefix/prefix-length* | **default**} [**no-advertise** | {[*valid-lifetime preferred-lifetime*] [**no-autoconfig**] [**off-link** | **no-onlink**]}] **no ipv6 nd prefix** [ipv6-prefix/prefix-length | **default**]	Configures which IPv6 prefixes are included in IPv6 Neighbor Discovery (ND) router advertisements. Use the no form of this command to return to the default value.
ipv6 nd ra lifetime *seconds* **no ipv6 ra lifetime**	Configures the Router Lifetime value in IPv6 router advertisements on an interface Use the no form of this command to return to the default value.
ipv6 nd ra suppress **no ipv6 ra suppress**	Suppresses IPv6 router advertisement transmissions on an interface. Use the no form of this command to return to the default value.
ipv6 nd reachable-time *milliseconds* **no ipv6 nd reachable-time**	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. Use the no form of this command to return to the default value.

Table 8-22. Router Advertisements CLI Commands *(continued)*

CLI Command	Description
ipv6 nd router-preference {high | medium | low} **no ipv6 nd router-preference**	Configures a default router preference (DRP) for the router on a specific interface. Use the no form to return the default value.

The following is an example of the CLI commands:

```
console(config)# vlan 2
console(config-interface)#ipv6 address 2001::1/64
console(config-interface)#ipv6 nd advertisement-interval
console(config-interface)#ipv6 nd hop-limit 15
console(config-interface)#ipv6 nd managed-config-flag
console(config-interface)#ipv6 nd ns-interval 9000
console(config-interface)#ipv6 nd prefix 2001::/64 3600
3600 no-onlink
console(config-interface)#ipv6 nd ra lifetime 1801
console(config-interface)#ipv6 nd ra suppress
console(config-interface)#ipv6 nd router-preference high
```

IPv6 Prefixes

To define prefixes to be advertised on the interfaces of the device:

1 Click **System** > **IPv6 Addressing** > **IPv6 Router** > **IPv6 Prefixes**.

2 If required, enable the Filter field and click **Go**. The group of interfaces matching the filter are displayed.

3 To add an interface, click **Add**.

4 Select the required IPv6 Interface on which a prefix is to be added.

5 Enter the following fields:

- **IPv6 Prefix**—Enter the following for the address to be defined on the interface:

    - *Prefix Address*—The IPv6 network. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal—using 16-bit values between colons.
    - *Prefix-Length*—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value
- **Prefix Advertisement**—Select to advertise this prefix.
- **Valid Lifetime(1 - 4294967295)**—Remaining length of time, in seconds, that this prefix will continue to be valid, i.e., time until invalidation. The address generated from an invalidated prefix should not appear as the destination or source address of a packet.
    - **Infinite**—Select this value to set the field to 4,294,967,295, which represents infinity.
    - **User Defined**—Enter a value.
- **Preferred Lifetime (1-Valid-Lifetime)**—The remaining length of time, in seconds, that this prefix will continue to be preferred. After this time has passed, the prefix should no longer be used as a source address in new communications, but packets received on such an interface are processed as expected. The preferred-lifetime must not be larger than the valid-lifetime.
    - *Infinite*—Select this value to set the field to 4,294,967,295, which represents infinity.
    - *User Defined*—Enter a value.
- **Auto Configuration**—Enable automatic configuration of IPv6 addresses using stateless auto configuration on an interface and enable IPv6 processing on the interface. Addresses are configured depending on the prefixes received in Router Advertisement messages
- **Prefix Status**—Select one of the following options:
    - *Onlink*—Configures the specified prefix as on-link. Nodes sending traffic to addresses that contain the specified prefix consider the destination to be locally reachable on the link. An onlink prefix is inserted into the routing table as a connected prefix (L-bit set).

- *No Onlink*—Configures the specified prefix as not onlink. A no onlink prefix is inserted into the routing table as a connected prefix but advertised with a L-bit clear.
- *Offlink*—Configures the specified prefix as offlink. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a connected prefix. If the prefix is already present in the routing table as a connected prefix (for example, because the prefix was also configured by adding an IPv6 address), it will be removed.

6 Click **Apply** to save the configuration to the Running Configuration file.

Configuring IPv6 Prefixes Using the CLI Commands

The following table summarizes the CLI commands for router advertisements.

Table 8-23. Pv6 Prefixes CLI Commands

CLI Command	Description
ipv6 route *ipv6-prefix/prefix-length* {*next--ipv6-address* | *interface-id*} [**metric**] **no ipv6 route** *ipv6-prefix/prefix-length* {*next--ipv6-address* | *interface-id*}	Establishes static IPv6 routes. Use the no form of this command to remove a previously configured static route.
ipv6 nd prefix {*ipv6-prefix/prefix-length* | **default**} [**no-advertise** | {[*valid-lifetime preferred-lifetime*][**no-autoconfig**] [**off-link** | **no-onlink**]}] **no ipv6 nd prefix** {*ipv6-prefix/prefix-length* | **default**}	Configures which IPv6 prefixes are included in IPv6 Neighbor Discovery (ND) router advertisements. Use the no form of this command to disable the interval option.

The following is an example of the CLI commands:

```
console(config)# vlan 2
console(config-interface)#ipv6 nd prefix 2001:0DB8::/35
1000 900
```

9

Network Security

This section describes the various mechanisms for providing security on the switch.

It contains the following topics:

- Port Security
- ACLs
- ACL Binding
- Proprietary Protocol Filtering
- Time Range
- Dot1x Authentication

Port Security

Network security can be enhanced by limiting access on a port to users with specific MAC addresses. The MAC addresses can be dynamically learned, or they can be statically configured.

Port security has the following modes:

- **Classic Lock** — Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port before it was locked.
- **Limited Dynamic Lock** — When a packet is received on a locked port, and the packet's source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), a protection mechanism, which provides various options is invoked. Unauthorized packets arriving to a locked port are either:
  - Forwarded
  - Discarded with no trap

- Discarded with a trap
- The port is shutdown

Locked port security enables storing a list of MAC addresses in the configuration file. The MAC addresses are restored when the device is reset.

Disabled ports can be activated from the **Port Configuration** page.

To configure port security:

1. Click **Switching** > **Network Security** > **Port Security** to display the **Port Security: Summary** page.

   Security parameters are displayed for all ports or LAGs, depending on the selected interface type.

2. To modify the security parameters for a port, select it, and click **Edit**.
3. Enter the following fields:
   - **Interface** — Select the interface to be configured. The possible options are **External Port, Internal Port** or **LAG**.
   - **Current Port Status** — Displays the current port status.
   - **Set Port** — Select to either lock or unlock the port.
   - **Learning Mode** — Set the locked port type. The **Learning Mode** field is enabled only if **Locked** is selected in the **Set Port** field. The possible options are:
     - **Classic Lock** — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
     - **Limited Dynamic Lock** — Locks the port by deleting the dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.
   - **Max Entries (0-128)** — Enter the maximum number of MAC addresses that can be learned on the port. The **Max Entries** field is enabled only if **Locked** is selected in the **Set Port** field, and the **Limited Dynamic Lock** mode is selected in **Learning Mode** field.
   - **Action on Violation** — Select the action to be applied to packets arriving on a locked port. The possible options are:
     - **Discard** — Discard the packets from any unlearned source.

        - **Forward** — Forward the packets from an unknown source, without learning the MAC address.
        - **Shutdown** — Discard the packet from any unlearned source, and shut down the port. Ports remain shutdown until they are reactivated, or the device is reset.
    - **Trap** — Enable/disable traps being sent when a packet is received on a locked port.
    - **Trap Frequency (1-1000000)** — Enter the amount of time (in seconds) between traps.

Configuring Port Security Using CLI Commands

The following table summarizes the CLI commands for configuring port security.

Table 9-1. Port Security CLI Commands

CLI Command	Description
set interface active {*interface-id*}	Reactivates an interface that is shut down due to port security reasons.
port security max {*max-addr}* **no port security max**	Specifies the maximum number of MAC addresses that can be learned on the port. Use the no form of this command to restore the default
port security mode {*max-addresses* | *lock*} **no port security mode**	Configures the port security learning mode. Use the no form of this command to restore the default configuration.
port security [*forward* | *discard* | *discard-shutdown*] [*trap* *seconds*] **no port security**	Enables port security on an interface. Use the no form of this command to disable port security on an interface.

Table 9-1. Port Security CLI Commands *(continued)*

CLI Command	Description
port security [***forward***|***discard***|***discard-shutdown***] [***trap*** *seconds*] **no port security**	Configures port security on an interface. Use the no form of this command to disable port security.
show ports security [*interface-id* | **detailed**]]	Displays lock status of specified interface or of all interfaces.

The following is an example of the CLI commands:

```
console # show ports security
Port    Status   Learning       Action          Maximum   Trap     Frequency
------- -------- --------      --------         -------   ----     ---------
gi0/1 Disabled Max-Addresses   -                 10        -         -
gi0/2 Disabled Lock            -                 1         -         -
gi0/3 Disabled Lock            -                 1         -         -
gi0/4 Disabled Lock            -                 1         -         -
gi0/5 Disabled Lock            -                 1         -         -
gi0/6 Disabled Lock            -                 1         -         -
gi0/7 Disabled Lock            -                 1         -         -
gi0/8 Disabled Lock            -                 1         -         -
```

ACLs

This section describes Access Control Lists (ACLs), which enable defining classification actions and rules for specific ingress or egress ports.

It contains the following topics:

- ACL Overview
- MAC-Based ACLs
- MAC-Based ACEs
- IPv4-Based ACLs
- IPv4-Based ACEs
- IPv6-Based ACLs
- IPv6-Based ACEs

ACL Overview

Access Control Lists (ACLs) enable network managers to define classification actions and rules for specific ingress or egress ports. Packets entering an ingress or egress port, with an active ACL, are either admitted or denied entry. If entry is denied, the ingress or egress port may be disabled, for example, a network administrator defines an ACL rule that states that port number 20 can receive TCP packets, however, if a UDP packet is received, the packet is dropped.

ACLs are composed of Access Control Entries (ACEs) that are rules that determine traffic classifications. Each ACE is a single rule, and up to 256 rules may be defined on each ACL, and up to 3000 rules globally.

Rules are not only used for user configuration purposes, they are also used for features like DHCP Snooping, and Protocol Group VLAN, so that not all 3000 rules are available for ACEs. It is expected that there will be at least 2000 rules available. If there are fewer rules available, this may be due to DHCP Snooping. Reduce the number of entries in DHCP Snooping to free rules for ACEs.

The following types of ACLs can be defined:

- **MAC-based ACL** — Examines Layer 2 fields only
- **IPv4-based ACL** —Examines the Layer 3 layer of IPv4 frames
- **IPv6-based ACL** —Examines the Layer 3 layer of IPv6 frames

MAC-Based ACLs

To define a MAC-based ACL:

1. Click **Switching** > **Network Security** > **MAC Based ACL** to display the **MAC Based ACL: Summary** page.

   The currently-defined MAC-based ACLs are displayed.

2. To add a new ACL, click **Add ACL**, and enter the name of the new ACL.

Configuring MAC-Based ACLs Using CLI Commands

The following table summarizes the CLI commands for configuring MAC-based ACLs.

Table 9-2. MAC Based ACL CLI Commands

CLI Command	Description
mac access-list extended *acl-name* **no mac access-list extended** *acl-name*	Defines an ACL and places the device in MAC-extended ACL configuration mode. Use the no form of this command to remove the ACL.
show interfaces access-lists [*interface-id*]	Displays access lists applied on interfaces.

The following is an example of some of the CLI commands:

```
console# show access-lists
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8  0.0.0.0 any
```

MAC-Based ACEs

To add rules to an ACL:

1 Click **Switching** > **Network Security** > **MAC Based ACE** to display the **MAC Based ACE: Summary** page.

The currently-defined rules for the selected ACL are displayed.

2 To add a rule click **Add ACE**.

3 Select the ACL for which a rule is being created.

4 Enter the fields:

– **New Rule Priority** — Enter the priority of the ACE. ACEs with higher priority are processed first. One is the highest priority

– **Source MAC Address** — Match the source MAC address from which packets have arrived to this source address. In addition to the Source MAC address, you can enter a **Wildcard Mask** that specifies which bits in the source address are used for matching and which bits are ignored. A wildcard of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.

- **Any** — Check to indicate that the source address is not matched.
- **Dest. MAC Address** — Match the destination MAC address to which packets are addressed to this address. In addition to the Destination MAC address, you can enter a **Wildcard Mask** that specifies which bits in the source address are used for matching and which bits are ignored. A wildcard of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
- **Any** — Check to indicate that the destination address is not matched.
- **VLAN ID** — Match the packet's VLAN ID to this VLAN ID. The possible VLAN IDs are 1 to 4095.
- **CoS** — Match the packet's CoS value to this CoS value.
- **Cos Mask** — Match the packet's CoS value to one of these CoS values.
- **Ether type** — Match the packet's Ethertype to this one.
- **Time Range Name** — Check to associate a time range with the ACE. Select one of the time ranges defined in the **Time Range** page.
- **Action** — Select the action taken upon a match. The following options are available:
  - **Permit** — Forward packets that meet the ACL criteria.
  - **Deny** — Drop packets that meet the ACL criteria.
  - **Shutdown** — Drop packets that meet the ACL criteria, and disable the port to which the packet was addressed.
- **Logging of Dropped Packets** — Check to activate logging of dropped packets.

Configuring MAC-Based ACEs Using CLI Commands

The following table summarizes the CLI commands for configuring MAC-based ACEs.

Table 9-3. MAC Based ACE CLI Commands

CLI Command	Description
permit {**any** | *source* source-wildcard} {***any*** |***destination*** *destination-wildcard*} [**eth-type** *0* | ***aarp*** | ***amber***|***dec-spanning*** | ***decnet-iv*** | ***diagnostic*** | ***dsm*** | ***etype-6000***] [**vlan** *vlan-id*] [***cos*** *cos cos-wildcard*] [***time-range*** *time-range-name*]	Sets permit conditions for an MAC access list (in MAC ACL configuration mode).
deny {***any***|*source source-wildcard*} {***any***|*destination destination-wildcard*} [***eth-type*** 0|***aarp***|***amber***|***dec-spanning***|***decnet-iv*** | ***diagnostic*** |***dsm***|***etype-6000***] [***vlan*** *vlan-id*] [***cos*** *cos cos-wildcard*] [***time-range*** *time-range-name*][***disable-port***|***log-input***]	Sets deny conditions for an MAC access list.

The following is an example of some of the CLI commands:

```
console(config)# mac access-list extended server1
console(config-mac-al)# permit 00:00:00:00:00:01
00:00:00:00:00:ff any
```

IPv4-Based ACLs

To define an IPv4-based ACL:

1 Click **Switching > Network Security > IPv4 Based ACL** to display the **IPv4 Based ACL: Summary** page.

The previously-defined IPv4 ACLs are displayed.

2 To add a new ACL, click **Add ACL**.

3 Enter the name of the new ACL. Names are case-sensitive.

Configuring IP-based ACLs Using CLI Commands

The following table summarizes the CLI commands for configuring IP-based ACLs.

Table 9-4. IP-Based ACL CLI Commands

CLI Command	Description

`ip access-list extended` *`acl-name`*
`no ip access-list extended` *`acl-name`*
	Defines an IPv4 access list and places the device in IPv4 access list configuration mode
	Use the no form of this command to remove the access list.

The following is an example of some of the CLI commands:

```
console(config)# ip access-list extended server-acl
```

IPv4-Based ACEs

To add a rule to an ACL:

1. Click **Switching** > **Network Security** > **IPv4 Based ACE** to display the **IPv4 Based ACE** page.

   The currently-defined rules for the selected ACL are displayed.

2. To add a rule, click **Add ACE**.

3. Select a user-defined ACL, and enter the following fields:

   – **New ACE Priority (1-2147483647)** —Enter the priority of the ACE. ACEs with higher priority are processed first. One is the highest priority.

   – **Protocol Select From List** — Select to create an ACE, based on a specific protocol. The following options are available:

     - **ICMP —** Internet Control Message Protocol (ICMP). The ICMP enables the gateway or destination host to communicate with the source host, for example, to report a processing error.

     - **IGMP —** Internet Group Management Protocol (IGMP). Enables hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.

- **IPinIP** — IP in IP. Encapsulates IP packets to create tunnels between two routers. This ensures that the IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP enables tunnel intranets occur the internet, and provides an alternative to source routing.
- **TCP —** Transmission Control Protocol (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they are sent.
- **EGP —** Exterior Gateway Protocol (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network.
- **IGP —** Interior Gateway Protocol (IGP). Enables for routing information exchange between gateways in an autonomous network.
- **UDP —** User Datagram Protocol (UDP). Communication protocol that transmits packets but does not guarantee their delivery.
- **HMP** — Host Mapping Protocol (HMP). Collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network.
- **RDP —** Reliable Data Protocol (RDP). provide a reliable data transport service for packet-based applications.
- **IDPR** — Matches the packet to the IDPR protocol.
- **IDRP** — Matches the packet to the Inter-Domain Routing Protocol (IDRP).
- **RVSP** — Matches the packet to the ReSerVation Protocol (RSVP).
- **AH** — Authentication Header (AH). Provides source host authentication and data integrity.
- **EIGRP** — Enhanced Interior Gateway Routing Protocol (EIGRP). Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.

  - **OSPF** — The Open Shortest Path First (OSPF) protocol is a link-state, hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).
  - **IPIP** — IP over IP (IPinIP). Encapsulates IP packets to create tunnels between two routers. This ensures that the IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP enables tunnel intranets occur the internet, and provides an alternative to source routing.
  - **PIM** — Matches the packet to Protocol Independent Multicast (PIM).
  - **L2TP** — Matches the packet to Internet Protocol (L2IP).
  - **ISIS** — Intermediate System - Intermediate System (ISIS). Distributes IP routing information throughout a single autonomous system in IP networks.
- **Protocol ID To Match** — Enter a protocol number if you did not select a protocol by name.
- **Any (IP)** — Check to use any protocol.
- **Source Port (0 - 65535)** — Enter the TCP/UDP source port. Enter either **Single**, **Range** or select **Any** to include all ports.
- **Destination Port (0 - 65535)** — Enter the TCP/UDP destination port. Enter either a **Single**, **Range** or select **Any** to include all ports.
- **Source IP Address** — Enter the source IP address to which addresses in the packet are compared.
  - **Wildcard Mask** —In addition to the **Source MAC address**, you can enter a mask that specifies which bits in the source address are used for matching and which bits are ignored. A wildcard of 0.0.0.0 means the bits must be matched exactly in addition to the IP source address; ff.ff.ff.ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
  - **Any** — Check to indicate that the source address is not matched.

- **Dest. IP Address** — Enter the destination IP address to which addresses in the packet are compared.
  - **Wildcard Mask** —In addition to the Destination MAC address, you can enter a mask that specifies which bits in the source address are used for matching and which bits are ignored. A wildcard of 0.0.0.0 means the bits must be matched exactly in addition to the IP destination address; ff.ff.ff.ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
  - **Any** — Check to indicate that the destination address is not matched.
- **TCP Flags** — To use TCP flags, check the **TCP Flag** checkbox and then check the desired flag(s).
- **ICMP** — Specifies an ICMP message type for filtering ICMP packets. This field is available only when ICMP is selected in the **Protocol** field. The following options are available:
  - **Select from List** — Select an ICMP type from the list.
  - **ICMP Type** — Enter the ICMP type.
  - **Any** — Check to use all ICMP types.
- **ICMP Code** — Enter an ICMP message code for filtering ICMP packets that are filtered by ICMP message type or ICMP message code. This field is available only when ICMP is selected in the **Protocol** field. The following options are available:
  - **ICMP Code** — Enter an ICMP code.
  - **Any** — Check to use all ICMP codes.
- **IGMP** — IGMP packets can be filtered by IGMP message type. This field is available only when IGMP is selected in the **Protocol** field. The following options are available:
  - **Select from List** — Select an IGMP message type from the list.
  - **IGMP Type** — Enter the IGMP message type.
  - **Any** — Check to use all IGMP message types.
- **Classification** — Select one of the following matching options:
  - **Match DSCP(0-63)** — Matches the packet DSCP value to the ACL.

    - **Match IP Precedence(0-7)** — Check to enable matching IP-precedence with the packet IP-precedence value. IP-precedence enables marking frames that exceed the CIR threshold. In a congested network, frames containing a higher DP value are discarded before frames with a lower DP value. If this field is checked, enter a value to be matched.

- **Time Range Name** — Check to associate a time range with the ACE. Select one of the time ranges defined in the **Time Range** page.
- **Action** — Select the ACL forwarding action. The following options are available:
    - **Permit** — Forward packets which meet the ACL criteria.
    - **Deny** — Drop packets which meet the ACL criteria.
    - **Shutdown** — Drop packet that meet the ACL criteria, and disable the port to which the packet was addressed.
- **Logging of Dropped Packets** — Check to activate logging of dropped packets.

Configuring IP-based ACEs Using CLI Commands

The following table summarizes the CLI commands for configuring IP-based ACLs.

Table 9-5. IP-Based ACE CLI Commands

CLI Command	Description
permit ***protocol*** {***any*** |*source source-wildcard*} {***any*** |*destination destination-wildcard*} [***dscp*** *number* | ***precedence*** *number*] [***time-range*** *time-range-name*]	Sets conditions to allow a packet to pass a named IP access list (in access list configuration mode). Each form of this command is relevant to a specific protocol (icmp, igmp, tcp, udp)
permit icmp {***any*** |*source source-wildcard*} {***any*** |*destination destination-wildcard*} [***any*** |*icmp-type*][***any*** |*icmp-code*]] [***dscp*** *number* | ***precedence*** *number*] [***time-range*** *time-range-name*]	
permit igmp {***any*** |*source source-wildcard*} {***any*** |*destination destination-wildcard*}[*igmp-type*] [***dscp*** *number* | ***precedence*** *number*] [***time-range*** *time-range-name*]	
permit tcp {***any*** |*source source-wildcard*} {***any*** |*source-port/port-range*} {***any*** |*destination destination-wildcard*} {***any*** |*destination-port/port-range*} [***dscp*** *number* | ***precedence*** *number*] [***match-all*** *list-of-flags*] [***time-range*** *time-range-name*]	
permit udp {***any*** |*source source-wildcard*} {***any*** | *source-port/*port-range} {***any*** | *destination destination-wildcard*} {***any*** | *destination-port/port-range* } [***dscp*** *number* | ***precedence*** *number*] [***time-range*** *time-range-name*]	

Table 9-5. IP-Based ACE CLI Commands *(continued)*

CLI Command	Description
deny protocol {**any** |*source source-wildcard*} {**any** |*destination destination-wildcard*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*]	Sets deny conditions for IPv4 access list (in access list configuration mode).
deny icmp {**any** | *source source-wildcard*} {**any** |*destination* destination-wildcard} [**any** | icmp-type] [**any** | icmp-code] [**dscp** number | **precedence** number] [**time-range** time-range-name]	Each form of this command is relevant to a specific protocol (icmp, igmp, tcp, udp)
deny igmp {**any** | *source source-wildcard*} {**any** | *destination* destination-wildcard} [igmp-type] [**dscp** number | **precedence** number] [***time-range*** *time-range-name*]	
deny tcp {**any** | *source source-wildcard*} {**any** | *source-port* | *port-range*} {**any** | *destination* destination-wildcard} {**any** | destination-port/port-range} [**dscp** number | **precedence** number] [**match-all** list-of-flags] [**time-range** time-range-name]	
deny udp {**any** | *source source-wildcard*} {**any** | *source-port* | *port-range*} {**any** | *destination* destination-wildcard} {**any** | *destination-port* | *port-range*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*]	

The following is an example of some of the CLI commands:

```
console(config)# ip access-list extended server
console(config-ip-al)# permit ip 1.1.1.0 0.0.0.255
1.1.2.0 0.0.0.0
```

IPv6-Based ACLs

The IPv6 Based ACL Page displays and enables the creation of IPv6 ACLs, which check pure IPv6-based traffic. IPv6 ACLs do not check IPv6-over-IPv4 or ARP packets.

To define IPv6-based ACLs:

1. Click **Switching** > **Network Security** > **IPv6 Based ACL** to display the **IPv6 Based ACL: Summary** page.

   A list of all of the currently defined IPv6-based ACLs is displayed.

2. To add a new ACL, click **Add ACL**.
3. Enter the name of the new ACL. Names are case-sensitive.

Configuring IPv6-based ACLs Using CLI Commands

The following table summarizes the CLI commands for configuring IPv6-based ACLs.

Table 9-6. IP-Based ACL CLI Commands

CLI Command	Description

`ipv6 access-list [acl-name]`
`no ipv6 access-list [acl-name]`
	Defines an IPv6 access list and places the device in IPv6 access list configuration mode
	Use the no form of this command to remove the access list.

The following is an example of some of the CLI commands:

```
console(config)# ipv6 access-list server-acl
```

IPv6-Based ACEs

To add a rule to an IPv6-based ACL:

1. Click **Switching** > **Network Security** > **IPv6 Based ACE** to display the **IPv6 ACE: Summary** page.

   The currently-defined rules for the selected ACL are displayed.

2. To add a rule click **Add ACE**.
3. Select a user-defined ACL for which a rule is being created.
4. Enter the following fields:
   - **New Rule Priority** — Enter the ACE priority that determines which ACE is matched to a packet, based on a first match.
   - **Protocol Select from List** — Select to create an ACE, based on a specific protocol. The following options are available:
     - **ICMP —** Internet Control Message Protocol (ICMP). The ICMP allows the gateway or destination host to communicate with the source host. For example, to report a processing error.
     - **TCP** — Transmission Control Protocol (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order the are sent.
     - **UDP —** User Datagram Protocol (UDP). Communication protocol that transmits packets but does not guarantee their delivery.
     - **IPV6 —** Matches the packet to the IPV6 protocol.
   - **Protocol ID To Match** — Enter a protocol.
   - **Source Port** — Enter the TCP/UDP source port. Enter either a **Single**, **Range** or select **Any** to include all ports.
   - **Destination Port** — Enter the TCP/UDP destination port. Enter either a **Single**, **Range** or select **Any** to include all ports.
   - **TCP Flags** — To use TCP flags, check the **TCP Flag** checkbox and then check the desired flag(s).

- **ICMP** — Specifies an ICMP message type for filtering ICMP packets. This field is available only when ICMP is selected in the **Protocol** field. The following options are available:
  - **Select from List** — Select an ICMP type from the list.
  - **ICMP Type** — Enter the ICMP type.
  - **Any** — Check to use all ICMP types.
- **ICMP Code** — Specifies an ICMP message code for filtering ICMP packets that are filtered by ICMP message type or ICMP message code. This field is available only when ICMP is selected in the **Protocol** field. The following options are available:
  - **ICMP Code** — Enter an ICMP code.
  - **Any** — Check to use all ICMP codes.
- **Source IP Address** — Enter the source IP address to which addresses in the packet are compared. The following options are available:
  - **Prefix Length** —The number of bits that comprise the source IP address prefix of the subnetwork.
  - **Any** — Check to indicate that the source address is not matched.
- **Dest. IP Address** — Enter the destination IP address to which addresses in the packet are compared. The following options are available:
  - **Prefix Length** —The number of bits that comprise the destination IP address prefix of the subnetwork.
  - **Any** — Check to indicate that the destination address is not matched.
- **Traffic Class** — Select one of the following options:
  - **Match DSCP** — Matches the packet DSCP value to the ACL.
  - **Match IP Precedence** — Matches the IP-precedence with the packet IP-precedence value. IP-precedence enables marking frames that exceed CIR threshold. In a congested network, frames containing a higher DP value are discarded before frames with a lower DP value.
- **Time Range Name** — Check to associate a time range with the ACE. Select one of the time ranges defined in the **Time Range** page.

- **Action** — The ACL forwarding action. The following options are available:
  - **Permit** — Forwards packets that meet the ACL criteria.
  - **Deny** — Drops packets that meet the ACL criteria.
  - **Shutdown** — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.
- **Logging of Dropped Packets** — Check to activate logging of dropped packets.

Configuring IP-based ACEs Using CLI Commands

The following table summarizes the CLI commands for configuring IP-based ACLs.

Table 9-7. IP-Based ACE CLI Commands

CLI Command	Description
permit protocol {***any*** | {*source-prefix /length*} {**any** |*destination-prefix/length*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*]	Sets permit conditions for IPv6 access list.
permit icmp {***any*** | {*source-prefix/length*} {**any** |*destination-prefix/length*} {**any** | *icmp-type*} {***any*** | *icmp-code*} [**dscp** *number* | **precedence** *number*] [***time-range*** *time-range-name*]	
permit tcp {***any*** | {*source-prefix/length*} {**any** |*source-port/port-range*}} {**any** |*destination prefix/length* } {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** number] [***match-all*** *list-of-flags*] [**time-range** *time-range-name*]	
permit udp {***any*** |{*source-prefix/length*}} {***any*** | *source-port* | *port-range*}} {***any*** | *destination prefix/length*} {***any*** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [***time-range*** *time-range-name*]	

Table 9-7. IP-Based ACE CLI Commands *(continued)*

CLI Command	Description
deny protocol {***any*** |{*source-prefix/length*} {**any** | *destination-prefix/length*} [***dscp*** *number* | ***precedence*** *number*] [***time-range*** *time-range-name*] [***disable-port*** | ***log-input***]	Sets deny conditions for IPv6 access list (in Access List Configuration mode).
deny icmp {***any*** {*source-prefix/length*} {***any*** | *destination-prefix/length*} {***any*** | *icmp-type*} {***any*** | icmp-code} [***dscp*** *number* | ***precedence*** *number*] [***time-range*** time-range-name] [***disable-port*** | ***log-input***]	
deny tcp {***any*** | {*source-prefix/length*} {***any*** | *source-port/port-range*}} {***any*** | *destination-prefix/length*} {***any*** | *destination-port/port-range*} [***dscp*** *number* | ***precedence*** *number*] [***match-all*** *list-of-flags*] [***time-range*** time-range-name] [***disable-port*** | ***log-input***]	
deny udp {***any*** | {*source-prefix/length*}} {***any*** | source-port/port-range}} {***any*** | *destination-prefix/length*} {***any*** | *destination-port/port-range*} [***dscp*** *number* | ***precedence*** *number*] [***time-range*** *time-range-name*] [***disable-port*** | ***log-input***]	

The following is an example of some of the CLI commands:

```
console(config)# ipv6 access-list server
console(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

ACL Binding

When an ACL is bound to an interface, all the rules that have been defined for the ACL are applied to that interface. Whenever an ACL is assigned on a port or LAG, flows from that ingress or egress interface that do not match the ACL, are matched to the default rule, which is to **Drop unmatched packets**.

To change the default action for unmatched packets to an action other than Drop, do the following:

- Add an additional ACE to the ACL with "Any" in all fields
- Set its action other than Drop
- Set the priority to the lowest in the ACL.

To bind ACLs to interfaces:

1. Click **Switching** > **Network Security** > **ACL Binding** to display the **ACL Binding: Summary** page.

   The ports are displayed along with their associated ACLs.

2. To bind an ACL to an interface, select an interface and click **Edit**.
3. Select an ACL(s). You can select one of each type (**MAC-based ACL, IPv4-based ACL** or **IPv6-based ACL**) or one **IPv4-based ACL** and one **IPv6-based ACL**.

Configuring ACL Bindings Using CLI Commands

The following table summarizes the CLI commands for configuring ACL Bindings.

Table 9-8. ACL Bindings CLI Commands

CLI Command	Description
service-acl input *acl-name1* [*acl-name2*] **default-action [deny-any | permit-any]** **no service-acl input**	Controls access to an interface Use the no form of the command to remove access control.
show access-lists [*acl-name*]	Displays access control lists (ACLs) configured on the switch.

The following is an example of some of the CLI commands:

```
console(config)# mac access-list extended server
console(config-mac-al)# permit 00:00:00:00:00:01
00:00:00:00:00:ff any
console(config-mac-al)# exit
console(config)# interface gi/0/1
console(config-if)# service-acl input server
```

Proprietary Protocol Filtering

Protocol filters are used to disallow receiving specific proprietary protocol packets through an interface. These can be enabled for specific ports.

If a protocol filter is enabled on a port, you cannot enable a QoS ACL on this port.

To configure Proprietary Protocol Filtering:

1 Click **Switching** > **Network Security** > **Proprietary Protocol Filtering** to display the **Proprietary Protocol Filtering: Summary** page.

A list of the ports and their filtered protocols is displayed.

2 Click **Edit** to modify the filtered protocols for a specific port.

3 Select an interface.

4 Move the required protocols from the **Available Protocols** list to the **Filtered Protocols** list. The following displays the protocols and the addresses that are blocked:

Table 9-9. Protocol Filtering

Protocol	Destination Address	Protocol Type
blockcdp	0100.0ccc.cccc	0x2000
blockvtp	0100.0ccc.cccc	0x2003
blockdtp	0100.0ccc.cccc	0x2004
blockudld	0100.0ccc.cccc	0x0111
blockpagp	0100.0ccc.cccc	0x0104
blocksstp	0100.0ccc.cccd	-
blockall	0100.0ccc.ccc0 - 0100.0ccc.cccf	-

Configuring Proprietary Protocol Filtering Using CLI Commands

The following table summarizes the CLI commands for setting fields in the **Proprietary Protocol Filtering** pages.

Only one of the following CLI commands can be active on a port at the same time. To add other protocol filters, the command must be negated and then run again with all the required protocol names.

.

Table 9-10. Proprietary Protocol Filtering CLI Commands

CLI Command	Description
service-acl input *acl-name1* [*acl-name2*] **default-action [deny-any | permit-any]** **no service-acl input**	Discards packets that are classified to specific protocols. Use the no form of those commands to disable discarding of the packets.

The following is an example of some of the CLI commands:

```
console (Config-if)# service-acl input blockcdp blockvtp
```

Time Range

Time ranges can be defined and associated with commands, such as QoS ACL, so that it is applied only during that time range.

There are two types of time ranges:

- **Absolute** —This type of time range begins on a specific date or immediately and ends on a specific date or extends infinitely. It is created in the **Time Range** pages. A recurring element can be added to it.
- **Recurring** — This is a time range element that is added to an absolute range, and begins and ends on a recurring basis. It is defined in the **Time Range Recurrence** pages.

If a time range includes both absolute and recurring ranges, the ACL is activated only if both absolute start time and the recurring time range have been reached. The ACL is deactivated when either of the time ranges is reached.

The switch supports a maximum of 10 absolute time ranges.

All time specifications are interpreted as local time (Daylight Savings Time does not affect this).

To ensure that the time range entries take effect at the desired times, the system time must be set. For more information on setting the system time, see Time Synchronization.

A possible use for this feature is to limit access of computers to the network only during business hours, after which they are locked, and access to the rest of the network is blocked.

Absolute Time Range

To define an absolute time range:

1. Click **Switching** > **Network Security** > **Time Range** to display the **Time Range: Summary** page.

   The existing Time Ranges are displayed.

2. To add a new time range, click **Add**.

3. Enter the name of the time range in the **Time Range Name** field.
4. Define the **Absolute Start** time.
   - To begin the Time Range immediately, click **Immediate**.
   - To determine at what time in the future the Time Range will begin, enter values in the **Date** and **Time** fields.
5. Define the **Absolute End** time.
   - To indicate that the Time Range should not end, click **Infinite**.
   - To determine the time at which the Time Range ends, enter values in the **Date** and **Time** fields.

See Configuring Time Ranges Using CLI Commands for the CLI commands for creating time ranges.

Time Range Recurrence

To add a recurring time range element to an absolute time range:

1. Click **Switching** > **Network Security** > **Time Range Recurrence** to display the **Recurring Time Range: Summary** page.

   A daily and weekly recurring element of the time range that is selected is displayed if they exist.

2. To add a recurring time range element to a time range, click **Add.**
3. Select the **Time Range Name** to which you want to add the Time Range Recurrence. The **Absolute Start** and **Absolute End** fields are displayed.
4. Check if the recurrence is **Daily** or **Weekly** in **Recurrence type**.
5. If the recurrence is **Daily**, enter:
   - **Start Time** — Select the time on which the time range starts.
   - **End Time**— Select the time on which the time range ends.
   - **Weekday** — Select the day of the week on which the time range occurs.
6. If the recurrence is **Weekly**, enter:
   - **Start** — Select the **Day of the Week** and **Time** on which the time range starts.
   - **End** —Select the **Day of the Week** and **Time** on which the time range ends.

Configuring Time Ranges Using CLI Commands

The following table summarizes the CLI commands for configuring time ranges.

Table 9-11. Time Range CLI Commands

CLI Command	Description
time-range *time-range-name* **no time-range** *time-range-name*	Enables time-range configuration mode, and defines time ranges for functions (such as access lists). Use the no form of this command to remove the time range configuration.
absolute start *hh:mm day month year* **no absolute start** **absolute end** *hh:mm day month year* **no absolute end**	Adds start and end times to the time range. Use the no form of the commands to remove the start and end times from the time range.
periodic *day-of-the-week hh:mm* ***to*** *day-of-the-week hh:mm* **no periodic** *day-of-the-week hh:mm* ***to*** *day-of-the-week hh:mm* ***periodic list*** *hh:mm* ***to*** *hh:mm day-of-the-week1* [*day-of-the-week2… day-of-the-week7*] **no periodic list** *hh:mm* ***to*** *hh:mm day-of-the-week1* [*day-of-the-week2… day-of-the-week7*] **periodic list** *hh:mm* ***to*** *hh:mm all* **no periodic list all** *hh:mm* ***to*** *hh:mm all*	Adds a recurring time range to the time range. Use the no form of the commands to remove the recurring time range.

The following is an example of some of the CLI commands:

```
console (config)# time-range http-allowed

console (config-time-range)# absolute start 12:00 1 jan
2005 end 12:00 31 dec 2005

console (config-time-range)# periodic monday 8:00 to
friday 20:00
```

Dot1x Authentication

This section describes Dot1x authentication.

It contains the following topics:

- Port-Based Authentication Overview
- Dot1x Overview
- Port-Based Authentication Global
- Port-Based Authentication Interface Settings
- Monitoring Users
- Host Authentication
- Port Authentication Users

Port-Based Authentication Overview

Port-based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP). Port Authentication includes:

- **Authenticators** — Specifies the device port that is authenticated before permitting system access.
- **Supplicants** — Specifies the host connected to the authenticated port hat is requesting to access the system services.
- **Authentication Server** — Specifies the external server, for example, a RADIUS server, which performs authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Port-based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication, regardless of the port authorization state.

The device supports Port Based Authentication via RADIUS servers.

Dot1x Overview

Dot1x is an IEEE standard for port-based network access control. The Dot1x framework enables a device (the supplicant) to request port access from a remote device (authenticator) to which it is connected. The supplicant is permitted to send data to the port only after it is authenticated and authorized. If it is not authenticated and authorized, the authenticator discards the supplicant data, unless the data is sent to a Guest VLAN and/or non-authenticated VLANs.

Authentication of the supplicant is performed by an external RADIUS server through the authenticator. The authenticator monitors the results of the authentication.

In the Dot1x standard, a device can be a supplicant and an authenticator at a port, simultaneously requesting and granting port access. However, this device can only act as an authenticator, and does not take on the role of a supplicant.

The following varieties of Dot1x exist:

- **Single session Dot1x:**
  - **A1—Single-session/Single Host** — In this mode, the switch, as an authenticator, supports a single Dot1x session, and grants permission to use the port to an authorized supplicant. All other access requests, made by other devices received from the same port, are denied until the authorized supplicant is no longer using the port, or the access request is to an unauthenticated or guest VLAN.
  - **Single-session/Multiple Hosts**—This follows the Dot1x standard. In this mode, the switch, as an authenticator, enables any device to use a port, as long as it has been granted permission as a supplicant at the port.

- **Multi-Session Dot1x**—Every device (supplicant) connecting to a port must be authenticated and authorized by the switch (authenticator), separately in a different Dot1x session. This is the only mode that supports Dynamic VLAN Assignment (DVA).

Dynamic VLAN Assignment (DVA)

Dynamic VLAN Assignment (DVA) is also referred to as RADIUS VLAN Assignment in this guide. When a port is in Multiple Session mode and is DVA-enabled, the switch automatically adds the port as an untagged member of the VLAN that is assigned by the RADIUS server during the authentication process. The switch classifies untagged packets to the assigned VLAN if the packets originated from the devices or ports that are authenticated and authorized.

For a device to be authenticated and authorized at a DVA-enabled port:

- The RADIUS server must authenticate the device and dynamically assign a VLAN to the device.
- The assigned VLAN must not be the default VLAN and must have been created on the switch.
- The switch must not be configured to use both a DVA and a MAC-based VLAN group.
- A RADIUS server must support DVA with RADIUS attributes tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6), and tunnel-private-group-id = a VLAN ID.

Dynamic Policy/ACL Assignment

The Dynamic Policy/ACL Assignment feature enables specifying a user-defined ACL or policy in the RADIUS server. After a successful authentication, the user is assigned that ACL.

Authentication Methods

The possible authentication methods are:

- **Dot1x** — The switch supports this authentication mechanism, as described in the standard, to authenticate and authorize Dot1x supplicants.

- **MAC-based** — The switch can be configured to use this method to authenticate and authorize devices that do not support Dot1x. The switch emulates the supplicant role on behalf of the non-Dot1x-capable devices, and uses the MAC address of the devices as the username and password, when communicating with the RADIUS servers. MAC addresses for username and password must be entered in lower case and with no delimiting characters (for example: aaccbb55ccff). To use MAC-based authentication at a port:
  - A Guest VLAN must be defined.
  - The port must be Guest-VLAN-enabled.
  - The packets from the first supplicant, at the port before it is authorized, must be untagged.

You can configure a port to use Dot1x only, MAC-based only, or Dot1x and MAC-based authentication. If a port is configured to use both Dot1x and MAC-based authentication, a Dot1x supplicant has precedence over a non-Dot1x device. The Dot1x supplicant preempts an authorized, but non-Dot1x device, at a port that is configured with a single session.

Unauthenticated VLAN and Guest VLANs

Unauthenticated VLANs and Guest VLANs provide access to services that do not require the subscribing devices or ports to be Dot1x or MAC-Based authenticated and authorized.

An unauthenticated VLAN is a VLAN that allows access by authorized and unauthorized devices or ports. You can configure one or more VLAN to be unauthenticated in the **VLAN Membership** pages in VLANs.

An unauthenticated VLAN has the following characteristics:

- It must be a static VLAN, and cannot be the Guest VLAN or the default VLAN.
- The VLAN's member ports must be manually configured as tagged members.
- The member ports must be trunk and/or general ports. An access port cannot be member of an unauthenticated VLAN.

The Guest VLAN, if configured, is a static VLAN with the following characteristics.

- It must be manually defined from an existing, static VLAN.

- It is automatically available only to unauthorized devices, or to ports of devices that are connected and Guest VLAN enabled.
- If a port is Guest-VLAN-enabled, the switch automatically adds the port as an untagged member of the Guest VLAN when the port is not authorized, and removes the port from the Guest VLAN when the first supplicant of the port is authorized.
- The Guest VLAN cannot be used as both the Voice VLAN and an unauthenticated VLAN.

The switch also uses the Guest VLAN for authentication at ports configured with Multiple Session mode and MAC-based authentication. Therefore, you must configure a Guest VLAN before you can use the MAC-based authentication mode.

For authentication to function, it must be activated both globally, in the **Port-Based Authentication Global** page and individually on each port, in the **Port-Based Authentication Interface Settings** pages.

Port-Based Authentication Global

To globally configure authentication:

1. Click **Switching** > **Network Security** > **Dot1x Authentication** > **Port Based Authentication Global** to display the **Port Based Authentication Global** page.
2. Enter the following fields:
   - **Port Based Authentication State** — Enable/disable port-based authentication.
   - **Authentication Method** — Select an authentication method. The possible options are:
     - **RADIUS, None** — Perform port authentication first by using the RADIUS server. If no response is received from RADIUS (for example, if the server is down), then no authentication is performed, and the session is permitted.
     - **RADIUS** — Authenticate the user on the RADIUS server. If no authentication is performed, the session is not permitted.
     - **None** — Do not authenticate the user. Permit the session.

- **Guest VLAN** — Enable/disable the use of a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, all unauthorized ports automatically join the VLAN selected in the Guest VLAN ID field. If a port is later authorized, it is removed from the Guest VLAN.
- **VLAN List** — Select the Guest VLAN from the VLAN list.
- **Accept Supplicant when Dynamic Policy/ACL Assignment Has No Resources** — If no resources remain in the TCAM, the system can either reject (disable) or allow (enable) successful authentication.

Enabling Port-Based Authentication Globally Using the CLI Commands

The following table summarizes the CLI commands for enabling the port based authentication as displayed in the **Port Based Authentication Global** page.

Table 9-12. Port-Based Authentication Global CLI Commands

CLI Command	Description

`aaa authentication dot1x default {radius | none | {radius | none}}`
`no aaa authentication dot1x default`
	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
	Use the no form of this command to restore the default configuration.

`dot1x system-auth-control`
`no dot1x system-auth-control`
	Enables 802.1x globally.
	Use the no form of this command to restore the default configuration.

`dot1x guest-vlan`
`no dot1x guest-vlan`
	Contains a list of VLANs. The guest VLAN is selected from the **VLAN List.**
	Use the no form of this command to disable access.

`show dot1x [interface` *`interface-id`* **`| detailed]`**	Displays 802.1X status for the device.

The following is an example of the CLI commands:

```
console(config)# aaa authentication dot1x default none
console(config)# interface vlan 5
console# show dot1x
802.1x is disabled
         Admin              Oper          Reauth   Reauth      Username
Port     Mode               Mode          Control  Period
-------- ----------------- ------------ -------- -------     --------
gi0/1  Force Authorized   Authorized*   Disabled   3600          n/a
gi0/2  Force Authorized   Authorized*   Disabled   3600          n/a
gi0/3  Force Authorized   Authorized*   Disabled   3600          n/a
gi0/4  Force Authorized   Authorized*   Disabled   3600          n/a
```

Port-Based Authentication Interface Settings

To configure 802.1x authentication on an interface:

1 Click **Switching > Network Security > Dot1 Authentication > Port Based Authentication Interface Settings** to display the **Port Based Authentication Interface Settings: Summary** page.

   Port parameters for the selected device are displayed.

2 Click **Edit**.

3 Select a port for which the authentication parameters apply in the **Interface** drop-down list.

4 Enter the parameters:

   – **User Name** — Displays the username of the port.

   – **Admin Interface Control** — Select the port authorization state. The possible options are:

     - **Auto** — Enables port-based authentication on the interface. The interface moves between an authorized or unauthorized state, based on the authentication exchange between the device and the client.

     - **Authorized** — Places the interface into an authorized state without being authenticated. The interface resends and receives normal traffic without client port-based authentication.

    - **Unauthorized** — Denies the selected interface system access by moving the interface into unauthorized state. The device cannot provide authentication services to the client through the interface.
- **Current Interface Control** — Displays the current port authorization state.
- **Authentication Type** — Select the type of authentication on the port. The possible options are:
    - **802.1x Only** — 802.1X authentication is the only authentication method performed on the port.
    - **MAC Only** — Port is authenticated, based on the supplicant MAC address. Only eight MAC-based authentications can be used on the port.
    - **802.1x & MAC** — Both 802.1X and MAC-based authentication are performed on the switch. The 802.1X authentication takes precedence.

NOTE: For MAC authentication to succeed, the RADIUS server supplicant username and password must be the supplicant MAC address. The MAC address must be in lower case letters and entered without the ":" or "-" separators; for example: 0020aa00bbcc.

- **Dynamic VLAN Assignment** — Enable/disable dynamic VLAN assignment for this port. This feature enables you to automatically assign users to VLANs during the RADIUS server authentication. When a user is authenticated by the RADIUS server, the user is automatically joined to the VLAN configured on a RADIUS server.
    - Port Lock and Port Monitor should be disabled when DVA is enabled.
    - Dynamic VLAN Assignment (DVA) can occur only if a RADIUS server is configured, and port authentication is enabled and set to 802.1x multi-session mode.
    - If the RADIUS Accept Message does not contain the supplicant's VLAN, the supplicant is rejected.
    - Authenticated ports are added to the supplicant VLAN as untagged.

- Authenticated ports remain unauthenticated VLAN and Guest VLAN members. Static VLAN configuration is not applied to the port.
- The following list of VLANs cannot participate in DVA: an Unauthenticated VLAN, a Dynamic VLAN that was created by GVRP, a Voice VLAN, a Default VLAN and a Guest VLAN.
- Delete the supplicant VLAN while the supplicant is logged in. The supplicant is authorized during the next re-authentication if this supplicant VLAN is re-created, or a new VLAN is configured on the RADIUS server.

NOTE: DVA provides the same functionality as the MAC to VLAN Assignment feature, but does so in a standard way. Therefore, when DVA is available, MAC to VLAN Assignment is not available.

- **Guest VLAN** — Enable/disable port access to the Guest VLAN. If enabled, unauthorized users, connected to this interface, can access the Guest VLAN.
- **Dynamic Policy / ACL Assignment** — Enable/disable this feature.
- **Periodic Reauthentication** — Select to enable port re-authentication attempts after the specified Reauthentication Period.
- **Reauthentication Period** (300-4294967295) — Enter the number of seconds after which the selected port is reauthenticated.
- **Reauthenticate Now** — Select to enable immediate port re-authentication.
- **Authentication Server Timeout** (1-65535) — Enter the time interval that lapses before the device resends a request to the authentication server. The field value is specified in seconds.
- **Resending EAP Identity Request** (1-65535) — Enter the amount of time that lapses before EAP request are resent.
- **Quiet Period** (10-65535) — Enter the number of seconds that the device remains in the quiet state, following a failed authentication exchange.
- **Supplicant Timeout** (1-65535) — Enter the amount of time that lapses before EAP requests are resent to the supplicant. The field value is in seconds.

- **Max EAP Requests (1-10)** — Enter the maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.

Enabling Port-Based Authentication on Interfaces Using the CLI Commands

The following table summarizes the CLI commands for enabling the port based authentication as displayed in the **Port Based Authentication Global** page.

Table 9-13. Port-Based Authentication Interface CLI Commands

CLI Command	Description
dot1x port-control {*auto* | *force-authorized* | *force-unauthorized*} **no dot1x port-control**	Enables manual control of the port authorization state. Use the no form of this command to restore the default configuration.
dot1x mac-authentication {*mac-only* | *mac-and-802.1x*} **no dot1x mac-authentication**	Enables authentication based on the station's MAC address. Use the no form of this command to disable access.
dot1x radius-attributes vlan [reject | *vlan-id***]** **no dot1x radius-attributes vlan**	Enables user-based VLAN assignment. Use the no form of this command to disable user-based VLAN assignment.
dot1x guest-vlan enable **no dot1x guest-vlan enable**	Enables unauthorized users on the interface access to the guest VLAN. Use the no form of this command to disable access.
dot1x max-req *count* **no dot1x max-req**	Sets the maximum number of times that the device sends an EAP to the client, before restarting the authentication process. Use the no form of this command to restore the default configuration.

Table 9-13. Port-Based Authentication Interface CLI Commands *(continued)*

CLI Command	Description
dot1x re-authentication **no dot1x re-authentication**	Enables periodic re-authentication of the client. Use the no form of this command to return to the default setting.
dot1x timeout re-auth-period *seconds* **no dot1x timeout reauth-period**	Sets the number of seconds between re-authentication attempts. Use the no form of this command to restore the default configuration.
dot1x re-authenticate [*interface-id***]**	Manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.
dot1x timeout quiet-period *seconds* **no dot1x timeout quiet-period**	Sets the number of seconds that the device remains in the quiet state following a failed authentication exchange. Use the no form of this command to restore the default configuration.
dot1x timeout server-timeout *seconds* **no dot1x timeout server-timeout**	Sets the time for the retransmission of packets to the authentication server. Use the no form of this command to restore the default configuration.
dot1x timeout supp-timeout *seconds* **no dot1x timeout supp-timeout**	Sets the time for the retransmission of an EAP request frame to the client. Use the no form of this command to restore the default configuration.
dot1x timeout tx-period *seconds* **no dot1x timeout tx-period**	Sets the number of seconds that the device waits for a response to an EAP -request/identity frame, from the client, before resending the request. Use the no form of this command to restore the default configuration.
show dot1x [**interface** *interface-id* | **detailed**]	Displays 802.1X status for the device or for the specified interface.

Table 9-13. Port-Based Authentication Interface CLI Commands *(continued)*

CLI Command	Description
show dot1x advanced [**interface** *interface-id* | **detailed**]	Displays 802.1X advanced features for the switch or specified interface.
show dot1x users [**username** *username*]	Displays 802.1X users for the device.
dot1x guest-vlan enable **no dot1x guest-vlan enable**	Enables using a guest VLAN for unauthorized ports. Use the no form of this command to restore the default configuration.

The following is an example of the CLI commands:

```
console(config)# aaa authentication dot1x default none
console(config)# interface vlan 5
console(config-if)# dot1x auth-not-req
console(config)# vlan database
console(config-vlan)# vlan 2
console(config-vlan)# exit
console(config)# interface vlan 2
console(config-if)# dot1x guest-vlan
console# show dot1x

Interface  Admin    Oper Mode   Reauth   Reauth  Username
           Mode                 Control  Period
--------   -------  ----------  -------- ------  --------
gi0/1      Auto     Authorized  Enabled  3600    Bob
gi0/2      Auto     Authorized  Enabled  3600    John
gi0/3      Auto     Unauthoriz  Enabled  3600    Clark
                    ed
gi0/4      Force-   Authorized  Disabled 3600    n/a
           auth
```

Host Authentication

Use the **Host Authentication** page to define the authentication mode on the port, and the action to perform if a violation is detected.

To view ports and their authentication information:

1. Click **Switching > Network Security > Dot1 Authentication > Host Authentication** to display the **Host Authentication: Summary** page.

   A list of the ports and their authentication modes is displayed. The fields are defined on the **Edit** page with the exception of the following field:

   – **Single Host Status** — Displays the host status. The possible options are:

     - **Unauthorized** — The port control is **Force Unauthorized**, the port link is down or the port control is **Auto**, but a client has not been authenticated via the port.
     - Not in Auto Mode — The port control is **Forced Authorized**, and clients have full port access.
     - Single-host Lock — The port control is **Auto** and a single client has been authenticated via the port.
     - **No Single Host** — Multiple Host is enabled.

   – **Number of Violations** — Displays the number of packets that arrive on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.

2. Click **Edit**.
3. In the **Port** drop-down list, select the port to which you want to apply the authentication mode.
4. Enter the fields:

   – **Host Authentication** — Define the host authentication type. The options are:

     - **Single** — Only a single authorized host can access the port. (Port Security cannot be enabled on a port in single-host mode.)

  - **Multiple Host** — Multiple hosts can be attached to a single 802.1x-enabled port. Only the first host must be authorized, and then the port is wide-open for all who want to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
  - **Multiple Session** — A number of specific authorized hosts may access the port. Each host is treated as if it was the first and only user and must be authenticated. Filtering is based on the source MAC address.
- **Action on Single Host Violation** — Select the action to be applied to packets arriving in Single Session/Single Host mode, from a host whose MAC address is not the supplicant MAC address. The options are:
  - **Discard** — Discard the packets from any unlearned source.
  - **Forward** — Forward the packets from an unknown source, however, the MAC address is not learned.
  - **Shutdown** — Discard the packet from any unlearned source and shut down the port. Ports remain shutdown until they are activated, or the switch is reset.

Configuring Host Authentication Using the CLI Commands:

The following table summarizes the CLI commands for configuring host authentication:

Table 9-14. Host Authentication CLI Commands

CLI Command	Description
dot1x host-mode {*multi-host* | *single-host* | *multi-sessions*}	Allows a single host (client) or multiple hosts on an IEEE 802.1x-authorized port.
dot1x traps mac-authentication failure **no dot1x traps mac-authentication failure**	Enables sending traps when a MAC address is successfully authenticated by the 802.1X mac-authentication access control. Use the no form of this command to disable the traps.

Table 9-14. Host Authentication CLI Commands *(continued)*

CLI Command	Description
dot1x traps mac-authentication success **no dot1x traps mac-authentication success**	Enables sending traps when MAC address was failed in authentication of the 802.1X MAC authentication access control. Use the no form of this command to disable the traps.
dot1x violation-mode {*restrict* | *protect* | *shutdown*} **no dot1x violation-mode**	Configures the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. Use the no form of this command to return to default.
show dot1x advanced [*interface-id* | ***detailed***]	Displays 802.1x advanced features for the device or specified interface.

The following is an example of the CLI commands:

```
console(config)# interface gi0/1
console(config-if)# dot1x host-mode multi-host
console(config-if)# dot1x host-mode single-host
console(config-if)# dot1x host-mode multi-sessions
```

Port Authentication Users

The **Port Authentication Users** page enables you to view users that attempted to be authenticated.

To view ports and their authentication definitions:

1 Click **Switching > Network Security > Dot1 Authentication > Port Authentication Users** to display the **Port Authentication Users** page.

The ports and their authentication definitions are displayed.

- **User Name** — Supplicant names that were authenticated on each port.
- **Port** — Number of port.

- **Session Time** — Amount of time (in seconds) that the supplicant was logged on the port.
- **Authentication Method** — Method by which the last session was authenticated. The options are:
  - **None**—No authentication is applied; it is automatically authorized.
  - **RADIUS**—Supplicant was authenticated by a RADIUS server.
  - **MAC Address**—Displays the supplicant MAC address.
- **MAC Address** — MAC address of user who attempted to be authenticated.
- **VLAN** — VLAN assigned to the user.
- **Filter** — Filter that was applied to the user by receiving the policy/ACL name from the RADIUS server (Dynamic ACL Assignment).

2 Click **Details** to view the names of the VLAN filters (**Filter #1** and **Filter #2**) defined on the port, in addition to the above fields.

Display Port Authentication Users Using the CLI Commands

The following table summarizes the CLI commands for displaying port authentication users:

Table 9-15. Display Port Authentication Users CLI Commands

CLI Command	Description
show dot1x users [username *username*]	Displays active 802.1x authenticated users for the device.

The following is an example of the CLI commands:

```
console# show dot1x users
Port    User Session      Auth    MAC              VLAN Filter
        Name Time         Method  Address
------ ----- ----------- -------- -------------    ---- ------
gi0/1   Bob  1d 03:08:58  Remote  0008.3b79.8787     3
Port    User Session      Auth    MAC              VLAN Filter
        Name Time         Method  Address
------ ----- ----------- -------- -------------    ---- ------
gi0/1   Bob  1d 09:07:38 Remote  0008.3b79.8787     3    OK
gi0/1   Tim  03:08:58    Remote  0008.3b79.3232     9    OK
gi0/3   Paul 02:12:48    Remote  0008.3b89.8237     8    Warning
console# show dot1x users username Bob
Port    User Session      Auth    MAC              VLAN Filter
        Name Time         Method  Address
------ ----- ----------- -------- -------------    ---- ------
gi0/1   Bob  1d 09:07:38  Remote  0008.3b79.8787    3   OK
```

10

Ports

This section describes how to configure port functionality.

It contains the following topics:

- Overview
- Jumbo Frames
- Green Ethernet Configuration
- Protected Ports
- Port Profile
- Port Configuration
- LAG Configuration
- Storm Control
- Port and VLAN Mirroring

Overview

This section includes a description of port features and describes the following:

- Auto-Negotiation
- MDI/MDIX
- Flow Control
- Back Pressure
- Port Default Settings

The device supports 802.3x flow control for ports configured to Full Duplex mode. By default, this feature is enabled on all ports, and it can be disabled per port.

The device supports back pressure for ports configured to Half Duplex mode. By default, this feature is disabled, and it can be enabled per port. The back-pressure mechanism prevents the sender from transmitting additional traffic temporarily. The receiver may occupy a link so it becomes unavailable for additional traffic.

Port default settings are described in Table 10-1.

Auto-Negotiation

Auto-negotiation enables automatic detection of speed, duplex mode and flow control on all switching 10/100/1000BaseT ports. Auto-negotiation is enabled on all ports by default.

Auto-negotiation is a mechanism established between two link partners to enable a port to advertise its transmission rate, duplex mode and flow control abilities to its partner. Both ports then operate at the highest common denominator.

If connecting a Network Interface Card (NIC) that does not support auto-negotiation or is not set to auto-negotiation, both the device switching port and the NIC must be manually set to the same speed and duplex mode.

If the station, on the other side of the link, attempts to auto-negotiate with a device 100BaseT port that is configured to full duplex, the auto-negotiation results in the station attempting to operate in half duplex.

MDI/MDIX

The device supports auto-detection of straight-through and crossed cables on all 10/100/1000BaseT ports. This feature is part of auto-negotiation and is enabled when Auto-negotiation is enabled.

When the MDI/MDIX (Media Dependent Interface with Crossover) is enabled, the automatic correction of errors in cable selection is possible, thus making the distinction between a straight-through cable and a crossover cable irrelevant. The standard wiring for end stations is known as MDI (Media Dependent Interface), and the standard wiring for hubs and switches is known as MDIX.

Flow Control

The device supports 802.3x flow control for ports configured to Full Duplex mode. By default, this feature is enabled on all ports, and it can be disabled per port.

Flow control creates a lossless link with no packet loss. The flow control mechanism enables the receiving side to signal to the transmitting side that transmission must temporarily be halted to prevent buffer overflow. This signaling is done by sending PAUSE frames. The ports that receives pause frames stops transmitting traffic.

Flow control on the device works in Receive-Only mode, meaning that the interfaces with enabled flow control receive PAUSE frames, but do not send them.

When flow control is enabled, the system buffers are allocated per port so that if the buffers of one port are consumed, other ports will still have their free buffers.

Back Pressure

The device supports back pressure for ports configured to Half Duplex mode. By default, this feature is disabled, and it can be enabled per port. The back-pressure mechanism prevents the sender from transmitting additional traffic temporarily. The receiver may occupy a link so it becomes unavailable for additional traffic.

Port Default Settings

Table 10-1 describes the port default settings.

Table 10-1. Port Default Settings

Function	Default Setting
Port speed and mode	10/100/1000 BaseT copper: auto-negotiation SFP+1000/10G Mbps full duplex, auto discovery
Port forwarding state	Enabled

Table 10-1. Port Default Settings *(continued)*

Function	Default Setting
Port tagging	No tagging
Flow Control	On
Back Pressure	Off

Jumbo Frames

Jumbo frames are frames of up to 10 Kb in size. If Jumbo frames are not enabled, the system supports a packet size of up to 1,632 bytes.

To enable jumbo frames:

1. Click **Switching** > **Ports** > **Jumbo Frames** in the tree view to display the **Jumbo Frames** page.

   The current jumbo frames setting is displayed.

2. Enable/disable jumbo frames in the **New Setting (after reset)** field.

NOTE: You must save the configuration and reboot the device in order to make jumbo frames operational.

Configuring Jumbo Frames Using CLI Commands

The following table summarizes the CLI commands for configuring Jumbo frames.

Table 10-2. Jumbo Frames CLI Commands

CLI Command	Description
`port jumbo-frame`	Enables jumbo frames on the device.
`no port jumbo-frame`	Use the no form of this command to disable jumbo frames.

The following is an example of the CLI commands:

```
console(config)# port jumbo-frame
```

Green Ethernet Configuration

Green Ethernet is a name of a set of features that are designed to reduce the power consumption of a device, and so make it environmentally friendly.

The Green Ethernet feature reduces overall power usage in the following ways:

- **Energy Efficient Ethernet** — When using EEE, systems on both sides of the link can disable portions of their functionality and save power during periods of low link utilization. EEE is a hardware feature that is enabled by default, and is transparent to users. This feature is defined per port, regardless of their LAG membership.
- **Link Short-Reach Energy Saving Mode** — Power usage is adjusted to the actual cable length. In this mode, the VCT (Virtual Cable Tester) length test is performed to measure cable length. If the cable is shorter than a predetermined length, the switch reduces the power used to send frames over the cable, thus saving energy. This mode is only supported on RJ45 ports.
- **Energy Detect Mode** — Power savings and current power consumption in Short Reach mode can be monitored. The total amount of saved energy can be viewed as a percentage of the power that would have been consumed by the physical interfaces had they not been running in Green Ethernet mode.

The above two energy saving modes must be enabled globally and then configured per port.

Green Ethernet Configuration

To configure Green Ethernet settings:

1. Click **Switching > Ports > Green Ethernet Configuration** in the tree view to display the **Green Ethernet Configuration: Summary** page.
2. The amount of energy saved from the last switch reboot is displayed in the **Cumulative Energy Saved** field. This value is updated each time there is an event that affects power saving. Click **Reset** to reset its value.
3. Enter the fields:
   - **Energy Efficient Ethernet** — Globally enable/disable the Energy Efficient Ethernet feature.

- **Link Short-Reach Energy Saving Mode** — Globally enable/disable Short Reach mode.
- **Energy Detect Mode** — Globally enable/disable the Energy Detect mode.
- **Current Power Consumption** — Displays the current power consumption.
- **Power Savings** — Displays the percentage of power saved by running in Green Ethernet mode.

4 Click **LLDP Interface Details**.

5 The following is displayed for each port on the device:

– **Port** — Port number.

- **Energy Efficient Ethernet**.
  - **Oper** — Displays the operational status of EEE mode.
  - **Remote Peer**— Displays the operational status of Green Ethernet on the other side of the link.
- **Short-Reach**.
  - **Oper** — Displays the operational status of Short-Reach mode.
  - **Fault Reason**— Reason if the operational mode is different than the administrative mode.
- **Energy Detect**.
  - **Oper** — Displays the operational status of Short-Reach mode.
  - **Fault Reason**— Reason if the operational mode is different than the administrative mode.

– **Cable Length (Meter)** — Indicates the length of the cable.

Configuring Green Ethernet Using CLI Commands

The following table summarizes the CLI commands for configuring Green Ethernet.

Table 10-3. Green Ethernet CLI Commands

CLI Command	Description

`green-ethernet short-reach`
`no green-ethernet short-reach`
	Enables/disables Green Ethernet short reach mode.

Table 10-3. Green Ethernet CLI Commands *(continued)*

CLI Command	Description
green-ethernet short-reach force	Forces short-reach mode on an interface.
no green-ethernet short-reach force	Use the no form of this command to return to the default.
green-ethernet short-reach threshold *cable-length*	Set the maximum cable length for applying short-reach mode.
no green-ethernet short-reach threshold	Use the no form of this command to return to the default.
green-ethernet power-meter reset	Resets the power save meter.
eee enable **no eee enable**	Enables the EEE mode globally. Can be used globally or per interface. Use the no format of the command to disable the mode.
eee lldp enable **no eee lldp enable**	Enables EEE support by LLDP on an Ethernet port. Use the no format of the command to disable the support.
show eee [*interface-id]*	Displays EEE information.

Protected Ports

Overview

Protected ports provide Layer 2 isolation between interfaces (Ethernet ports and LAGs) that share the same Broadcast domain (VLAN) with other interfaces. This can be used to set up a group of ports that receive similar services.

A protected port does not forward traffic (Unicast, Multicast, or Broadcast) to any other protected port on the same switch.

A community is a group of protected ports. Protected ports within the same community can forward traffic to each other.

The following types of ports can be defined:

- **Protected Port** — Can send traffic only to uplink ports.
- **Community Port** — A protected port that is associated with a community. It can send traffic to other protected ports in the same community and to uplink ports.
- **Uplink Port** — An uplink port is an unprotected port that can send traffic to any port.
- **Isolated Port** — A protected port that does not belong to a community.

Port Protection is independent of all other features and configuration settings. Two protected ports in a common VLAN cannot communicate with each other.

Protected Port Restrictions

The following restrictions apply to protected ports:

- When a protected port is placed in a LAG, it loses its protected port attribute and takes upon itself the LAG's protection attributes. When the port is removed from the LAG, its attributes are re-applied.
- Mirrored traffic is not subject to protected ports rules.
- Routing is not affected by the protected port forwarding rule, so that if a packet enters a protected port, it can be routed by the device to another protected port.

Protected Ports

To configure protected ports and establish their communities:

1. Click **Switching** > **Ports** > **Protected Ports** in the tree view to display the **Protected Ports: Summary** page.

   A summary of all the ports and their statuses is displayed.

2. Click **Edit**.
3. Select the interface.
4. Enter values for the following fields:

   - **State** — Select **Protected/Unprotected** to enable/disable port protection.

- **Community** — Select the community to which to add the port, or define the port as **Isolated**.

Configuring Protected Ports Using CLI Commands

The following table summarizes the CLI commands for configuring protected ports.

Table 10-4. Protected Ports CLI Commands

CLI Command	Description
switchport protected-port **no switchport protected-port**	Isolates Unicast, Multicast, and Broadcast traffic on a port at Layer 2 from other protected ports on the same switch. Use the no form of this command to disable protection on the port.
switchport community *community*	Associates a protected port with a community
no switchport community	Use the no form of this command to return to default.
show interfaces protected-ports [*interface-id* | ***detailed*****]**	Displays protected ports configuration.

The following is an example of the CLI commands:

```
console(config)# interface gi0/3
console(config-if)# switchport protected-port
console(config-if)# switchport community 1
```

Port Profile

Port profiles provide a convenient way to save and share a port configuration. When a port profile, which is a set of CLI commands having a unique name, is applied to a port, the CLI commands contained within the profile (macro) are executed and added to the Running Configuration file.

Port profiles can be applied to a specific interface, a range of interfaces, or globally.

There are two types of port profiles:

- **User Defined** — Enables the user to bundle configurations, as a port profile, and then apply it to one or more interfaces at a time. Up to 20 user-defined macros can be supported. These can only be defined through CLI commands.
- **Built-In** — Pre-defined macros that cannot be changed or deleted. The device includes the following built-in macros:
  - Global
  - Desktop
  - Phone
  - Switch
  - Router
  - Wireless Configuration

Before a built-in profile can be applied to an interface, the global profile must be applied. The global profile enables QoS Advanced mode, sets Advanced mode parameters, CoS to queue mapping, and DSCP to queue mapping and defines certain standard ACLs. Use the CLI command **show parser macro name profile-global** to display the Global profile contents.

To assign a profile to a port:

1. Click **Switching > Ports > Port Profile** in the tree view to display the **Port Profiles: Summary** page.

   A summary of all the interfaces and their profiles is displayed.

2. To assign the **Global** profile to the system, check **Run Global Profile**. Apply the global profile before applying a built-in interface profile.
3. To assign a profile to an interface, click **Edit**.

4. Select an interface and a **Assigned Profile**. The **Profile Description** is displayed.
5. Each profile requires entering various elements of VLAN information. Enter the fields according to the profile:
   - **VLAN Port Mode** — Displays the port mode applied to ports in the profile.
   - **VLAN ID-Untagged (1-4094)** — Enter the VLAN for untagged traffic.
   - **VLAN ID-Tagged (1-4095)** — Enter the VLAN for tagged traffic.
   - **Native VLAN ID(1-4094)** — Enter the VLAN ID used for untagged traffic to trunk ports, or check **None**.

   The remaining fields on this page are display-only, and describe the port configuration of the profile. The following fields are described:

   Port Security fields:

   - **Mode** — Learning mode. The possible options are:
     - **Classic Lock** — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
     - **Limited Dynamic Lock** — Locks the port by deleting the dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.
   - **Max Entries** — Displays the maximum number of MAC addresses that can be learned on the port.
   - **Action on Violation** — Action to be applied to packets arriving on a locked port. The possible options are:
     - **Discard** — Discard the packets from any unlearned source.
     - **Forward** — Forward the packets from an unknown source, without learning the MAC address.
     - **Shutdown** — Discard the packet from any unlearned source, and shut down the port. Ports remain shutdown until they are reactivated, or the device is reset.

Spanning Tree fields:

- **Point-to-Point Admin Status** — Displays whether a point-to-point links is established. The possible options are:
  - **Enable** — Enables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link. To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual switch port link type. It may differ from the administrative state.
  - **Disable** — Disables point-to-point link.
  - **Auto** — The device automatically establishes a point-to-point link.
- **Fast Link** — Displays whether Fast Link mode is enabled for the port. If this is enabled, the **Port State** is automatically placed in the **Forwarding** state when the port is up.
- **BPDU Guard** — Displays whether BPDU Guard is enabled on the port.

Miscellaneous fields:

- **Policy Name** — Displays the name of a policy if one is defined on the port.
- **Auto Negotiation** — Displays whether auto-negotiation is enabled on the port. Auto-Negotiation enables a port to advertise its transmission rate, duplex mode, and Flow Control abilities to other devices.

6 Click **Apply Profile** to apply the profile to the specified interface.

Configuring Port Profile Using CLI Commands

The following table summarizes the CLI commands for configuring port profiles.

Table 10-5. Port Profiles CLI Commands

CLI Command	Description
macro {***apply***|***trace***} *macro-name* [*parameter-name1* {*value*}] [*parameter-name2* {*value*}] [*parameter-name3* {*value*}]	Applies a macro to an interface or traces a macro configuration on an interface.
show parser macro [{***brief***|***description*** [***interface*** *interface-id* | **detailed**]| ***name*** *macro-name*}]	Displays the parameters for all configured macros or for one macro on the switch.

The following is an example of the CLI commands:

```
Switch(config) # interface gi0/2
Switch(config-if) # macro trace dup
Applying command… ‘duplex full’
Applying command… ‘speed auto’
Switch(config) # interface gi0/2
Switch(config-if) # macro apply duplex $DUPLEX full
$SPEED auto
Switch(config-if) # exit
Switch(config) # interface gi0/3
Switch(config-if) # macro apply dup
Switch(config-if) # exit
```

Sample CLI Scripts

This section provides sample scripts of CLI commands. These particular actions cannot be performed through the GUI, which only allows applying built-in macros. These scripts describe how to create macros, display them and apply them.

The following is a script that creates a global macro.

Table 10-6. Create a Global Macro Script

CLI Command	Description

`console#config`
`console(config)#` **`macro name`** `interswitch`
`Enter macro commands one per line. End with the character '@'.`
	Create a macro called **interswitch**.

`vlan database`
`vlan 40-50`
`@`
	Enter the commands in the macro, which create VLANs 40 through 50.

`console(config)#` **`do show parser macro name`** `interswitch`	Display the macro.
`console(config)#` **`macro global apply`** `interswitch`	Apply the macro.

The following is a script that creates an interface macro

Table 10-7. Create an Interface Macro Script

CLI Command	Description

`console#`**`config`**
`console(config)#` **`interface range gi0/1-24`**
	Enter Interface mode for ports 1-24.

`console(config-if-range)#` **`macro name`** `access_port`
`Enter macro commands one per line. End with the character '@'.`
	Create a macro called **access_port**.

`disable spanning-tree`
`@`
	Enter the commands in the macro, disables spanning tree on the interfaces.

`console(config)#` **`do show parser macro name`** `access_port`	Display the macro.

Table 10-7. Create an Interface Macro Script *(continued)*

CLI Command	Description
`console(config)# macro global apply access_port`	Apply the macro to ports 1-24.

Port Configuration

If port configuration is modified while the port is a LAG member, the configuration change is only effective after the port is removed from the LAG.

To configure a port:

1. Click **Switching** > **Ports** > **Port Configuration** in the tree view to display the **Port Configuration: Summary** page.

   All ports and their configuration settings are displayed.

2. To modify the port settings, click **Edit** and select a port.

3. Enter the following fields:

   – **Description (1 - 64 Characters)** — Enter a user identification attached to the port.

   – **Physical Port Type** — Displays the type of port.

   – **Admin Status** — Enable/disable traffic forwarding through the port.

     - **Up** — Traffic is enabled through the port.
     - **Down** — Traffic is disabled through the port.

   – **Current Port Status** — Displays whether the port is currently operational or non-operational.

   – **Re-Activate Suspended Port** — Check to reactivate a port if the port has been disabled through the locked port security option.

   – **Operational Status** — Displays the port operational status. The possible options are:

     - **Suspended** — Port is currently active, and is not receiving or transmitting traffic.
     - **Active** — Port is currently active, and is receiving and transmitting traffic.

  - **Disable** — Port is currently disabled, and is not receiving or transmitting traffic.

- **Admin Speed** — Select the configured rate for the port. The port type determines the available speed setting options. You can designate Administrative Speed only when port auto-negotiation is disabled.
- **Current Port Speed** — Displays the actual synchronized port speed (bps).
- **Admin Duplex** — Select the port duplex mode (this is only possible if Auto Negotiation is not enabled). The options are:
  - **Full** — The interface supports transmission between the device and the client in both directions simultaneously.
  - **Half** — The interface supports transmission between the device and the client in only one direction at a time.
- **Current Duplex Mode** — Displays the synchronized port duplex mode.
- **Auto Negotiation** — Select to enable auto-negotiation on the port. Auto-Negotiation enables a port to advertise its transmission rate, duplex mode, and Flow Control abilities to other devices.
- **Energy Efficient Ethernet** — Globally enable/disable Energy Efficient Ethernet and the EEE LLDP advertisement feature.
- **Short Reach Energy Saving** —TBD Globally enable/disable Short Reach Energy Saving feature.
- **Current Auto Negotiation** — Displays the current auto-negotiation setting.
- **Admin Advertisement** — Check the auto-negotiation setting the port advertises. The possible options are:
  - **Max Capability** — The port advertises all the options that it can support.
  - **10 Half** — The port advertises for a 10 mbps speed port and half duplex mode setting.
  - **10 Full** — The port advertises for a 10 mbps speed port and full duplex mode setting.
  - **100 Half** — The port advertises for a 100 mbps speed port and half duplex mode setting.

  - **100 Full** — The port advertises for a 100 mbps speed port and full duplex mode setting.
  - **1000 Full** — The port advertises for a 1000 mbps speed port and full duplex mode setting.
- **Current Advertisement** — Displays the port advertises its speed to its neighbor port to start the negotiation process. The possible field values are those specified in the **Admin Advertisement** field.
- **Neighbor Advertisement** — Displays the neighboring port's advertisement settings. The field values are identical to the **Admin Advertisement** field values.
- **Back Pressure** — Enable/disable Back Pressure mode that is used with Half Duplex mode to disable ports from receiving messages.
- **Current Back Pressure** — Displays the current Back Pressure setting.
- **Flow Control** — Set flow control on the port. The following options are available:
  - **Enable/Disable** — Enable/disable flow control on the port (Enabled is the default).
  - **Auto Negotiation** — Enables auto-negotiation of flow control on the port.
- **Current Flow Control** — Displays the current Flow Control setting.
- **MDI/MDIX** — Select one of the options that enables the device to decipher between crossed and uncrossed cables. Hubs and switches are deliberately wired opposite to the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are match up properly. When two hubs/switches are connected to each other, or two end stations are connected to each other, a crossover cable is used ensure that the correct pairs are connected. The possible options are:
  - **Auto** — Use to automatically detect the cable type.
  - **MDIX** — Use for hubs and switches.
  - **MDI** — Use for end stations.
- **Current MDI/MDIX** — Displays the current device MDIX settings.
- **LAG** — Displays whether the port is part of a LAG.

Configuring Ports Using CLI Commands

The following table summarizes the CLI commands for configuring ports as displayed in the **Port Configuration** pages.

Table 10-8. Port Configuration CLI Commands

CLI Command	Description
eee enable **no eee enable**	Enables the EEE mode globally. Use the no format of the command to disable the mode.
eee lldp enable **no eee lldp enable**	Enables EEE support by LLDP on an Ethernet port. Use the no format of the command to disable the support.
description *string* **no description**	Adds a description to an interface configuration. Use the no form of this command to remove the description.
shutdown **no shutdown**	Disables an interfaces. Use the no form of this command to restart a disabled interface.
set interface active {*interface-id*}	Reactivates an interface that is shutdown.
speed {*10*|*100*|*1000*|} **no speed**	Configures the speed of a given Ethernet interface when not using auto negotiation. Use the no form of this command to restore the default configuration.
duplex {*half*|*full*} **no duplex**	Configures the full/half duplex operation of a given Ethernet interface when not using auto negotiation.
negotiation [*capability* [*capability2…capability5*] **no negotiation**	Enables auto negotiation operation for the speed and duplex parameters of a given interface. Use the no form of this command to disable auto-negotiation.

Table 10-8. Port Configuration CLI Commands *(continued)*

CLI Command	Description
back-pressure **no back-pressure**	Enables Back Pressure on a given interface. Use the no form of this command to disable back pressure.
flowcontrol {*auto*|*on*|*off*} **no flowcontrol**	Configures the flow control on a given interface. Use the no form of this command to disable flow control.
mdix {*on*|*auto*} **no mdix**	Enables automatic crossover on a given interface or Port-channel. Use the no form of this command to disable cable crossover.
show interfaces configuration [*interface-id* | ***detailed***]	Displays the configuration for all configured interfaces.
show interfaces advertise [*interface-id* | ***detailed***]	Displays the interface's negotiation advertisement settings.
show interfaces status [*interface-id* | ***detailed***]	Displays the status for all configured interfaces.
show interfaces description [*interface-id* | ***detailed***]	Displays the description for all configured interfaces.

The following is an example of the CLI commands:

```
console(config)# interface gi2/1
console(config-if)# description "RD SW#3"
console(config-if)# shutdown
console(config-if)# no shutdown
console(config-if)# speed 100
console(config-if)# duplex full
console(config-if)# negotiation
console(config-if)# back-pressure
console(config-if)# flowcontrol on
console(config-if)# mdix auto
console(config-if)# end
console# show interfaces configuration gi2/1
                                              Flow    Admin     Back    Mdix
Port     Type         Duplex  Speed  Neg      control State    Pressure Mode
-------- ------------ ------  -----  -------- ------- -----    -------- ----
gi2/1  1G-Copper    Full    1000   Enabled    Off      Up      Disabled Auto
console# show interfaces status gi2/1
                                            Flow  Link            Back    Mdix
Port     Type         Duplex  Speed Neg     ctrl  State          Pressure Mode
-------- ------------ ------  ----- -------- ---- ----------- -------- ----
gi2/1  1G-Copper      --      --     --     --    Down           --      --
```

LAG Configuration

Use the **LAG Configuration** pages to configure LAGs. The device supports up to 12 LAGs per system. For information about Link Aggregated Groups (LAGs) and assigning ports to LAGs, see Link Aggregation.

To configure LAGs:

1 Click **Switching > Ports > LAG Configuration** in the tree view to display the **LAG Configuration: Summary** page.

   The LAG parameters are displayed.

2 To configure a LAG, click **Edit**.

3 Select the LAG and enter the fields:

   – **LAG Mode** — Select the LAG mode. The possible options are:

      - **Static** — The ports comprise a single logical port for high-speed connections between networking devices.

    - **LACP** — Link Aggregate Control Protocol. LACP-enabled LAGs can exchange information with other links in order to update and maintain LAG configurations automatically.
- **Description (0 - 64 Characters)** — Enter a user-defined description of the configured LAG.
- **LAG Type** — Displays the port types that comprise the LAG.
- **Admin Status** — Enable/disable the selected LAG.
- **Current Status** — Displays the LAG is currently operating.
- **Admin Speed** — Select the configured speed at which the LAG is operating. The possible options are:
    - **10M** — The LAG is currently operating at 10 Mbps.
    - **100M** — The LAG is currently operating at 100 Mbps.
    - **1000M** — The LAG is currently operating at 1000 Mbps.
- **Current Speed** — Displays the speed at which the LAG is currently operating.
- **Admin Auto Negotiation** — Enable/disable auto-negotiation, which is a protocol between two link partners that enables a LAG to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- **Current Auto Negotiation** — Displays the current auto-negotiation setting.
- **Admin Advertisement** — If auto-negotiation is enabled, select the auto-negotiation setting the LAG advertises. The possible options are:
    - **Max Capability** — All LAG speeds and Duplex mode settings are accepted.
    - **10 Full** — The LAG advertises for a 10 Mbps speed LAG and full duplex mode setting.
    - **100 Full** — The LAG advertises for a 100 Mbps speed LAG and full duplex mode setting.
    - **1000 Full** — The LAG advertises for a 1000 Mbps speed LAG and full duplex mode setting.

- **Current Advertisement** — Displays the speed that the LAG advertises to its neighbor LAG to start the negotiation process. The possible field values are those specified in the **Admin Advertisement** field.
- **Neighbor Advertisement** — Displays the neighboring LAG advertisement settings. The field values are identical to the **Admin Advertisement** field values.
- **Admin Flow Control** — Enable/disable flow control on the LAG. Flow Control mode is effective on the ports operating in Full Duplex in the LAG. The possible options are:
  - **Enable** — Enables flow control on the LAG (default).
  - **Disable** — Disables flow control on the LAG.
  - **Auto Negotiation** — Enables the auto-negotiation of flow control on the LAG.
- **Current Flow Control** — Displays the current Flow Control setting.

Configuring LAGs Using CLI Commands

The following table summarizes the CLI commands for configuring LAGs as displayed in the **LAG Configuration** pages.

Table 10-9. LAG Configuration CLI Commands

CLI Command	Description
`interface` *`port-channel LAG-number`*	Enters the interface configuration mode of a specific LAG.

`channel-group port-channel mode {`*`on`*`|`*`auto`*`}`
`no channel-group`
	Sets a mode for a LAG.
	Use the no form of this command restore the default configuration.

`description` *`string`*
`no description`
	Adds a description to a LAG.
	Use the no form of this command to remove the description.

`shutdown`
`no shutdown`
	Disables the LAG.
	Use the no form of this command to restart the LAG.

Table 10-9. LAG Configuration CLI Commands *(continued)*

CLI Command	Description
speed {*10*|*100*|*1000*} **no speed**	Configures the speed of the LAG when not using auto negotiation. Use the no form of this command to restore the default configuration.
negotiation [*capability* [*capability2…capability5*] **no negotiation**	Enables auto negotiation operation for the speed and duplex parameters of a LAG. Use the no form of this command to disable auto-negotiation.
flowcontrol {*auto*|*on*|*off*} **no flowcontrol**	Configures the flow control on a given LAG. Use the no form of this command to disable flow control.
show interfaces configuration [*interface-id* | ***detailed***]	Displays the configuration for the LAGs.
show interface advertise [*interface-id* | ***detailed***]	Displays the LAG's negotiation advertisement settings.
show interfaces status [*interface-id* | ***detailed***]	Displays the status for all configured LAGs.
show interfaces description [*interface-id* | ***detailed***]	Displays the description for all configured LAGs.
show interfaces *port-channel* [*interface-id*]	Displays LAG information.

The following is an example of the CLI commands:

```
console(config)# interface port-channel 1
console(config-if)# no negotiation
console(config-if)# speed 100
console(config-if)# flowcontrol on
console(config-if)# exit
console(config)# interface port-channel 2
console(config-if)# shutdown
console(config-if)# exit
console(config-if)# end
console# show interfaces port-channel
Channel         Ports
---------       ---------
ch1             Inactive: gi0/(1-3)
ch2             Active: gi0/4
```

Storm Control

When Broadcast, Multicast, or Unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice, they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a storm.

Storm protection provides the ability to limit the number of frames entering the switch, and to define the types of frames that are counted towards this limit.

When a threshold (limit) is configured on the device, the port discards traffic when that threshold is reached. The port remains blocked until the traffic rate drops below this threshold. It then resumes normal forwarding.

To configure Storm Control:

1. Click **Switching > Ports > Storm Control** in the tree view to display the **Storm Control: Summary** page.

   Storm control parameters are displayed for all ports.

2. To configure Storm Control on a port, click **Edit.**

3 Select a port from the Port drop-down list and enter the following fields:

- **Broadcast Control** — Enable/disable forwarding Broadcast packets on the specific interface.
- **Broadcast Mode** — Select the counting mode. The possible options are:
  - **Multicast & Broadcast** — Counts Broadcast and Multicast traffic together towards the bandwidth threshold.
  - **Broadcast Only** — Counts only Broadcast traffic towards the bandwidth threshold.
- **Broadcast Rate Threshold (3500-1000000)** — Enter the maximum rate (Kbits/sec) at which unknown packets are forwarded.

Configuring Storm Control Using CLI Commands

The following table summarizes the CLI commands for configuring Storm Control as displayed on the **Storm Control** pages.

Table 10-10. Storm Control CLI Commands

CLI Command	Description
storm-control include-multicast [*unknown-unicast*]	Counts Multicast packets in the Broadcast storm control.
no storm-control *include-multicast*	Use the no form of this command to disable counting of multicast packets in the Broadcast storm control.
storm-control broadcast enable	Enables Broadcast storm control.
no storm-control broadcast enable	Use the no form of this command to disable Broadcast storm control.
storm-control broadcast level kbps *kbps*	Configures the maximum Broadcast rate.
no storm-control broadcast level	Use the no form of this command to return the Broadcast level to the default value.
show storm-control **[***interface-id* **| *detailed*]**	Displays the storm control configuration.

The following is an example of the CLI commands:

```
console(config)# interface gi0/1
console(config-if)# storm-control broadcast enable
console(config-if)# storm-control include-multicast
unknown-unicast
console# show storm-control gi0/1
Port     State      Rate [Kbits/Sec]  Included
-------- --------   ----------------  ---------------------
gi0/1    Disabled   8500              Broadcast
```

Port and VLAN Mirroring

Switches usually only forward frames to relevant ports. To monitor traffic, either for information gathering, such as statistical analysis, or for troubleshooting higher-layer protocol operation, the Mirroring feature forwards frames to a monitoring port.

Mirroring provides the ability to specify that a desired destination (target) port will receive a copy of all traffic passing through designated source ports.

The frames arriving at the destination port are copies of the frames passing through the source port at ingress, prior to any switch action.

It is possible to specify several source ports to be monitored by a single target port. However, in this case, the traffic sent to the target port is placed in the target port's queues on a first come, first served basis, and any excess traffic is silently discarded. This may mean that the traffic actually seen by any device attached to the target port is an arbitrarily selected subset of the actual traffic going through the source ports.

Port mirroring is only relevant to physical ports. Therefore, if you want a LAG to function as the source of a port mirroring session, the member ports must be individually specified as sources.

Up to eight sources can be mirrored. This can be any combination of eight individual ports.

Before configuring Port Mirroring, note the following:

- Monitored ports cannot operate faster than the monitoring port.
- All Rx/Tx packets should be monitored to the same port.

Destination Port Restrictions

The following restrictions apply to destination ports:

- Destination ports cannot be configured as source ports.
- Destination ports cannot be a member of a LAG.
- IP interfaces cannot be configured on the destination port.
- GVRP cannot be enabled on the destination port.
- The destination port cannot be a member of a VLAN.
- Only one destination port can be defined.
- All QoS/CoS rules that apply to the destination port, as an egress, such as traffic shaping, are suspended for the duration of the mirroring session. Any such settings, configured on the port during the mirroring session, take effect only after the port is no longer a destination port for a mirroring session.
- Ingress mirrored packets may arrive at the ingress port either with an 802.1q tag or without. When the packets are mirrored to a port analyzer, they should be transmitted as they are received on the ingress port. However, in the device, the packet is transmitted out of the port analyzer as always tagged or always untagged (user configurable), regardless of the input encapsulation.

Source Port Restrictions

The following restrictions apply to ports specified as source ports:

- Source ports cannot be a member of a LAG.
- Source ports cannot be configured as a destination port.
- Up to eight source ports can be mirrored.

NOTE: When a port is set to be a target port for a port-mirroring session, all normal operations on it are suspended. This includes Spanning Tree and LACP. All currently active protocols and services on that port are suspended.

Port and VLAN Mirroring

To specify source and destination interfaces for port mirroring:

1. Click **Switching > Ports > Port and VLAN Mirroring** in the tree view to display the **Port Mirroring: Summary** page.

   The previously-defined source interfaces for the selected **Destination Interface** are displayed, along with the fields defined in the **Add** page and their status.

   - **Status** — Indicates if the port is currently being monitored (**Active**) or not being monitored (**notReady**), because of some problem.

2. Select the Destination Interface.
3. To add an interface to be mirrored, click **Add**, and enter the fields:
   - **Source Interface** — The port number from which port traffic is copied.
   - **Type** — Type of traffic (Tx or Rx or both) to be copied.

Configuring Port Mirroring Using CLI Commands

The following table summarizes the CLI commands for configuring Port Mirroring.

Table 10-11. Port Mirroring CLI Commands

CLI Command	Description
port monitor *src-interface-id* [*rx*|*tx*]**vlan** *vlan-id*	Starts a port monitoring session. This must be performed in Interface Configuration mode, which is the destination interface.
no port monitor *src-interface-id* **vlan** *vlan-id*	Use the no form of this command to stop a port monitoring session.
show ports monitor	Displays the port monitoring status.

The following is an example of the CLI commands:

```
console(config)# interface gi0/1
console(config-if)# port monitor gi0/8
console# show ports monitor
Source port Destination Port   Type     Status
----------- ----------------   ----     -----------
gi0/1        gi0/8             RX,TX    Active
```

11

Address Tables

This section describes how MAC addresses are handled on the device.

It contains the following topics:

- Overview
- Static Address Table
- Dynamic Address Table

Overview

MAC addresses, associated with ports, are stored in the Static Address or the Dynamic Address tables. Packets, addressed to a destination stored in one of these tables, are forwarded to the associated port.

MAC addresses are dynamically learned when packets arrive at the device. Addresses are associated with ports by learning the source address of the frame. Frames, addressed to a destination MAC address that is not associated with any port, are flooded to all ports of the relevant VLAN. In order to prevent the bridging table from overflowing, dynamic MAC addresses, from which no traffic is seen for a certain period, are erased.

Static addresses are manually entered into the table.

Static Address Table

Static addresses are manually assigned to a specific interface and VLAN on the switch. If a static address is seen on another interface, the address is ignored and it is not written to the address table.

To define a static address:

1 Click **Switching > Address Tables > Static Address Table** in the tree view to display the **Static Address Table: Summary** page.

   A list of the currently-defined static addresses is displayed.

2 To add a static address, click **Add**.

3 Enter the following fields:

- **Interface** — Select a port or LAG for the entry.
- **MAC Address** — Enter the interface MAC address.
- **VLAN ID** — Check and select the VLAN ID for the port.

  or

- **VLAN Name** — Check and enter the VLAN name.
- **Status** — Select how the entry in the table will be treated. The possible options are:
  - **Permanent** — The MAC address is never aged out of the table and, if it is saved to the Startup Configuration, it is retained after rebooting.
  - **Delete on Reset** — The MAC address is deleted when the device is reset.
  - **Delete on Timeout** — The MAC address is deleted when a timeout occurs.
  - **Secure** — The MAC address is secure when the interface is in classic locked mode.

To prevent Static MAC addresses from being deleted when the Ethernet device is reset, ensure that the port attached to the MAC address is locked.

Configuring Static Addresses Using CLI Commands

The following table summarizes the CLI commands for configuring static address parameters as displayed in the **Static Address Table** pages.

Table 11-1. Static Address CLI Commands

CLI Command	Description
mac address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-id* [**permanent | delete-on-reset | delete-on-timeout |secure**] **no mac address-table static** [*mac-address*] ***vlan*** *vlan-id*	Adds a MAC-layer station source address to the MAC address table. Use the no form of this command to delete the MAC address.

Table 11-1. Static Address CLI Commands *(continued)*

CLI Command	Description
show mac address-table [***dynamic***|***static***|***secure***] [***vlan*** *vlan*] [**interface** *interface-id*] [***address*** *mac-address*]	Displays entries in the MAC address table.

The following is an example of the CLI commands:

```
console(config-if)#bridge address 00:60:70:4C:73:FF
permanent gi0/8
console# show mac address-table static

Aging time is 300 sec

VLAN   MAC Address         Port       Type
----   -----------------   --------   --------
1      00:60:70:4C:73:FF   gi0/8      static
1      00:60:70:8C:73:FF   gi0/8      static
```

Dynamic Address Table

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

To prevent the table from overflowing and to make room for new addresses, an address is deleted from the table if no traffic is received from a dynamic MAC address for a certain period. This period of time is called the aging interval.

To configure dynamic addresses:

1. Click **Switching > Address Tables > Dynamic Address Table** in the tree view to display the **Dynamic Address Table** page.

   The current address table is displayed along with other parameters.

2 Enter **Address Aging (10-630)**. The aging time is a value between the user-configured value and twice that value minus 1. For example, if you entered 300 seconds, the aging time is between 300 and 599 seconds.

3 To clear the table, check **Clear Table**.

4 To display a subset of the addresses in a particular order, enter the query criteria and sort key under **Query By**, and click **Query**. The following fields are displayed for entries matching the query criteria:

- **Interface** — Port or LAG associated with the MAC address.
- **MAC Address** — Interface MAC address.
- **VLAN ID** — VLAN ID in the entry.

5 Address Table Sort Key TBD

Configuring Dynamic Addresses Using CLI Commands

The following table summarizes the CLI commands for configuring static address parameters as displayed in the **Dynamic Address Table** pages.

Table 11-2. Dynamic Address CLI Commands

CLI Command	Description
`mac address-table aging-time` *`seconds`*	Sets the aging time of the address table.
`no mac address-table aging-time`	Use the no form of this command to restore the default.

`clear mac address-table` ***`dynamic`*** **`interface`** *`interface-id`*
`clear mac address-table` ***`secure`*** **`interface`** *`interface-id`*
	Removes learned or secure entries from the forwarding database.

`show mac address-table` `[`***`dynamic`***`|`***`static`***`|`***`secure`***`] [`***`vlan`*** *`vlan`*`] [`***`interface`*** *`interface-id`*`] [`***`address`*** *`mac-address`*`]`	Displays entries in the MAC address table.

The following is an example of the CLI commands:

```
console(config)# mac address-table aging-time 600
console# show mac address-table dynamic

Aging time is 300 sec

VLAN      MAC Address                   Port            Type

----      ------------------            --------        --------

1         00:60:70:4C:73:FF             gi0/8           dynamic

1         00:60:70:8C:73:FF             gi0/8           dynamic
```

12

GARP

This section describes how to configure Generic Attribute Registration Protocol (GARP) on the device.

It contains the following topics:

- Overview
- GARP Timers

Overview

Generic Attribute Registration Protocol (GARP) is a general-purpose protocol that registers network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or Multicast address.

The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby devices in a bridged LAN, such as end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, these attributes are propagated to devices in the bridged LAN, and these devices form a reachability tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines and variables for the registration and deregistration of attribute values.

When configuring GARP, ensure the following:

- The leave time must be greater than or equal to three times the join time.
- The leave-all time must be greater than the leave time.
- Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP application does not operate successfully.

GARP Timers

To enable a GARP timer on an interface:

1 Click **Switching** > **GARP** > **GARP Timers** in the tree view to open the **GARP Timers: Summary** page.

   The GARP timers are displayed.

2 Click **Edit**.

3 Select an interface, and enter the fields:

   – **GARP Join Timer** (10 - 2147483640) — Enter the time, in milliseconds, during which Protocol Data Units (PDU) are transmitted.

   – **GARP Leave Timer** (10 - 2147483640) — Enter the time interval, in milliseconds, which the device waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. Leave time must be greater than or equal to three times the join time.

   – **GARP Leave All Timer** (10 - 2147483640) — Enter time interval, in milliseconds, which all devices wait before leaving the GARP state. The leave all time must be greater than the leave time.

Defining GARP Timers Using CLI Commands

This table summarizes the CLI commands for defining GARP timers as displayed in the **GARP Timers** pages.

Table 12-1. GARP Timer CLI Commands

CLI Command	Description
garp timer {*join*|*leave*|*leaveall*} *timer_value* **no garp timer**	Adjusts the GARP application join, leave, and leaveall GARP timer values. Use the **no** form of this command to restore the default configuration.
show gvrp configuration [*interface-id* | ***detailed***]	Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP.

The following is an example of the CLI commands:

```
console(config)# interface gi0/1
console(config-if)# garp timer leave 900
console(config-if)# end
console# show gvrp configuration gi0/11
GVRP Feature is currently Disabled on the device.
Maximum VLANs: 223
Port(s)   GVRP      Registration  Dynamic VLAN   Timers  (milliseconds)
          Status                  Creation       Join    Leave    Leave All
--------  -------   ------------  -----------    ------  -----    ---------
gi0/11    Disabled  Normal        Enabled        200     900      10000
```

13

Spanning Tree

This chapter describes the Spanning Tree Protocol. It contains the following topics:

- Overview
- Global Settings
- STP Port Settings
- STP LAG Settings
- Rapid Spanning Tree
- Multiple Spanning Tree

Overview

Spanning Tree Protocol (STP) provides tree topography for any bridge arrangement. STP eliminates loops by providing a unique path between end stations on a network.

Loops occur when alternate routes exist between hosts. Loops, in an extended network, can cause bridges to forward traffic indefinitely, resulting in packets not arriving at their destination, increased traffic, and reduced network efficiency.

The device supports the following Spanning Tree versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops. For more information on configuring Classic STP, see Global Settings.
- **Rapid STP (RSTP)** — Provides faster convergence of the spanning tree than Classic STP. RSTP is most effective when the network topology is naturally tree-structured, and therefore faster convergence might be possible. RSTP is enabled by default.

Although Classic STP is guaranteed to prevent Layer 2 forwarding loops, in a general network topology, there might be an unacceptable delay before convergence. This means that before convergence, each bridge or switch in the network must decide if it should actively forward traffic or not, on each of its ports.

For more information on configuring Rapid STP, see Rapid Spanning Tree.

- **Multiple STP (MSTP)** — MSTP is based on RSTP. It detects Layer 2 loops, and attempts to mitigate them by preventing the involved port from transmitting traffic.

  Since loops exist on a per-Layer 2-domain basis, a situation can occur where there is a loop in VLAN A and no loop in VLAN B. If both VLANs are on Port X, and STP wants to mitigate the loop, it stops traffic on the entire port, including VLAN B traffic, where there is no need to stop traffic.

  Multiple Spanning Tree Protocol (MSTP) solves this problem by enabling several STP instances, so that it is possible to detect and mitigate loops separately in each instance. By associating instances to VLANs, each instance is associated with the Layer 2 domain on which it performs loop detection and mitigation. This enables a port to be stopped in one instance, such as traffic from VLAN A that is causing a loop, while traffic can remain active in another domain where no loop was seen, such as on VLAN B.

  MSTP provides full connectivity for packets allocated to any VLAN, and transmits packets assigned to various VLANs, through different multiple spanning tree (MST) regions.

  MST regions act as a single bridge.

  For more information on configuring Multiple STP, see Multiple Spanning Tree.

Global Settings

To enable STP and select the STP mode on the device:

1. Click **Switching > Spanning Tree > Global Settings** in the tree view to display the **Global Settings** page.

   The currently-defined settings are displayed.

2. Enter the fields:

   – **Spanning Tree State** — Enable Spanning Tree on the device.

   – **STP Operation Mode** — Select the STP mode enabled on the device. The possible options are:

   - **Classic STP** — Enables Classic STP on the device.
   - **Rapid STP** — Enables Rapid STP on the device. This is the default value.
   - **Multiple STP** — Enables Multiple STP on the device.

   – **BPDU Handling** — Select how Bridge Protocol Data Unit (BPDU) packets are managed when STP is disabled on the port/device. BPDUs are used to transmit spanning tree information. The possible options are:

   - **Filtering** — Filter BPDU packets when spanning tree is disabled on an interface.
   - **Flooding** — Flood BPDU packets when spanning tree is disabled on an interface.

   – **Path Cost Default Values** — Select the method used to assign default path costs to STP ports. The possible options are:

   - **Short** — Specifies 1 through 65,535 range for port path costs.
   - **Long** — Specifies 1 through 200,000,000 range for port path costs.

The default path costs assigned to an interface vary according to the selected method:

Interface	Long Cost	Short Cost
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

Bridge Settings

- **Priority (0-61440 in steps of 4096)** — Enter the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The port priority value is provided in increments of 4096. For example, 4096, 8192, 12288, etc.
- **Hello Time (1-10)** — Check to use the device Hello Time, which is the interval of time in seconds that a root bridge waits between configuration messages. Enter a value.
- **Max Age (6-40**) — Check to use device Maximum Age Time, which is the time interval in seconds that a bridge waits before sending configuration messages. Enter a value.
- **Forward Delay (4-30)** — Check to use device forward delay time, which is the interval of time in seconds that a bridge remains in a listening and learning state before forwarding packets. Enter a value.

Designated Root — Displays the following:

- **Bridge ID** — The bridge priority and MAC address.
- **Root Bridge ID** — The root bridge priority and MAC address.
- **Root Port** — The port number that offers the lowest cost path from this bridge to the Root Bridge. This is significant when the Bridge is not the Root.
- **Root Path Cost** — The cost of the path from this bridge to the root.
- **Topology Changes Counts** — The total amount of STP state changes that have occurred.

– **Last Topology Change** — The amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change occurred.

Defining STP Global Parameters Using CLI Commands

The following table summarizes the CLI commands for defining STP global parameters as displayed in the **Global Settings** pages.

Table 13-1. STP Global Parameter CLI Commands

CLI Command	Description

`spanning-tree`
`no spanning-tree`
	Enables spanning tree functionality.
	Use the no form of this command to disable the spanning-tree functionality.

spanning-tree mode {*stp*|*rstp*|*mst*} **no spanning-tree mode**	Configures the mode of the spanning tree protocol. Use the no form of this command to restore the default configuration.
spanning-tree bpdu {*filtering*|*flooding*} **no spanning-tree bpdu**	Defines BPDU handling when the spanning tree is disabled globally or on a single interface. Use the no form of this command to restore the default configuration.
spanning-tree pathcost method {*long*|*short*} **no spanning-tree pathcost method**	Sets the default path cost method. Use the no form of this command to return to the default configuration.
spanning-tree priority *priority* **no spanning-tree priority**	Configures the spanning tree priority. Use the no form of this command to restore the default device spanning-tree priority.
spanning-tree hello-time *seconds* **no spanning-tree hello-time**	Configures the spanning tree bridge Hello Time, which is how often the device Broadcasts Hello messages to other devices. Use the no form of this command to restore the default configuration.

Table 13-1. STP Global Parameter CLI Commands *(continued)*

CLI Command	Description
spanning-tree max-age *seconds* **no spanning-tree max-age**	Configures the spanning tree bridge maximum age. Use the no form of this command to restore the default configuration
spanning-tree forward-time *seconds* **no spanning-tree forward-time**	Configures the spanning tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the no form of this command to restore the default configuration.
show spanning-tree [*interface-id*] [**instance** *instance-id*]	Displays spanning tree configuration.
show spanning-tree [***detail***] [***active***|***blockedports***] [***instance*** *instance-id*]	Displays detailed spanning tree information on active or blocked ports.
show spanning-tree mst-configuration	Displays spanning tree MST configuration identifier.

The following is an example of the CLI commands:

```
console(config)# spanning-tree
console(config)# spanning-tree mode rstp
console(config)# spanning-tree priority 12288
console(config)# spanning-tree hello-time 5
console(config)# spanning-tree max-age 12
console(config)# spanning-tree forward-time 25
console(config)# exit
```

STP Port Settings

To assign STP properties to individual ports:

1. Click **Switching** > **Spanning Tree** > **STP Port Settings** in the tree view to display the **STP Port Settings: Summary** page.

   The ports and their STP settings are displayed.

2. To modify STP settings on a port, click **Edit**.
3. Select the port, and enter the fields:
   - **STP** — Enable/disable STP on the port.
   - **Fast Link** — Check to enable Fast Link mode for the port. If this is enabled, the **Port State** is automatically placed in the **Forwarding** state when the port is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.
   - **BPDU Guard** — Check to enable BPDU Guard on the port.
   - **Root Guard** — Check to prevent devices outside the network core from being assigned the spanning tree root.
   - **Port State** — Displays the current STP state of a port. If the port state is not disabled, it determines what forwarding action is taken on traffic. The possible port states are:
     - **Disabled** — STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
     - **Blocking** — The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
     - **Listening** — The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses.
     - **Learning** — The port is currently in the learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
     - **Forwarding** — The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.

- **Role** — Displays the port role assigned by the STP algorithm that provides STP paths. The possible options are:
  - **Root** — This port provides the lowest cost path to forward packets to root switch.
  - **Designated** — This port is the interface through which the bridge is connected to the LAN, which provides the lowest cost path from the LAN to the Root Bridge.
  - **Alternate** — This port provides an alternate LAG to the root switch from the root interface.
  - **Backup** — This port provides a backup path to the designated port. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - **Disabled** — This port is not participating in the Spanning Tree.
- **Speed** — Displays the speed at which the port is operating.
- **Path Cost (1-200000000)** — Enter the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.
- **Default Path Cost** — Check to use the default path cost.
- **Priority** — Select the priority value that influences the port choice when a bridge has two ports connected in a loop. The priority value is provided in increments of 16.
- **Designated Bridge ID** — Displays the bridge priority and the MAC address of the designated bridge.
- **Designated Port ID** — Displays the designated port's priority and interface.
- **Designated Cost** — Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions** — Displays the number of times the port has changed from the **Forwarding** state to **Blocking**.
- **LAG** — Displays the LAG to which the port is attached.

Defining STP Port Settings Using CLI Commands

The following table summarizes the CLI commands for defining STP port parameters as displayed in the **STP Port Settings** page.

Table 13-2. STP Port Settings CLI Commands

CLI Command	Description

`spanning-tree disable`
`no spanning-tree disable`
	Disables spanning tree on a specific port.
	Use the no form of this command to enable the spanning tree on a port.

`spanning-tree cost cost`
`no spanning-tree cost`
	Configures the spanning tree cost contribution of a port
	Use the no form of this command to restore the default configuration.

`spanning-tree port-priority priority`
`no spanning-tree port-priority`
	Configures port priority.
	Use the no form of this command to restore the default configuration.

`show spanning-tree [interface-id][instance instance-id]`	Displays spanning tree configuration.
`spanning-tree portfast [auto]`	Enables Fast Link mode.
`no spanning-tree portfast`	Use the no form of this command to disable the PortFast mode.

`spanning-tree bpduguard {enable|disable}`
`no spanning-tree bpduguard`
	Shuts down an interface when it receives a bridge protocol data unit (BPDU).
	Use the no form of this command to restore the default configuration.

`spanning-tree guard root`
`no spanning-tree guard root`
	Enables root guard on all spanning tree instances on the interface.
	Use the no form of this command to disable the root guard on the interface.

`show spanning-tree [detail] [active|blockedports] [instance instance-id]`	Displays detailed spanning tree information on active or blocked ports.

The following is an example of the CLI commands:

```
console> enable
console# configure
console(config)# interface gi0/1
console(config-if)# spanning-tree disable
console(config-if)# spanning-tree cost 35000
console(config-if)# spanning-tree port-priority 96
console(config-if)# spanning-tree portfast
console(config-if)# exit
console(config)# exit
console# show spanning-tree gi0/8 instance 12
Port gi0/8 enabled
State: discarding                  Role: alternate
Port ID: 128.15                    Port cost: 19
Type: P2p (configured: Auto) Internal Port Fast: No
(configured: No)
Designated bridge Priority :       Address:
32768                              00:00:b0:07:07:49
Designated port ID: 128.11         Designated path cost: 0
Guard root: Disabled
Number of transitions to forwarding state: 3
BPDU: sent 482, received 1035
```

STP LAG Settings

To assign STP parameters to LAGs:

1. Click **Switching** > **Spanning Tree** > **STP LAG Settings** in the tree view to display the **STP LAG Settings: Summary** page.

   The LAGs and their STP settings are displayed.

2. To modify STP settings on a LAG, click **Edit**.
3. Select a LAG from the **Select a LAG** drop-down menu.
4. Enter the fields.

- **STP** — Enable/disable STP on the LAG.
- **Fast Link** — Check to enable Fast Link mode for the LAG. If Fast Link mode is enabled for a LAG, the **LAG State** is automatically placed in **Forwarding** when the LAG is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take from 30-60 seconds in large networks.
- **BPDU Guard** — Check to enable BPDU Guard on the LAG.
- **Root Guard** — Check to prevent devices outside the network core from being assigned the spanning tree root.
- **LAG State** — Displays the current STP state of the LAG. If enabled, the LAG state determines what forwarding action is taken on traffic. If the bridge discovers a malfunctioning LAG, the LAG is placed in the **Broken** state. Possible LAG states are:
  - **Disabled** — STP is currently disabled on the LAG. The LAG forwards traffic while learning MAC addresses.
  - **Blocking** — The LAG is blocked and cannot be used to forward traffic or learn MAC addresses.
  - **RSTP Discarding State** — The LAG does not learn MAC addresses and does not forward frames. This state is union of Blocking and Listening state introduced in STP (802.1.D).
  - **Listening** — The LAG is in the listening mode, and cannot forward traffic or learn MAC addresses.
  - **Learning** — The LAG is in the learning mode, and cannot forward traffic, but it can learn new MAC addresses.
  - **Forwarding** — The LAG is currently in the forwarding mode, and it can forward traffic and learn new MAC addresses.
  - **Broken** — The LAG is currently malfunctioning, and cannot be used for forwarding traffic.
- **Role** — Displays the LAG role assigned by the STP algorithm that provides STP paths. The possible options are:
  - **Root** — This LAG provides the lowest cost path to forward packets to root switch.

    - **Designated** — This LAG is the interface through which the bridge is connected to the LAN, which provides the lowest cost path from the LAN to the Root Bridge.
    - **Alternate** — This LAG provides an alternate LAG to the root switch from the root interface.
    - **Backup** — This LAG provides a backup path to the designated port. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
    - **Disabled** — This LAG is not participating in the Spanning Tree.
  - **Path Cost (1-200000000)** — Enter the amount the LAG contributes to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is being rerouted. The path cost has a value of 1 to 200000000.
  - **Default Path Cost** — Check for the device to use the default path cost.
  - **Priority** — Select the priority value of the LAG. The priority value influences the LAG choice when a bridge has looped ports. The priority value is given in steps of 16.
  - **Designated Bridge ID** — Displays the priority and the MAC address of the designated bridge.
  - **Designated Port ID** — Displays the ID of the selected interface.
  - **Designated Cost** — Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
  - **Forward Transitions** — Displays the number of times the **LAG State** has changed from the **Forwarding** state to a **Blocking state**.

Defining STP LAG Settings Using CLI Commands

For information about CLI commands for defining STP LAG settings, see Table 13-2.

The following is an example of the CLI commands:

```
console(config)# interface port-channel 1
console(config-if)# spanning-tree disable
console(config-if)# spanning-tree cost 35000
console(config-if)# spanning-tree port-priority 96
console(config-if)# spanning-tree portfast
```

Rapid Spanning Tree

While classic spanning tree prevents Layer 2 forwarding loops on a general network topology, convergence can take from 30 to 60 seconds. This delay provides time to detect possible loops, and propagate status changes.

Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that enable a faster convergence of the spanning tree, without creating forwarding loops.

To configure RSTP:

1 Click **Switching** > **Spanning Tree** > **Rapid Spanning Tree** in the tree view to display the **Rapid Spanning Tree: Summary** page.

2 To modify RSTP settings on an interface, click **Edit** and enter the fields:

   – **Interface** — Select a port or LAG.

   – **State** — Displays the RSTP state of the selected interface.

   – **Role** — Displays the port role assigned by the STP algorithm in order to provide STP paths. The possible options are:

      - **Root** — This port provides the lowest cost path to forward packets to root switch.
      - **Designated** — This port is the interface through which the bridge is connected to the LAN, which provides the lowest cost path from the LAN to the Root Bridge.
      - **Alternate** — This port provides an alternate LAG to the root switch from the root interface.

  - **Backup** — This port provides a backup path to the designated port. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - **Disabled** — This port is not participating in the Spanning Tree.
- **Mode** — Displays if RSTP is enabled.
- **Fast Link Operational Status** — Displays if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for an interface, the interface is automatically placed in the forwarding state. The possible options are:
  - **Enable** — Fast Link is enabled.
  - **Disable** — Fast Link is disabled.
  - **Auto** — Fast Link mode is enabled a few seconds after the interface becomes active.
- **Point-to-Point Admin Status** — Select if a point-to-point links is established, or permits the device to establish a point-to-point link. The possible options are:
  - **Enable** — Enables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link. To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual switch port link type. It may differ from the administrative state.
  - **Disable** — Disables point-to-point link.
  - **Auto** — The device automatically establishes a point-to-point link.

- **Point-to-Point Operational Status** — Displays the Point-to-Point operating state.
- **Active Protocol Migration Test** — Check to run a Protocol Migration test. This discovers whether the link partner using STP still exists, and if so whether it has migrated to RSTP or MSTP. If it still exists as an STP link, the device continues to communicate with it by using STP. Otherwise, if it has been migrated to RSTP or MSTP, the device communicates with it using RSTP or MSTP, respectively.

Defining Rapid STP Parameters Using CLI Commands

The following table summarizes the CLI commands for defining Rapid STP parameters as displayed in the **Rapid Spanning Tree** pages.

Table 13-3. Rapid STP Parameters CLI Command

CLI Command	Description
spanning-tree link-type {***point-to-point***|***shared***} **no spanning-tree spanning-tree link-type**	Overrides the default link-type setting determined by the port duplex mode, and enables RSTP transitions to the forwarding state. Use the no form of this command to restore the default configuration.
clear spanning-tree detected-protocols [***interface*** *interface-id*]	Restarts the protocol migration process.
show spanning-tree [*interface-id*] [***instance*** *instance-id*]	Displays spanning tree configuration.

The following is an example of the CLI commands:

```
console(config)# interface gi0/5
console(config-if)# spanning-tree link-type shared
```

Multiple Spanning Tree

This section describes Multiple Spanning Tree Protocol (MSTP).

It contains the following topics:

- MSTP Overview
- MSTP Properties
- VLAN to MSTP Instance
- MSTP Instance Settings
- MSTP Interface Settings

MSTP Overview

MSTP maps VLANs into STP instances, using various load balancing scenarios. As a result of this partitioning into instances, if port A is blocked in one STP instance, the same port can be placed in the **Forwarding State** in another STP instance.

In addition, packets assigned to various VLANs are transmitted along different paths within Multiple Spanning Trees Regions (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted.

MSTP Properties

To set an MSTP region:

1. Click **Switching** > **Spanning Tree** > **MSTP Properties** in the tree view to display the **MSTP Properties: Summary** page.
2. Enter the following fields:
   - **Region Name (1-32 Characters)** — Enter the user-defined MSTP region name.
   - **Revision (0-65535)** — Enter the unsigned 16-bit number that identifies the current MST configuration revision. The revision number is required as part of the MST configuration.
   - **Max Hops (1-40)** — Enter the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out.

- **IST Master** — Displays the Internal Spanning Tree Master ID. The IST Master is the instance 0 root.

Configuring MST Properties Using CLI Commands

The following table summarizes the CLI commands for configuring MST properties in the **MSTP Properties** pages.

Table 13-4. MSTP Properties CLI Commands

CLI Command	Description
`spanning-tree mst configuration`	Enters MST Configuration mode.

`spanning-tree mst` ***`max-hops`*** *`hop-count`*
`no spanning-tree mst` ***`max-hops`***
	Configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out (in Global Configuration mode).
	Use the no form of this command to restore the default configuration.

`name` *`string`*
`no name`
	Sets the MSTP region name.
	Use the no form of this command to restore the default setting.

`revision` *`value`*
`no revision`
	Defines the MST configuration revision number.
	Use the no form of this command to restore the default configuration.

`exit`	Exits the MST region configuration mode after applying configuration changes.
`show` `{`***`current`***`|`***`pending`***`}`	Displays the current or pending MST region configuration.
`show spanning tree mst-configuration`	Displays the MSTP configuration.

The following is an example of the CLI commands:

```
console(config)# spanning-tree mst configuration
console(config-mst)# instance 1 add vlan 10-20
console(config-mst)# name region1
console(config-mst)# revision 1
console(config)# interface gi0/1
console(config-if)# spanning-tree mst 1 port-priority 144
console(config)# spanning-tree mst max-hops 10
console(config)# spanning-tree mst configuration
console(config-mst)# instance 2 add vlan 21-30
console(config-mst)# name region1
console(config-mst)# revision 1
console(config-mst)# show pending
Pending MST configuration
Name: Region1
Revision: 1
Instance VLANs Mapped
-------- -----------
0        1-9,31-4094
1        10-20
2        21-30
```

VLAN to MSTP Instance

To map VLANs to MSTP instances:

1. Click **Switching** > **Spanning Tree** > **VLAN to MSTP Instance** in the tree view to display the **VLAN to MSTP Instance: Summary** page.

   The MSTP instances and their associated VLANs are displayed.

2. To associate a VLAN with an MSTP instance, click **Edit**.
3. Select the MSTP instance, the VLAN and whether to add or remove the VLAN from the MSTP instance association.

4 Enter the fields:

- **Select MST Instance ID** — Select an MST instance.
- **VLANs** — Enter the VLANs being mapped to this instance.
- **Action** — Select the mapping action. The possible options are:
  - **Add** —Add these VLANS to the MST instance.
  - **Remove** —Remove these VLANS from the MST instance.

Mapping VLAN to MSTP Instances Using CLI Commands

The following table summarizes the CLI commands for mapping VLANs to MSTP instances.

Table 13-5. Mapping VLAN to MSTP Instances Using CLI Commands

CLI Command	Description
spanning-tree mst configuration	Enters MST Configuration mode.
instance *instance-id* **vlan** *vlan-range* **no instance** *instance-id* **vlan** *vlan-range*	Maps VLANs to an MST instance. Use the no form of this command to restore default mapping.
show spanning-tree detail	Displays the spanning-tree configuration

The following is an example of the CLI commands:

```
console(config)# spanning-tree mst configuration
console(config-mst)# instance 1 vlan 10-20
```

MSTP Instance Settings

To configure MSTP instances:

1 Click **Switching** > **Spanning Tree** > **MSTP Instance Settings** in the tree view to display the **MSTP Instance Settings** page.

The MSTP instances and their associated VLANs are displayed.

2 Select an **Instance ID**.

3 Enter the **Bridge Priority (0-61440)** of this bridge for the selected MSTP instance.

4 The following fields are displayed:

- **Included VLANs** — Displays VLANs included in this instance.
- **Designated Root Bridge ID** — Priority and MAC address of the Root Bridge for the MST instance.
- **Root Port** — Root port of the selected instance.
- **Root Path Cost** — Root path cost of the selected instance.
- **Bridge ID** — Bridge priority and the MAC address of this switch for the selected instance.
- **Remaining Hops** — Number of hops remaining to the next destination.

Configuring MSTP Instances Using CLI Commands

The following table summarizes the CLI commands for configuring the fields in the **MSTP Instance** pages.

Table 13-6. Configuring MSTP Instances CLI Commands

CLI Command	Description
spanning-tree mst configuration	Enters MST Configuration mode.
spanning-tree mst *instance-id* **priority** *priority* **no spanning-tree mst** *instance-id* **priority**	Configures the device priority for the specified spanning-tree instance. Use the no form of this command to restore the default configuration.
show spanning-tree detail	Displays the spanning-tree configuration

The following is an example of the CLI commands:

```
console(config)# spanning-tree mst configuration
console(config-mst)# spanning-tree mst 1 priority 4096
```

MSTP Interface Settings

To assign interfaces to MSTP instances:

1. Click **Switching > Spanning Tree > MSTP Interface Settings** in the tree view to display the **MSTP Interface Settings: Summary** page.

   MSTP interface settings for the selected instance is displayed.

2. To set MSTP settings for an interface, click **Edit**.

3. Select an instance, and enter the fields:

   - **Interface ID —** Assign either ports or LAGs to the selected MSTP instance.
   - **Port State —** Displays whether the port is enabled or disabled in the specific instance.
   - **Type —** Displays whether MSTP treats the port as a point-to-point port, or a port connected to a hub, and whether the port is internal to the MST region or a boundary port. A Master port provides connectivity from a MSTP region to the outlying CIST root. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode.
   - **Role —** Displays the port role assigned by the STP algorithm in order to provide to STP paths. The possible options are:
     - **Root** — This port provides the lowest cost path to forward packets to root switch.
     - **Designated** — This port is the interface through which the bridge is connected to the LAN, which provides the lowest cost path from the LAN to the Root Bridge.
     - **Alternate** — This port provides an alternate LAG to the root switch from the root interface.
     - **Backup** — This port provides a backup path to the designated port. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
     - **Disabled** — This port is not participating in the Spanning Tree.
   - **Interface Priority —** Enter the interface priority for specified instance.

- **Path Cost (1-200,000,000)** — Enter the port contribution to the Spanning Tree instance. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the Forwarding state.
- **Default Path Cost** — Check to use the default path cost.
- **Designated Bridge ID —** Displays the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID —** Displays the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost —** Displays the cost of the path from the link or the shared LAN to the root.
- **Forward Transitions —** Displays the number of times the port changed to the forwarding state.
- **Remain Hops —** Displays the number of hops remaining to the next destination.

Defining MSTP Interfaces Using CLI Commands

The following table summarizes the CLI commands for defining MSTP interfaces as displayed in the **MSTP Interfaces** pages.

Table 13-7. MSTP Interface CLI Commands

CLI Command	Description
spanning-tree mst *instance-id* **cost** *cost* **no spanning-tree mst** *instance-id cost*	Sets the path cost of the port for MST calculations (in Interface Configuration mode). Use the no form of this command to restore the default configuration.
spanning-tree mst *instance-id* **port-priority** *priority*	Configures the device priority for the specified spanning-tree instance (in Interface Configuration mode). Use the no form of this command to restore the default configuration.
show spanning-tree mst-configuration	Displays the MST configuration.

The following is an example of the CLI commands:

```
console(config)# interface gi0/8
console(config-if)# spanning-tree mst 1 cost 4
```

14

VLANs

This chapter describes how VLANs are configured on the device.

It contains the following topics:

- Overview
- VLAN Membership
- Port Settings
- LAG Settings
- Protocol Groups
- Protocol Port
- GVRP Parameters
- Private VLAN
- Voice VLAN

Overview

A VLAN is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network, or the fact that they might be intermingled with other teams. Reconfiguration of the network can be done through software rather than by physically unplugging and moving devices or wires.

A VLAN can be thought of as a Broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate bridge group for each VLAN.

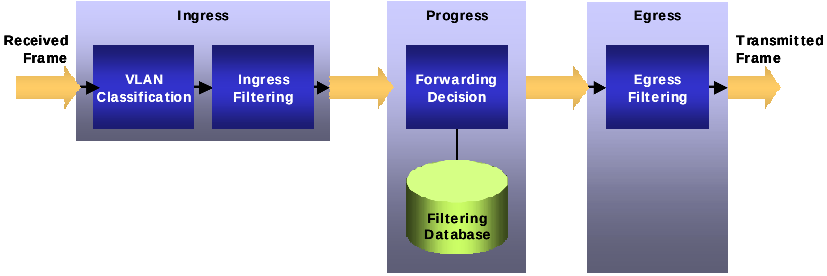
VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management.

None of the switches, within a defined group, will bridge any frames, not even broadcast frames, between two VLANs.

Frame Flow

Figure 14-1 describes the flow of VLAN frames from the Ingress port to the Egress port:

Figure 14-1. Frame Flow Through a VLAN



When a frame is received, it must be assigned a VLAN. VLAN assignment is accomplished by the following steps:

1. If the frame contains a VLAN tag, that tag is used, otherwise the frame is classified by the port's default VLAN (PVID), if it is defined.
2. After classification, the frame may pass (if enabled) through ingress filtering, where the frame is dropped if the frame's VLAN ID is not one of the VLANs to which the ingress port belongs.
3. A forwarding decision is made, as a function of the VLAN ID and the destination MAC address.

4. The egress rules define whether the frame is to be sent as tagged or untagged.

Special-case VLANs

VLAN#1 and VLAN#4095 are special-case VLANs:

- **VLAN1** — Defined as the default VLAN, and may only be used as a Ports Default VLAN ID (PVID). This means that if the VLAN, whose VID is the current port's PVID, is deleted from the port (or from the system), that port's PVID is set to 1. VLAN#1 cannot be deleted from the system.
- **VLAN #4095** — Defined (according to standard and industry practice) as the "discard" VLAN. A frame classified to this VLAN is silently dropped.

QinQ Tagging

QinQ tagging enables you to add an additional tag to previously-tagged packets. The added tag provides a VLAN ID to each customer, which ensures private and segregated network traffic. The VLAN ID tag is assigned to a customer port in the service provider network. The designated port then provides additional services to the packets with the double-tags. This enables administrators to expand service to VLAN users.

Port Modes

Ports participating in Layer 2 switching may be classified as:

- **Access Ports**

  Ports set to Access mode belong to a single VLAN, whose VID is the currently set PVID (default =1). These ports accept all untagged frames, and all frames tagged with the VID, currently set as the port's PVID. All traffic is sent untagged. If the VLAN, whose VID is set as the current PVID of the port, is deleted from the system, or deleted from the port, the port's PVID will be set to 1, meaning that the port will be made a member of VLAN#1, the default VLAN.

  Ingress filtering is always enabled for ports in Access mode.

  Setting an Access port’s PVID to 4095 effectively shuts it down, as no frames will be transferred in either direction.

  Access mode ports are intended to connect end-stations to the system, especially when the end-stations are incapable of generating VLAN tags.

- **Trunk Ports**

  Ports set to Trunk mode may belong to multiple VLANs. The default VLAN membership of a trunk port is all VLANs (1-4094). A PVID must be set on the port (it can be a non-existing VLAN). Trunk ports accept tagged and untagged frames. Untagged frames will be classified to the VLAN whose VLAN ID (VID) is configured as the port's PVID.

  Frames, sent from the port in the VLAN, whose VID is the current PVID, are sent untagged. Frames sent in all other VLANs active on the port are sent tagged.

  Ingress filtering is always enabled on Trunk-mode ports. Incoming frames will undergo ingress filtering, and if correctly tagged, (tagged with a VID of one of the VLANs to which the port currently belongs) are admitted.

  The default PVID is 1 (the default VLAN). If another VID is configured as the port's PVID, and the corresponding VLAN is deleted from the port or from the system, the port's PVID reverts to 1, meaning that the port is made a member of the default VLAN.

  Setting a trunk-port's PVID to 4095 limits traffic to tagged frames. Incoming untagged frames are silently discarded, and no frames are sent untagged.

  Trunk-mode ports are intended for switch-to-switch links, where traffic is usually tagged.

- **General Ports**

  Ports set to General mode may be members of multiple VLANs. Each of these VLANs may be configured to be tagged or untagged. This setting applies to transmitted frames. Incoming untagged frames are classified into the VLAN whose VID is the currently configured PVID.

  Ingress filtering may be disabled on General ports. Ingress filtering is enabled by default.

- **Promiscuous Ports**

  A promiscuous port can communicate with all ports of the same Private VLAN (PVLAN), including the isolated ports of the same PVLAN.

- **Isolated**

  An isolated port has complete Layer 2 isolation from the other ports within the same PVLAN, but not from the promiscuous ports. Isolated ports can communicate with promiscuous ports.

In the factory default configuration, all ports are designated as Access ports, and are associated with the default VLAN.

Acceptable Frame Type

The acceptable frame type can be set on a port to accept all frames (tagged and untagged), tagged only, or untagged only. This setting takes precedence over all other settings, so that if the acceptable frame type is tagged only, incoming untagged frames are silently discarded, even if the port has a valid PVID.

VLAN Membership

The device supports up to 4092 VLANs (VLANs 2-4094).

Ports are assigned to a VLAN in the **Port Settings** pages.

To view the ports in a VLAN, and assign various parameters:

1 Click **Switching > VLAN > VLAN Membership** in the tree view to display the **VLAN Membership: Summary** page.

   The ports in the selected VLAN are displayed along with their statuses.

   Each port/LAG is labeled with one of the following codes, regarding its membership in the VLAN:

   – **T** — Tagged. The interface is a member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.

   – **U** — Untagged. The interface is a member of a VLAN. Packets forwarded by the interface are untagged.

   – **F** — Forbidden. The interface is denied membership to a VLAN.

   – **Blank** — The interface is not a VLAN member. Packets associated with the interface are not forwarded.

2 Enter the fields:

- **Show VLAN** — Check one of the possible options:
  - **VLAN ID** — Check VLAN ID, and select a VLAN ID to view.
  - **VLAN Name** — Check VLAN Name, and select a VLAN ID to view.
- **VLAN Name (0-32 Characters)** — Enter a new VLAN name.
- **Status** — The VLAN type. Possible values are:
  - **Dynamic** — The VLAN was dynamically created through GVRP.
  - **Static** — The VLAN is user-defined.
- **Authentication Not Required** — Enable/disable authentication on the VLAN.

3 To define a new VLAN, click **ADD**, and enter the fields. The fields in this page are described above.

Defining VLAN Membership Using CLI Commands

The following table summarizes the CLI commands for defining VLAN membership as displayed in the **VLAN Membership** pages.

Table 14-1. VLAN Membership CLI Commands

CLI Command	Description
vlan database	Enters the VLAN configuration mode.
vlan {*vlan-range*}[**name** *vlan-name*] **no vlan** *vlan-range*	Creates a VLAN. Use the no form of this command to restore the default configuration or delete a VLAN.
name *string* **no name**	Adds a name to a VLAN. Use the no form of this command to remove the VLAN name.
dot1x auth-not-req **no dot1x auth-not-req**	Enables unauthorized devices access to the VLAN. Use the no form of this command to disable access to the VLAN.

The following is an example of the CLI commands:

```
console(config)# vlan database
console(config-vlan)# vlan 1972
console(config-vlan)# end
console(config)# interface vlan 1972
console(config-if)# name Marketing
console(config-vlan)# dot1x auth-not-req
console(config-if)# end
```

Port Settings

After a VLAN has been defined, assign ports to it.

To assign a VLAN to untagged packets, arriving on the device, enter the port default VLAN ID (PVID). All untagged packets arriving to the device are tagged by the ports PVID.

All ports must have a defined PVID. If no other value is configured, the default VLAN PVID is used. VLAN ID #1 is the default VLAN, and cannot be deleted from the system.

To configure ports on a VLAN:

1 Click **Switching** > **VLAN** > **Port Settings** in the tree view to display the **Port Settings: Summary** page.

  All interfaces and their settings are displayed.

2 To modify the port settings, click **Edit,** and enter the fields:

  – **Port** — Enter the port number to be modified.

  – **Switchport Mode (Layer 2+ mode)**— Enter the port system mode. The possible options are:

    - **Layer 2**— Set the port to layer 2 mode.
    - **Layer 2+**— Set the port to layer 3 mode. in which static routing is supported.

  – **Port VLAN Mode** — Enter the port VLAN mode. The possible options are:

  - **Access** — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types that are accepted on the port cannot be designated. Ingress filtering cannot be enabled/disabled on an access port.
  - **Trunk** — The port belongs to VLANs on which all ports are tagged (except for one port that can be untagged).
  - **General** — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
  - **Customer** — When a port is in Customer mode, an added tag provides a VLAN ID to each customer, ensuring private and segregated network traffic for that customer.
  - **Private VLAN Promiscuous** — The port is a promiscuous port.
  - **Private VLAN Host** — The port is an isolated port

- **Current Reserved VLAN** — Displays the VLAN currently designated by the system as the reserved VLAN.
- **Reserve VLAN for Internal Use (1-4094)** — Check to enter a reserved VLAN, and enter its ID. If none is required, check **None**.
- **PVID (1-4095)** — Enter a VLAN ID to be added to untagged packets. The possible values are 1-4095. VLAN 4095 is defined according to standard and industry practice as the discard VLAN. Packets classified to the discard VLAN are dropped.
- **VLAN List (I - Inactive Configuration)** — Enter the VLAN(s) to which this port belongs, and indicate its type. The possible options are:
  - **T** — Tagged. The port is a member of a VLAN. All packets forwarded by the LAG are tagged. The packets contain VLAN information.
  - **U** — Untagged. The port is a member of a VLAN. Packets forwarded by the LAG are untagged.
  - **F** — Forbidden. The port is denied membership to a VLAN.

  Click **Add** to move the port to the VLAN list together with its type.
- **Frame Type** — Select the packet type accepted on the port. The possible options are:

    - **Admit All** — Both tagged and untagged packets are accepted on the port.
    - **Admit Tagged Only** — Only tagged packets are accepted on the port.
    - **Admit Untagged Only** — Only untagged packets are accepted on the port.
  - **Ingress Filtering** — Enable/disable ingress filtering, which discards packets that are destined to VLANs of which the specific port is not a member.
  - **Native VLAN ID(1-4094)** — Enter VLAN used for untagged traffic to trunk ports.
  - **Multicast VLAN ID(1-4094)** — Enter VLAN used for Multicast TV VLAN traffic on access ports.
  - **Customer VLAN ID(1-4094)** — Enter VLAN used for customer ports.

Assigning Ports to VLAN Groups Using CLI Commands

The following table summarizes the CLI commands for assigning ports to VLAN groups.

Table 14-2. Port-to-VLAN Group Assignments CLI Commands

CLI Command	Description
switchport general acceptable-frame-type {*tagged-only*|*untagged-only*|*all*} **no switchport general acceptable-frame-type**	Configures ingress filtering based on packet type tagged/untagged. Use the no form of this command to return to default.
switchport mode {*access*|*trunk*|*general*|*private-vlan {promiscuous |host}*|*customer}* **no switchport mode**	Configures the VLAN membership mode of a port. Use the no form of this command to restore the default configuration.

Table 14-2. Port-to-VLAN Group Assignments CLI Commands *(continued)*

CLI Command	Description
switchport access vlan {*vlan-id* | ***none***} **no switchport access vlan**	Configures the VLAN ID when the interface is in access mode. Use the no form of this command to restore the default configuration.
switchport trunk allowed vlan {***all*** |***none***|***add*** *vlan-list*|***remove*** *vlan-list*|***except*** *vlan-list*}	Sets the trunk characteristics when the interface is in Trunking mode.
switchport trunk native vlan **{***vlan-id*|***none***} **no switchport trunk native vlan**	Defines the native VLAN when the interface is in trunk mode. Use the no form of this command to restore the default configuration.
switchport general allowed vlan **{*add*|*remove*}** *vlan-list* **[*tagged*|*untagged*]** **no switchport general allowed vlan**	Sets the general characteristics when the interface is in general mode. Use the no form of this command to reset a general characteristic to the default.
switchport general pvid *vlan-id* **no switchport general pvid**	Configures the PVID when the interface is in general mode. Use the no form of this command to restore the default configuration.
switchport customer *vlan* *vlan-id* **no switchport customer vlan**	Sets the port's VLAN when the interface is in customer mode. Use the no form of this command to restore the default configuration.
switchport mode {***access***|***trunk***|***general***|***private-vlan*** {***promiscuous***|***host***}|***customer***} **no switchport mode**	Configure the VLAN membership mode of a port. Use the no form of this command to restore the default configuration.
switchport **no switchport**	Put an interface that is in Layer 3mode into Layer 2 mode. Use the no form of this command to put an interface in Layer 3 mode.

The following is an example of the CLI commands:

```
console(config)# vlan database
console(config-vlan)# vlan 23-25
console(config-vlan)# end
console(config)# interface vlan 23
console(config-if)# name Marketing
console(config-if)# end
console(config)# interface gi0/5
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 23
console(config-if)# end
console(config)# interface gi0/6
console(config-if)# switchport mode trunk
console(config-if)# switchport mode trunk allowed vlan add
23-25
console(config-if)# end
console(config)# interface gi0/8
console(config-if)# switchport mode general
console(config-if)# switchport general allowed vlan add
23,25 tagged
console(config-if)# switchport general pvid 25
```

LAG Settings

VLANs can either be composed of individual ports or of LAGs. Untagged packets entering the device are tagged with the LAGs ID specified by the PVID.

To configure LAGs on a VLAN:

1 Click **Switching > VLAN > LAG Settings** in the tree view to display the **VLAN LAG Settings** page.

All LAGs and their settings are displayed.

2 To modify the LAG settings, click **Edit**, and enter the fields:

- **LAG** — Select the LAG to be modified.
- **Switchport Mode (Layer 2+ mode)**— Enter the LAG system mode. The possible options are:
  - **Layer 2**— Set the LAG to layer 2 mode.
  - **Layer 2+**— Set the LAG to layer 3 mode. in which static routing is supported.
- **Port VLAN Mode** — Enter the port VLAN mode. The possible options are:
  - **General** — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
  - **Access** — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types that are accepted on the port cannot be designated. Ingress filtering cannot be enabled/disabled on an access port.
  - **Trunk** — The port belongs to VLANs on which all ports are tagged (except for one port that can be untagged).
  - **Customer** — When a port is in Customer mode, an added tag provides a VLAN ID to each customer, ensuring private and segregated network traffic for that customer.
  - **Private VLAN Promiscuous** — The port is a promiscuous port.
  - **Private VLAN Host** — The port is an isolated port
- **Current Reserved VLAN** — Displays the VLAN currently designated as the reserved VLAN.
- **Reserve VLAN for Internal Use (1-4094)** — Enter the VLAN that is designated as the reserved VLAN after the device is reset, or select **None**.
- **PVID (1-4095)** —Assigns a VLAN ID to untagged packets. The possible VLAN IDs are 1-4095. VLAN 4095 is defined as per standard and industry practice, as the discard VLAN. Packets classified to this VLAN are dropped.

- **VLAN List (I - Inactive Configuration)** — Enter the VLAN(s) to which this LAG belongs, and indicate its type. The possible options are:
  - **T** — Tagged. The LAG is a member of a VLAN. All packets forwarded by the LAG are tagged. The packets contain VLAN information.
  - **U** — Untagged. The LAG is a member of a VLAN. Packets forwarded by the LAG are untagged.
  - **F** — Forbidden. The LAG is denied membership to a VLAN.

  Click **Add** to move the LAG to the VLAN list together with its type.
- **Frame Type** — Packet type accepted by the LAG. The possible options are:
  - **Admit All** — Tagged and untagged packets are both accepted by the LAG.
  - **Admit Tag Only** — Only tagged packets are accepted by the LAG.
  - **Admit Untagged Only** — Only untagged packets are accepted on the LAG.
- **Ingress Filtering** — Enable/disable Ingress filtering by the LAG. Ingress filtering discards packets that are destined to VLANs of which the specific LAG is not a member.
- **Native VLAN ID (1-4094)** — Enter VLAN used for untagged traffic to trunk ports, or select **None**.
- **Multicast VLAN ID (1-4094)** — Enter VLAN used for Multicast TV VLAN traffic on access ports, or select **None**.
- **Customer VLAN ID (1-4094)** — Enter VLAN used for customer ports, or select **None**.

Assigning LAGs to VLAN Groups Using CLI Commands

Refer to Table 14-2 for a list of the LAG settings CLI commands.

Protocol Groups

Protocol groups are based on protocol-based VLANs.

Protocol-based VLANs

Untagged frames received on a VLAN-aware switch can be classified by methods others than source port, such as data-link-layer protocol identification. This classification method is referred to as protocol-based VLANs.

Protocol-based VLANs are useful for isolating Layer 2 traffic of various Layer 3 protocols. If, for example, a switch serves IP stations and IPX stations that communicate with a single VLAN-unaware server, without using protocol-based VLANs, all the Layer 2 Broadcast traffic would reach all the stations. With protocol-based VLANs, the switch can forward incoming traffic from the server to stations in a specific VLAN only.

Protocol-based VLANs are only available on General ports.

Classification rules are set on a per-port basis, and may be sensitive to the frame's encapsulation. The default encapsulation assumed is Ethernet.

On each port, a user can define associations between groups of data-link layer protocols and ports. For each group/port combination, the user may set the VLAN to which frames incoming on that port will be classified if they belong to any of the protocols in the group.

Several protocol-groups may be associated to a single port, and a protocol group may be assigned to multiple ports, if so desired.

It is not guaranteed that the VLAN to which the frame is classified exists in the system, or is active on that port.

Restrictions

The following frames (packet) types are supported: Ethernet, RFC 1042, and LLC Other.

There may be dependencies between protocols and encapsulations, and specifying one protocol may automatically add additional protocols to the protocol-group, such as specifying IP implies ARP and vice-versa.

Similarly, there may be implied dependencies between encapsulations, so that specifying an encapsulation implies defining the protocol group for related encapsulations. An example of this is specifying the Ethernet encapsulation, even by default, implies IEEE802 encapsulation, as per RFC 1042.

The following standards are relevant:

- IEEE802.1V defines VLAN assignment by protocol type.
- IETF RFC 10-2 defines a standard for the transmission of IP datagrams over IEEE 802 Networks

Defining Protocol Groups

Define protocol groups in two steps:

1. Define a protocol group by assigning one or more protocols to the group and giving it a protocol-group ID (any integer), using the **Protocol Group** pages.
2. Associate the group with a desired VLAN classification, per port, using the **Protocol Port** pages.

To define a protocol group:

1. Click **Switching > VLAN > Protocol Group** in the tree view to display the **Protocol Group: Summary** page.

   The currently-defined protocol groups are displayed.

2. To add a new protocol group, click **Add**, and enter the fields:
   – **Frame Type** — Select a frame type to be accepted in the protocol group.
   – **Protocol Value** — Select a protocol name.

     or

   – **Ethernet-Based Protocol Value (0600 - FFFF)** — Enter the Ethernet protocol group type.
   – **Protocol Group ID** — Assign a protocol group ID number.

Defining VLAN Protocol Groups Using CLI Commands

The following table summarizes the CLI commands for defining VLAN Protocol groups.

Table 14-3. VLAN Protocol Groups CLI Commands

CLI Command	Description
map protocol *protocol [encapsulation-value]* **protocols-group** *group*	Maps a protocol to a protocol group. Protocol groups are used for protocol-based VLAN assignment.
no map protocol protocol [*encapsulation*]	Use the no form of this command to delete a protocol from a group.

The following is a sample of the CLI commands:

```
console (config)# vlan database
console (config-vlan)# map protocol ip protocols-group 213
```

Protocol Port

A protocol port is a port assigned to a particular protocol group. Traffic from particular types of frames may be assigned to a protocol group, which has a port and VLAN associated with it.

To add an interface to a protocol group:

1 Click **Switching** > **VLAN** > **Protocol Port** in the tree view to display the **Protocol Port: Summary** page.

  A list of previously-defined protocol groups is displayed.

2 To assign an interface to a protocol group, click **Add**, and enter the fields:

  – **Interface** — Port number to be added to a protocol group.

  – **Group ID** — Select a protocol group ID to which the interface is added.

    Protocol ports can either be attached to a VLAN ID or a VLAN name.

  – **VLAN ID (1- 4094)** —Check and enter a VLAN ID.

    or

  – **VLAN Name** — Check and enter a VLAN name.

Defining Protocol Ports Using CLI Commands

The following table summarizes the CLI command for defining protocol ports.

Table 14-4. **Protocol Port CLI Commands**

CLI Command	Description
switchport general map protocols-group *group* **vlan** *vlan-id* **no switchport general map protocols-group** *group*	Sets a protocol-based classification rule. Use the no form of this command to delete a classification.

The following is a sample of the CLI commands:

```
console (config-if)# switchport general map protocols-
group 1 vlan 8
```

GVRP Parameters

GARP VLAN Registration Protocol (GVRP) is provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP enables VLAN-aware bridges to automatically learn VLANs-to-bridge-ports mapping, without having to individually configure each bridge and register VLAN membership.

To ensure the correct operation of the GVRP protocol, it is advised to set the maximum number of GVRP VLANs equal to a value which significantly exceeds:

- The number of all static VLANs both currently configured and expected to be configured.
- The number of all dynamic VLANs participating in GVRP, both currently configured (initial number of dynamic GVRP VLANs is 128) and expected to be configured.

To set GVRP parameters:

1. Click **Switching > VLAN > GVRP Parameters** in the tree view to display the **GVRP Parameters: Summary** page.
2. Enable/disable GVRP on the device in the **GVRP Global Status** field.

3 Check **Ports** and select either an **External** or **Internal** port to view ports on the device, or select **LAGs** to view the LAGs in the system.

4 To set GVRP for an interface, click **Edit,** and enter the fields:

- **Interface** — Specifies port or LAG for editing GVRP settings.
- **GVRP State** — Enable/disable GVRP on the interface.
- **Dynamic VLAN Creation** — Enable/disable Dynamic VLAN creation on the interface.
- **GVRP Registration** — Enable/disable VLAN registration through GVRP on the interface.

Configuring GVRP Using CLI Commands

The following table summarizes the CLI commands for configuring GVRP as displayed in the **GVRP Global Parameters** page.

Table 14-5. GVRP Global Parameters CLI Commands

CLI Command	Description

`gvrp enable`
`no gvrp enable`
	In Global Configuration mode, this command enables GVRP globally. In Interface Configuration mode, it enables GVRP on the interface.
	Use the no form of this command to disable GVRP on the device.

`gvrp vlan-creation-forbid`
`no gvrp vlan-creation-forbid`
	Enables or disables dynamic VLAN creation.
	Use the no form of this command to enable dynamic VLAN creation or modification.

`gvrp registration-forbid`
`no gvrp registration-forbid`
	De-registers all dynamic VLANs, and prevents dynamic VLAN registration on the port.
	Use the no form of this command to allow dynamic registration of VLANs on a port.

Table 14-5. GVRP Global Parameters CLI Commands *(continued)*

CLI Command	Description
show gvrp configuration [*interface-id*]|**detailed**]	Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.
show gvrp error-statistics [*interface-id*]	Displays GVRP error statistics.
show gvrp statistics [*interface-id*]	Displays GVRP statistics.
clear gvrp statistics [*interface-id*]	Clears all the GVRP statistics information.

```
console(config)# gvrp enable
console(config)# interface gi0/1
console(config-if)# gvrp enable
console(config-if)# gvrp vlan-creation-forbid
console(config-if)# gvrp registration-forbid
console(config-if)# end
console# show gvrp configuration
GVRP Feature is currently Disabled on the device.
Maximum VLANs: 4094
Port(s) GVRP-Status Registration Dynamic VLAN Timers(milliseconds)
                                 Creation      Join     Leave      Leave All
-------- ----------- ------------ ------------ ----      -----      --------
gi0/1    Disabled    Normal       Enabled       200       600        10000
gi0/2    Disabled    Normal       Enabled       200       600        10000
gi0/3    Disabled    Normal       Enabled       200       600        10000
gi0/4    Disabled    Normal       Enabled       200       600        10000
gi0/5    Disabled    Normal       Enabled       200       600        10000
gi0/6    Disabled    Normal       Enabled       200       600        10000
gi0/7    Disabled    Normal       Enabled       200       600        10000
```

Private VLAN

Private VLANs (PVLANs) provide Layer 2 isolation between ports that share the same Broadcast domain, or in other words, they create a point-to-multipoint Broadcast domain. The ports can be located anywhere in the Layer 2 network, as opposed to protected ports which must be in the same stack.

The switch ports can be members of a Private VLAN (PVLAN) in the following membership types:

- Promiscuous ports that can communicate with all ports of the same PVLAN, including the isolated ports of the same PVLAN.
- Isolated ports that have complete Layer 2-isolation from the other ports within the same PVLAN, but not from the promiscuous ports. Isolated ports can communicate with promiscuous ports.

The PVLAN entity is implemented by allocating the following VLANs per PVLAN:

- Primary VLAN: Carries traffic from promiscuous ports.
- Isolated VLAN: Carries traffic from isolated ports.

To configure PVLANs:

1. Click **Switching > VLAN > Private VLAN** in the tree view to display the **Private VLAN: Summary** page.

   The previously-defined private VLANs are displayed.

2. To query by **Associated Primary VLAN ID**, check that field, enter a VLAN ID, and click **Query**. The associated VLANs are displayed.
3. To define a private VLAN, click **Assign,** and enter the fields:
   - **Private VLAN ID** — Select a VLAN to be assigned.
   - **Private VLAN Type** — Select one of the possible options:
     - **Primary** — Traffic from promiscuous ports flow through this type of VLAN. This is for the internet or shared servers.
     - **Isolated** —Traffic from isolated ports flow through this type of VLAN.

- **Associate Primary VLAN** — If the Private VLAN type is Isolated, check to associate the isolated VLAN with a primary VLAN, thus allowing traffic between isolated and promiscuous ports.
- **Primary VLAN ID** — Select a VLAN to be associated with the isolated VLAN.

4 To assign ports to the private VLAN, click **Membership**.

5 Select a Primary VLAN ID.

6 Select an Isolated VLAN ID.

7 Select the ports to be assigned to each VLAN, and assign each port/LAG a port type in the Admin row of ports/LAGs. Click on a port to toggle through the various options. The possible options are:

- **H - Host (Isolated)** — Port is isolated.
- **P - Promiscuous** — Port is promiscuous.
- **C - Conditional (operational state depends on Port VLAN Mode)** — Port receives the Port VLAN type set in the **VLAN Port Settings** page.

See Port Modes for a description of the various port modes.

Configuring Private VLAN Using CLI Commands

The following table summarizes the CLI commands for configuring private VLANs.

Table 14-6. Private VLAN CLI Commands

CLI Command	Description
private-vlan {*primary*|*isolated*} **no private-vlan**	Configures a private VLAN. Use the no form of this command to return the VLAN to normal VLAN configuration.
private-vlan association [***add***|***remove***] *secondary-vlan-list*	Configures the association between the primary VLAN and the secondary VLANs.
no private-vlan association	Use the no form of this command to remove the association.

Table 14-6. Private VLAN CLI Commands *(continued)*

CLI Command	Description
switchport private-vlan mapping *primary-vlan-id* [**add**|**remove**] *secondary-vlan-list* **no switchport private-vlan mapping**	Configures the VLANs of the private-vlan promiscuous port. Use the no form of this command to reset to default
switchport private-vlan host-association *primary-vlan-id secondary-vlan-id* **no switchport private-vlan host-association**	Configures the VLANs of the private-vlan host port. Use the no form of this command to reset to default.
show vlan private-vlan [**tag** *vlan-id*]	Displays private VLAN information.

The following is an example of the CLI commands:

```
console# show vlan private-vlan
Primary    Secondary   Type         Ports
--------   ---------   ----------   ---------------------
20                     Primary      gi0/1-2
20         201         Isolated     gi0/1-8
20         202         Isolated    gi0/1-2 gi0/5-7
20         203         Isolated    gi0/1-2 gi0/2-3
```

Voice VLAN

This section describes voice VLAN. It covers the following topics:

- Overview
- Properties
- Port Setting
- OUI

Overview

The Voice VLAN feature enables you to enhance VoIP service by configuring ports to carry IP-voice traffic from IP phones on a specific VLAN. This VLAN is configured with a QoS profile that ensures high voice quality.

Equipment, such as VOIP phones, transmits IP traffic with a pre-configured Organizational Unique Identifier (OUI) prefix in the source MAC address. This enables the switch to dynamically identify ports connected to the VoIP equipment and automatically add these ports to the Voice VLAN.

IP phones use one of the following modes, both of which are supported by the device:

- Use only tagged packets for all communications.
- Initially use untagged packets while retrieving the initial IP address through DHCP. Then the phone uses the Voice VLAN and starts sending tagged VoIP packets.

Non-VoIP traffic is dropped from the Voice VLAN when the device is in Auto Voice VLAN secured mode.

The Voice VLAN feature also provides QoS actions to VoIP, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly.

To summarize, when Voice VLAN is enabled and configured, and VoIP equipment is connected to one of the switch ports, the VoIP traffic triggers the switch's Voice VLAN feature to add this port to the Voice VLAN (a VLAN that usually carries only voice traffic), and to assign traffic from this port a specific QoS profile, ensuring high voice quality.

The device supports a single voice VLAN.

Properties

To set voice VLAN parameters that apply to the voice VLAN on the device:

1. Click **Switching > VLAN > Voice VLAN > Properties** in the tree view to display the **Properties** page.
2. Enter the fields:
   - **Voice VLAN State** — Select **Enable** to use the Voice VLAN feature on the device.
   - **Voice VLAN ID** — Select the VLAN that is to be the voice VLAN.

- **Class of Service** — Select to add a CoS level to untagged packets, received on the voice VLAN. The possible values are 0 to 7, where 7 is the highest priority. 0 is used as a best-effort, and is invoked automatically when no other value has been set.
- **Remark CoS** — Select Enable to use the Remark CoS feature.
- **Voice VLAN Aging Time** — Enter the interval of time after which the port exits the voice VLAN, if no voice packets are received.

  The aging time starts after the MAC address is aged out from the Dynamic MAC Address table. The default time is 300 sec. For more information on defining MAC address age out time, see Dynamic Address Table.

Defining Voice VLAN Properties Using CLI Commands

The following table summarizes the CLI command for defining voice VLAN properties.

Table 14-7. Voice VLAN Properties CLI Commands

CLI Command	Description
**`voice vlan state{oui-enabled	disabled]`**	Sets the type of voice VLAN that is functional on the device.
`no voice vlan state`	Use the no form of this command to disable voice VLAN entirely.

`voice vlan id` *`vlan-id`*
 `no voice vlan id`
	Enables the voice VLAN and configures the voice VLAN ID in Global Configuration mode.
	 Use the no form of this command to disable voice VLAN.

`voice vlan cos` *`cos`* `[`***`remark`***`]`
 `no voice vlan cos`
	Sets the voice VLAN Class of Service (CoS) queue.
	 Use the no form of this command to restore the default configuration.

`voice vlan aging-timeout` *`minutes`*	Sets the voice VLAN aging timeout in Global Configuration mode.
`no voice aging-timeout`	Use the no form of this command to return to default.

Table 14-7. Voice VLAN Properties CLI Commands *(continued)*

CLI Command	Description
show voice vlan [**type oui**] [interface-id|**detailed**]	Use the show voice vlan EXEC command to display the voice VLAN status.

The following is an example of some of the CLI commands:

```
console# show          voice vlan
Aging timeout:         1440 minutes
OUI table
MAC Address Prefix     Description
00:E0:BB               3COM
00:03:6B               Cisco
00:E0:75               Veritel
00:D0:1E               Pingtel
00:01:E3               Siemens
00:60:B9               NEC/Philips
00:0F:E2               Huawei-3COM
00:09:6E               Avaya
Voice VLAN VLAN ID: 8
CoS: 6
Remark: Yes
Interface              Enabled         Secure   Activated
---------              --------        ------   ---------
gi0/1                  Yes             Yes      Yes
gi0/2                  Yes             Yes      Yes
gi0/3                  Yes             Yes      Yes
gi0/4                  Yes             Yes      Yes
```

Port Setting

To configure voice VLAN ports properties:

1. Click **Switching > VLAN > Voice VLAN > Port Setting** in the tree view to display the **Port Setting: Summary** page.

   A list of the ports and their voice VLAN settings is displayed.

2. To modify the voice VLAN settings for an interface, click **Edit**, and enter the fields:

   – **Interface** — Enter the specific port or LAG to which the Voice VLAN settings are applied.

   – **Voice VLAN Mode** — Select the Voice VLAN mode. The possible options are:

     - **None** — Disables the selected port/LAG on the Voice VLAN. This is the default.
     - **Static** — Statically adds the port to the Voice VLAN. This is usually done for VoIP uplink ports that connect the device to VoIP PBX, for example.
     - **Auto** — Indicates that if traffic with an IP phone MAC address is transmitted on the port/LAG, the port/LAG joins the Voice VLAN. The port/LAG is aged out of the voice VLAN if the IP phone's MAC address (with an OUI prefix) is aged out. If the MAC address of the IP phones OUI was added manually to a port/LAG in the voice VLAN, the user cannot add it to the Voice VLAN in Auto mode, only in Static mode.

   – **Voice VLAN Security** — Enable/disable security on the interface. Security ensures that packets arriving with an unrecognized OUI are dropped (for example data packets).

Defining Voice VLAN Port Settings Using CLI Commands

The following table summarizes the CLI command for defining Voice VLAN port settings.

Table 14-8. Voice VLAN Port Settings CLI Commands

CLI Command	Description
voice vlan enable	Enables OUI voice VLAN on a port.
no voice vlan enable	Use the no form of this command to disable OUI voice VLAN on a port.
voice vlan secure **no voice vlan secure**	Specifies that packets that are classified to the voice VLAN with a source MAC address that is not a OUI address (defined by Voice Vlan OUI table) are discarded. Use the no form of this command to disable secure mode.

The following is an example of the CLI commands:

```
console# voice vlan state oui-enabled
console(config)# interface gi0/1
switchport trunk allowed remove vlan 8
console(config-if)# voice vlan enable
console(config-if)# voice vlan secure
console(config-if)#
```

OUI

Organizationally Unique Identifiers (OUIs) are a 24-bit numbers assigned by the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority to equipment manufacturers.

Up to 128 OUIs can be stored on the switch. Nine specific OUIs of popular VoIP phones manufacturers are stored by default.

Traffic from each type of IP phone contains the OUI for the phone manufacturer. When frames are received, in which the source MAC address’s first three octets match one of the OUIs in the OUI list, the port on which they are received is automatically assigned to the Voice VLAN.

To view existing OUIs, and add new OUIs:

1. Click **Switching** > **VLAN** > **Voice VLAN** > **OUI** in the tree view to display the **OUI Summary**.

   The previously-defined OUIs are displayed.

2. To add a new OUI, click **Add**, and enter the fields:

   – **Telephony OUI** — Enter a new OUI.

   – **Description** — Enter an OUI description up to 32 characters.

Defining Voice VLAN OUIs Using CLI Commands

The following table summarizes the CLI command for defining Voice VLAN OUIs.

Table 14-9. Voice VLAN OUIs CLI Commands

CLI Command	Description
voice vlan oui-table {***add*** *mac-address-prefix*|***remove*** *mac-address-prefix*} [*text*]	Configures the voice OUI table. Use the no form of this command to restore the default configuration.
no voice vlan oui-table	

The following is an example of the CLI commands:

```
console(config)# voice vlan oui-table add 00:E0:BB
console(config)#
```

15

Link Aggregation

This section describes link aggregation of ports.

It contains the following topics:

- Overview
- LACP Parameters
- LAG Membership

Overview

Link Aggregation optimizes port usage by linking a group of ports together to form a single LAG (aggregated group). Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

The device supports the following types of LAGs:

- **Static LAGs** — Manually-configured LAGs.
- **Link Aggregation Control Protocol (LACP) LAGs** — LACP LAGs negotiate aggregating a port's links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establishes a LAG between them.

When you aggregate ports, the ports and LAG must fulfill the following conditions:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to another LAG.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.

- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to 32 LAGs, and eight ports in each LAG.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports.

The device uses a hash function to assign packets to a LAG member. The hash function statistically load-balances the aggregated link members. The device considers an Aggregated Link to be a single logical port.

Aggregate ports can be linked into link-aggregation port-groups. Each group comprises ports with the same speed, set to full-duplex operations.

Ports in a LAG can contain different media types if the ports are operating at the same speed. Aggregated links can be manually or automatically configured by enabling LACP on the relevant links.

LACP Parameters

To define LACP LAGs, configure LACP global and port parameters, such as LACP system priority, timeout, and port priority.

With all factors equal, when the LAG is configured with more candidate ports than the maximum number of active ports allowed, the switch activates the highest priority candidate ports from the dynamic LAG.

To set LACP parameters:

1. Click **Switching > Link Aggregation > LACP Parameters** in the tree view to display the **LACP Parameters** page.

   The LACP parameters for all ports are displayed.

2. Enter the global **LACP System Priority** (1-65535) value that determines which candidate ports will become members of the LAG.

   The page displays the LACP settings of the ports.

3 To modify LACP parameters for a particular port, click **Edit**, and enter the following fields:

- **Select a Port** — Select the port for which timeout and priority values are assigned.
- **LACP Port Priority (1-65535)** — Enter the LACP priority value for the port.
- **LACP Timeout** — Select the rate of periodic transmissions of LACP PDUs. The possible options are:
  - **Long** — Slow transmission rate
  - **Short** — Fast transmission rate

Configuring LACP Parameters Using CLI Commands

The following table summarizes the CLI commands for configuring LACP parameters as displayed in the **LACP Parameters** page.

Table 15-1. LACP Parameters CLI Commands

CLI Command	Description

`lacp system-priority` *`value`*
`no lacp system-priority`
	Configures the system priority.
	Use the no form of this command to restore the default configuration.

`lacp port-priority` *`value`*
`no lacp port-priority`
	Configures the priority value for physical ports.
	Use the no form of this command to restore the default configuration.

`lacp timeout` `{`***`long`***` `**`|`**` `***`short`***`}`
`no lacp timeout`
	Assigns an administrative LACP timeout.
	Use the no form of this command to restore the default configuration.

`show lacp` *`interface-id`* `[`***`parameters`***` | `***`statistics`***` | `***`protocol-state`***`]`	Displays LACP information for ethernet ports.

The following is an example of the CLI commands:

```
console (config)# lacp system-priority 120
console (config)# interface gi0/8
console (config-if)# lacp port-priority 247
console (config-if)# lacp timeout long
console (config-if)# end
console# show lacp gi0/8 statistics
Port gi0/7 LACP Statistics:
LACP PDUs sent:2
LACP PDUs received:2
```

LAG Membership

Each device supports up to 32 LAGs per system, and eight ports per LAG.

When you add a port to a LAG, the port acquires the LAG's properties. If the port cannot be configured with the LAG's properties, it is not added to the LAG and an error message is generated.

If the first port joining the LAG cannot be configured with the LAG settings, the port is added to the LAG, using the port default settings, and an error message is generated. Since this is the only port in the LAG, the entire LAG operates with the port's settings, instead of the LAG's defined settings.

To assign ports to LAGs:

1. Click **Switching** > **Link Aggregation** > **LAG Membership** in the tree view to display the **LAG Membership: Summary** page.

   The LACP and static LAGs are displayed along with their member ports.

   This page displays the following fields:

   – **LACP** — Aggregates the port to a LAG, using LACP.

   – **LAG** — Adds a port to a LAG, and indicates the specific LAG to which the port belongs.

2. Click **Edit** to change the status of a port in a LAG.

3. Select the LAG.

4 In the LACP row (the first row), toggle the button under the port number to assign either the LACP or the static LAG.

5 In the LAG row (the second row), toggle the button to a specific number to aggregate or remove the port to that LAG number.

Adding Ports to LAGs Using CLI Commands

The following table summarizes the CLI commands for assigning ports to LAGs as displayed in the **LAG Membership** pages.

Table 15-2. LAG Membership CLI Commands

CLI Command	Description
channel-group *port-channel* ***mode*** {***on*** **|** ***auto***}	Associates a port with a port-channel with or without a LACP operation.
no channel-group	Use the no form of this command to remove the channel-group configuration from the interface.
show interfaces port-channel [*interface-id*]	Displays port-channel information for all port channels or for a specific port channel.

The following is an example of the CLI commands:

```
console(config)# interface gi0/8
console(config-if)# channel-group 1 mode on
```

16

Multicast Support

This chapter describes Multicast support on the device.

It contains the following topics:

- Overview
- Global Parameters
- Bridge Multicast Groups
- Bridge Multicast Forward All
- IGMP Snooping
- MLD Snooping
- Unregistered Multicast
- Multicast TV VLAN

Overview

Multicast forwarding enables a single packet to be forwarded to multiple destinations. Layer 2 Multicast service is based on a Layer 2 device receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

There are two types of Multicast groups:

- **Registered Multicast Group** — When traffic addressed to a registered Multicast group is received, it is handled according to its entry in the Multicast Filtering Database and forwarded only to the registered ports.
- **Unregistered Multicast Group** — If traffic addressed to an unregistered Multicast group is received, it is handled by a special entry in the Multicast Filtering Database. The default setting of this is to flood all such traffic (traffic in unregistered Multicast groups).

The device supports:

- **Forwarding L2 Multicast Packets** — Forwards Layer 2 Multicast packets. Layer 2 Multicast filtering is enabled by default, and is not user-configurable.
- **Filtering L2 Multicast Packets** — Forwards Layer 2 packets to interfaces. If Multicast filtering is disabled, Multicast packets are flooded to all relevant ports.

NOTE: The system supports Multicast filtering for 256 Multicast groups.

Layer 2 Switching

Layer 2 switching forwards Multicast packets to all relevant VLAN ports by default, managing the packet as a single Multicast transmission. While Multicast traffic forwarding is effective, it is not optimal, as irrelevant ports also receive the Multicast packets. The excess packets cause increased network traffic. Multicast forwarding filters enable forwarding of Layer 2 packets to a subset of ports instead of to all ports.

IGMP Snooping

Internet Group Multicast Protocol (IGMP) adds IGMP packets to Multicast traffic. When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.
- What routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that the Multicast group is accepting members. This results in the creation of an entry in the Multicast filtering database.

MLD Snooping

Hosts use the MLD protocol to report their participation in Multicast sessions, and the device uses MLD snooping to build Multicast membership lists. It uses these lists to forward Multicast packets only to device ports where there are host nodes that are members of the Multicast groups. The device does not support MLD Querier.

Hosts use the MLD protocol to report their participation in Multicast sessions.

The device supports two versions of MLD snooping:

- MLDv1 snooping detects MLDv1 control packets, and sets up traffic bridging, based on IPv6 destination Multicast addresses.
- MLDv2 snooping uses MLDv2 control packets to forward traffic based on the source IPv6 address, and the destination IPv6 Multicast address.

The actual MLD version is selected by the Multicast router in the network.

In an approach similar to IGMP snooping, MLD frames are snooped as they are forwarded by the device from stations to an upstream Multicast router and vice versa. This facility enables a device to conclude the following:

- On which ports stations interested in joining a specific Multicast group are located
- On which ports Multicast routers sending Multicast frames are located

This knowledge is used to exclude irrelevant ports (ports on which no stations

have registered to receive a specific Multicast group) from the forwarding set of an incoming Multicast frame.

If you enable MLD snooping in addition to the manually-configured Multicast groups, the result is a union of the Multicast groups and port memberships derived from the manual setup and the dynamic discovery by MLD snooping. Only static definitions are preserved when the system is rebooted.

Global Parameters

To enable Multicast filtering and IGMP Snooping:

1 Click **Switching** > **Multicast Support** > **Global Parameters** in the tree view to display the **Global Parameters** page.

2 Enter the fields:

- **Bridge Multicast Filtering** — Enable/disable Multicast filtering. Enabled is the default value.
- **IGMP Snooping Status** — Enable/disable IGMP Snooping on the device. Disabled is the default value.
- **IGMP Querier Status**— Enable/disable IGMP Querier. Disabled is the default value. Enable IGMP querier if IGMP snooping is enabled. IGMP querier fills the tables used by IGMP snooping.
- **MLD Snooping Status** — Enable/disable MLD Snooping on the device. Disabled is the default value.
- **MLD Querier Status** — Enable/disable MLD Querier on the device. Disabled is the default value. Enable MLD querier if MLD snooping is enabled. MLD querier fills the tables used by MLD snooping.
- **VLAN ID**— Select the VLAN ID whose forwarding method is set in the next fields.
- **Forwarding Method for IPv6**—Set one of the following forwarding methods for IPv6 addresses: **MAC Group Address**, **IP Group Address**, or **Source Specific IP Group Address**.
- **Forwarding Method for IPv4**—Set one of the following forwarding methods for IPv4 addresses: **MAC Group Address**, **IP Group Address**, or **Source Specific IP Group Address.**

Enabling Multicast Filtering and IGMP Snooping Using CLI Commands

The following table summarizes the CLI commands for enabling Multicast Filtering and IGMP snooping as displayed on the **Global Parameters** page.

Table 16-1. Multicast Filtering and Snooping CLI Commands

CLI Command	Description
bridge multicast filtering	Enables filtering of Multicast addresses.
no bridge multicast filtering	Use the no form of this command to disable Multicast address filtering.
ip igmp snooping	Enables IGMP Snooping.
no ip igmp snooping	Use the no form of this command to disable IGMP Snooping.
ip igmp snooping vlan vlan-id querier **version** *{2 | 3}*	Configures the IGMP version of an IGMP Snooping querier on a specific VLAN.
no ip igmp snooping vlan *vlan-id* **querier version**	Use the no form of this command to disable IGMP Snooping.
ipv6 mld snooping querier	Enables MLD Snooping querier.
no ipv6 mld snooping querier	Use the no form of this command to disable IGMP Snooping querier.
ipv6 mld snooping	Enables MLD Snooping.
no ipv6 mld snooping	Use the no form of this command to disable MLD Snooping.
ipv6 mld snooping vlan ***vlan-id***	Enables MLD Snooping on a specific VLAN.
no ipv6 mld snooping vlan ***vlan-id***	Use the no form of this command to disable MLD Snooping on a specific VLAN.
bridge multicast mode {mac-group | ip-group | ip-src-group}	Configures the Multicast bridging mode.
no bridge multicast mode	Use the no form of this command to return to the default configuration

The following is an example of the CLI commands:

```
console(config)# bridge multicast filtering
console(config)# ip igmp snooping
console(config) ipv6 mld snooping
```

Bridge Multicast Groups

The **Bridge Multicast Group: Summary** page displays the ports and LAGs attached to a Multicast service group and the manner in which the port or LAG joined it.

To add and configure a Multicast group:

1. Click **Switching > Multicast Support > Bridge Multicast Group** in the tree view to display the **Bridge Multicast Group: Summary** page.

   The ports and LAGs in the selected Multicast Group are displayed.

2. Select a VLAN and enter the Multicast group IP address in **Bridge Multicast Address**.

   Two rows of ports and LAGs are displayed:

   – **Static** — Displays available static ports/LAGs. These port/LAGs can be included or excluded from the Multicast groups, as described below.

   – **Current** — Displays status of ports/LAGs in the Multicast group, as actually applied.

3. For each port in the VLAN, toggle to **S** to join the port to the selected Multicast group as a static port. Toggle a port to **F** to indicate that it is **Forbidden** to this group. Leave the field empty if it is not involved in the VLAN.

4. To add a new Multicast group, click **Add**, and enter the fields:

   – **IP Format**— Select whether this is an IPv4 or IPv6 group.

   – **VLAN ID** — Select the VLAN ID to set its forwarding method.

   – **New Bridge IP Multicast** — Enter a Multicast group IP address.

   – **New Bridge MAC Multicast** — Enter a Multicast group MAC address.

– **Source IP Address**— Enter the source IP address to be used in outgoing packets.

– **Ports** — Select the ports to be added to a Multicast service. Toggle a port to **S** to join the port to the selected Multicast group as a static port. Toggle a port to **F** to indicate that it is **Forbidden** to this service. Leave the field empty if it is not involved in the VLAN.

– **LAGs** — Select the LAGs to be added to a Multicast service. Toggle a LAG to **S** to join the port to the selected Multicast group as a static LAG. Toggle a port to **F** to indicate that it is **Forbidden** to this service. Leave the field empty if it is not involved in the VLAN.

The following table describes the codes used for the interface in this page:

Table 16-2. IGMP Port/LAG Members Table Control Settings

Port Control	Definition
S	Attaches the port to the Multicast group as static member in the static row. The port/LAG has joined the Multicast group statically in the current row.
F	Forbidden. The port cannot belong to the Multicast group.
Blank	The port is not attached to a Multicast group, but it is also not forbidden.

Managing Bridge Multicast Groups Using CLI Commands

The following table summarizes the CLI commands for managing Multicast service members as displayed in the **Bridge Multicast Group** pages.

Table 16-3. Bridge Multicast Group CLI Commands

CLI Command	Description
bridge multicast address {*mac-multicast-address* | *ipv4-multicast-address*} [[**add** | **remove**] {**ethernet** interface-list | **port-channel** port-channel-list}] **no bridge multicast filtering** {mac-multicast-address}	Registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group. Use the no form of this command to disable Multicast address filtering.
bridge multicast forbidden address {*mac-multicast-address* | *ipv4-multicast-address*} [***add*** | ***remove***] {[***ethernet*** *interface-list* | ***port-channel*** *port-channel-list*} **no bridge multicast forbidden address** {*mac-multicast-address*}	Forbids adding a specific Multicast address to specific ports. Use the no form of this command to return to default Use the no form of this command to restore the default configuration.
bridge multicast source *ip-address* **group** *ip-multicast-address* [[***add*** | ***remove***] {***ethernet*** *interface-list* | ***port-channel*** *port-channel-list*}] **no bridge multicast source** *ip-address* ***group*** *ip-multicast-address*	Registers a source IP address - Multicast IP address pair to the bridge table, and statically adds or removes ports to or from the source-group. Use the no form of this command to unregister the source-group-pair.
show bridge multicast address-table [***vlan*** *vlan*-id] [***address*** {*mac-multicast-address* | *ipv4-multicast-address* | *ipv6-multicast-address*}] [***format*** {**ip** | **mac**}]	Displays Multicast MAC address table information.

The following is an example of the CLI commands:

```
console(config-if)# bridge multicast address 0100.5e02.0203
add gi0/7,gi0/8
console(config-if)# end
console # show bridge multicast address-table

VLAN      MAC Address            Type               Ports
----      -----------            -----              ----------
1         0100.5e02.0203         static             gi0/5, gi0/6
Forbidden ports for multicast addresses:
VLAN      MAC Address            Ports
----      -----------            ----------
1         0100.5e02.0203         gi0/8
19        0100.5e02.0208         gi0/8

console # show bridge multicast address-table format ip

VLAN      IP Address             Type               Ports
----      -----------            -----              ----------
1         224-239.130.2.2.3      static             gi0/3, gi0/4

Forbidden ports for multicast addresses:

VLAN      IP Address             Ports
----      -----------            ----------
1         224-239.130.2.2.3      gi0/8
```

Bridge Multicast Forward All

Use the **Bridge Multicast Forward All** page to attach ports or LAGs to a device that is attached to a neighboring Multicast router/switch. After IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN.

To attach interfaces to a Multicast service:

1. Click **Switching** > **Multicast Support** > **Bridge Multicast Forward All** in the tree view to display the **Bridge Multicast Forward All** page.
2. Select a VLAN and click on the ports and LAGs to be attached to the Multicast service. Toggle a port to **S** to join the port to the selected Multicast group as a static port. Toggle a port to **F** to add it as a Forbidden port.

   Two rows of ports and LAGs are displayed:

   – **Static** — Displays available static ports/LAGs. These port/LAGs can be included or excluded from the Multicast groups, as described below.

   – **Current** — Displays status of ports/LAGs, as actually applied, in the Multicast group.

Managing LAGs and Ports Attached to Multicast Routers Using CLI Commands

The following table summarizes the CLI commands for managing LAGs and ports attached to Multicast routers as displayed on the **Bridge Multicast Forward All** page.

Table 16-4. Managing LAGs and Ports Attached to Multicast Routers CLI Commands

CLI Command	Description
show bridge multicast filtering *vlan-id*	Displays the Multicast filtering configuration.
bridge multicast forward-all {add | remove} {*ethernet* interface-list **| *port-channel*** *port-channel-list*}	Enables forwarding of all Multicast packets on a port. Use the no form of this command to return to default.

The following is an example of the CLI commands:

```
console(config)# interface vlan 1
console(config-if)# bridge multicast forward-all add
gi0/3
console(config-if)# end
console# show bridge multicast filtering 1
```

```
Filtering: Enabled
VLAN:           Forward-All
Port            Static                 Status
-------         -----------------      -----------
gi0/3           Forbidden              Filter
gi0/4           Forward                Forward(s)
gi0/5           -                      Forward(d)
```

IGMP Snooping

IGMP Snooping can be enabled globally, as described in the **Global Parameters** page. It can also be enabled per VLAN to support selective IPv4 Multicast forwarding. In this case, Bridge Multicast filtering must also be enabled.

By default, a Layer 2 switch forwards Multicast frames to all ports of the relevant VLAN, essentially treating the frame as if it were a Broadcast. When IGMP Snooping is enabled per VLAN, the switch forwards Multicast frames to ports that have registered as Multicast clients in the VLAN.

NOTE: The switch supports IGMP Snooping only on static VLANs. It does not support IGMP Snooping on dynamic VLANs.

The IGMP Snooping Querier is used to support a Layer 2 Multicast domain of snooping switches in the absence of a Multicast router, for example, where Multicast content is provided by a local server, but the router (if one exists) on that network does not support Multicast.

There should only be a single IGMP Querier in a Layer 2 Multicast domain. The switch supports standards-based IGMP Querier election when more than one IGMP Querier is present in the domain.

The speed of IGMP Querier activity should be aligned with the IGMP-snooping-enabled switches. Queries should be sent at a rate that is aligned to the snooping table aging time. If queries are sent at a rate lower than the aging time, the subscriber cannot receive the Multicast packets.

To enable IGMP Snooping on a VLAN:

1 Click **Switching** > **Multicast Support** > **IGMP Snooping** in the tree view to display the **IGMP Snooping** page.

  The IGMP snooping information for the VLANs on the switch is displayed.

2 To enable IGMP Snooping on a VLAN, click **Edit** and select the VLAN from the **VLAN ID** drop down menu.

3 Enter the fields:

  - **IGMP Snooping Status** — Enable/disable the monitoring of network traffic to determine which hosts have asked to be sent Multicast traffic. The switch performs IGMP snooping only if IGMP snooping and Bridge Multicast filtering are both globally enabled.
  - **Operational IGMP Snooping Status** — Displays whether IGMP Snooping is enabled.
  - **MRouter Ports Auto Learn** — Enables or disables auto learning of the ports to which the Mrouter is connected.
  - **Query Robustness** (1-7) — Enter the Robustness variable value to be used. The Robustness value enables tuning for the expected packet loss on a link. If a link is expected to have losses, the Robustness Value may be increased.
  - **Operational Query Robustness** — Displays the robustness variable sent by the elected querier.
  - **Query Interval** (30-18000) — Enter the interval between general queries sent by the querier.
  - **Operational Query Interval** — The time interval in seconds between general queries sent by the elected querier
  - **Query Max Response Interval** (5-20) — Enter the amount of time in which a host should respond to a query.
  - **Operational Max Response Interval** — Displays the actual delay.
  - **Last Member Query Counter** (1-7) — Enter the number of IGMP group-specific queries sent before the switch assumes there are no local members. To use the default, check **Use Default**.

- **Operational Last Member Query Counter** — Displays the operational value of the Last Member Query counter.
- **Last Member Query Interval** (100-25500) **—** Enter the time between two consecutive group-specific queries that are sent by the querier.
- **Operational Last Member Query Interval —** Displays the Last Member Query Interval sent by the elected querier.
- **Intermediate Leave** — Enable/disable an immediate timeout period. The default timeout is 10 seconds.
- **IGMP Querier Status** — Enables or disables the IGMP Querier. The IGMP Querier simulates the behavior of a Multicast router, enabling snooping of the Layer 2 Multicast domain even though there is no Multicast router.
- **IGMP Querier Version** — Select the version of IGMP snooping querier to be used.
- **Querier Source IP Address** — Select the IP address of the IGMP Querier. Use either the VLAN's IP address or define a unique IP address that will be used as a source address of the querier.
- **Operational Source Querier IP Address** — Operational Querier IP address.

Configuring IGMP Snooping Using CLI Commands

The following table summarizes the CLI commands for configuring IGMP snooping on a VLAN:

Table 16-5. IGMP Snooping CLI Commands

CLI Command	Description
ip igmp snooping vlan *vlan-id* **no ip igmp snooping vlan** *vlan-id*	Enables IGMP snooping on a specific VLAN. Use the no form of this command to disable IGMP snooping on a VLAN interface.

Table 16-5. IGMP Snooping CLI Commands *(continued)*

CLI Command	Description
ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp** **no ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	Enables automatic learning of Multicast router ports in the context of a specific VLAN. Use the no form of this command to remove the configuration.
ip igmp robustness *count* **no ip igmp robustness**	Changes the value of the IGMP robustness variable. Use the no format of the command to return to default.
ip igmp query-interval *seconds* **no ip igmp query-interval**	Configures the Query interval. Use the no format of the command to return to default.
ip igmp query-max-response-time *seconds* **no ip igmp query-max-response-time**	Configures the Query Maximum Response time. Use the no format of the command to return to default.
ip igmp last-member-query-count *count* **no ip igmp last-member-query-count**	Configures the Last Member Query Counter. Use the no format of the command to return to default.
ip igmp snooping vlan *vlan-id* **immediate-leave** **no ip igmp snooping vlan** *vlan-id* **immediate-leave**	Enables the IGMP Snooping Immediate-Leave processing on a VLAN. Use the no format of the command to disable IGMP Snooping Immediate-Leave processing.
ip igmp snooping vlan *vlan-id* **querier** **no ip igmp snooping vlan** *vlan-id* **querier**	Enables the IGMP querier on a specific VLAN. Use the no form of this command to disable the IGMP querier on a VLAN interface.

Table 16-5. IGMP Snooping CLI Commands *(continued)*

CLI Command	Description
ip igmp snooping vlan *vlan-id* **querier address** *ip-address*	Defines the source IP address that the IGMP Snooping querier would use.
no ip igmp snooping vlan vlan-id **querier address**	Use the no form of this command to return to default.
show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*] [*source ip-address*]	Displays the Multicast groups learned by IGMP snooping.
show ip igmp snooping interface *vlan-id*	Displays IGMP snooping configuration.
show ip igmp snooping mrouter [**interface** *vlan-id*]	Displays information about dynamically learned Multicast router interfaces.

The following is an example of the CLI commands:

```
console (config)# ip igmp snooping
console (config)# interface vlan 1
console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
console (config)# interface vlan 1
console (config-if)# ip igmp snooping leave-time-out 60
console # do show ip igmp snooping groups
VLAN IP Address       Querier     Ports
---- ----------       ------      ----------------------
1    224-239.130      |2.2.3 Yes  gi0/1, gi0/2
console # show ip igmp snooping interface 1
IGMP Snooping is globally disabled
IGMP Snooping admin: Enabled
IGMP Snooping oper mode: Disabled
Routers IGMP version: 3
IGMP snooping querier admin: disabled
IGMP snooping querier oper: disabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 10.5.234.232
IGMP snooping robustness: admin 2  oper 2
IGMP snooping query interval: admin 125 sec oper 125 sec
IGMP snooping query maximum response: admin 10 sec oper 10 sec
IGMP snooping last member query counter: admin 2  oper 2
IGMP snooping last member query interval: admin 1000 msec oper
1000 msec
IGMP snooping last immediate leave:  disable
Automatic learning of Multicast router ports is enabled
```

MLD Snooping

To enable MLD Snooping and configure it on a VLAN:

1. Click **Switching > Multicast Support > MLD Snooping**.
2. Enable or disable **MLD Snooping Status.** When MLD Snooping is globally enabled, the device monitoring network traffic can determine which hosts have requested to receive Multicast traffic. The device performs MLD Snooping only if both MLD snooping and Bridge Multicast filtering are enabled.
3. Click **Edit** and enter the parameters.
   - **VLAN ID**—Select the VLAN ID.
   - **MLD Snooping Status**—Enable or disable MLD snooping on the VLAN. The device monitors network traffic to determine which hosts have asked to be sent Multicast traffic. The device performs MLD snooping only when MLD snooping and Bridge Multicast filtering are both enabled
   - **Operational MLD Snooping Status**—Displays the current status of MLD Snooping for the selected VLAN.
   - **MRouter Ports Auto-Learn**—Enable or disable Auto Learn for the Multicast router.
   - **Query Robustness (1-7)**—Enter the robustness variable value to be used if the device cannot read this value from messages sent by the elected querier.
   - **Operational Query Robustness**—Displays the robustness variable sent by the elected querier.
   - **Query Interval (30-18000)**—Enter the Query Interval value to be used by the device if the device cannot derive the value from the messages sent by the elected querier.
   - **Operational Query Interval**—The time interval in seconds between General Queries received from the elected querier.
   - **Query Max Response Interval (5-20)**—Enter Query Max Response delay to be used if the device cannot read the Max Response Time value from General Queries sent by the elected querier.

- **Operational Query Max Response Interval**—Displays the delay used to calculate the Maximum Response Code inserted into the General Queries.
- **Last Member Query Counter** (**1-7**)—Enter the Last Member Query Count to be used if the device cannot derive the value from the messages sent by the elected querier.
- **Operational Last Member Query Counter**—Displays the operational value of the Last Member Query Counter.
- **Last Member Query Interval** (**100-25500**)—Enter the Maximum Response Delay to be used if the device cannot read Max Response Time value from Group-Specific queries sent by the elected querier.
- **Operational Last Member Query Interval**—The Last Member Query Interval sent by the elected querier.
- **Immediate Leave**—When enabled, reduces the time it takes to block unnecessary MLD traffic sent to a device port.
- **MLD Querier Status**—Enable or disable MLD querier.
- **MLD Querier Election**—Enable or disable MLD election.
- **MLD Querier Version**—Select the MLD querier version.

4 Click **Apply**. The Running Configuration file is updated.

Configuring IGMP Snooping Using CLI Commands

The following table summarizes the CLI commands for configuring IGMP snooping on a VLAN:

Table 16-6. IGMP Snooping CLI Commands

CLI Command	Description
ipv6 mld snooping	Enables MLD Snooping.
no ipv6 mld snooping	Use the no form of this command to disable MLD Snooping.
ipv6 mld snooping vlan ***vlan-id*** **no ipv6 mld snooping vlan** ***vlan-id***	Enables MLD Snooping on a specific VLAN. Use the no form of this command to disable MLD Snooping on a specific VLAN.
ipv6 mld snooping querier	Enables MLD Snooping querier.
no ipv6 mld snooping querier	Use the no form of this command to disable IGMP Snooping querier.
ipv6 mld robustness *count* **no ipv6 mld robustness**	Changes the value of the MLD robustness variable. Use the no format of the command to return to default.
ipv6 mld snooping vlan *vlan-id* **mrouter learn** ***pim-dvmrp***	Enables automatic learning of Multicast router ports.
no ipv6 mld snooping vlan *vlan-id* **mrouter learn** ***pim-dvmrp***	Use the no format of the command to return to default.
ipv6 mld query-interval *seconds* **no ipv6 mld query-interval**	Configures the Query interval. Use the no format of the command to return to default.
ipv6 mld query-max-response-time *seconds*	Configures the Query Maximum Response time.
no ipv6 mld query-max-response-time	Use the no format of the command to return to default.

Table 16-6. IGMP Snooping CLI Commands *(continued)*

CLI Command	Description
ipv6 mld last-member-query-count *count*	Configures the Last Member Query Counter.
no ipv6 mld last-member-query-count	Use the no format of the command to return to default.
ipv6 mld last-member-query-interval *milliseconds*	Configures the Last Member Query Interval.
no ipv6 mld last-member-query-interval	Use the no format of the command to return to default.
ipv6 mld snooping vlan *vlan-id* **immediate-leave** **no ipv6 mld snooping vlan** *vlan-id* **immediate-leave**	Enables the MLD Snooping Immediate-Leave processing on a VLAN. Use the no format of the command to disable MLD Snooping Immediate-Leave processing.
show ipv6 mld snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*] [*source ip-address*]	Displays the Multicast groups learned by MLD snooping.
show ipv6 mld snooping interface *vlan-id*	Displays MLD snooping configuration.
show ip igmp snooping mrouter [**interface** *vlan-id*]	Displays information about dynamically learned Multicast router interfaces.

The following is an example of the CLI commands:

```
console (config)# ip mld snooping
console (config)# interface vlan 1
console (config-if)# ipv6 mld robustness 3
console (config-if)# ipv6 mld snooping mrouter learn-pim-dvmrp
console (config-if)# ipv6 mld snooping leave-time-out 60
```

.

```
console# show ipv6 mld snooping groups
VLAN  Group     Source Address             Include   Exclude   Compatibility
----  Address   ---------------------      Ports     Ports     Mode
1     -------   FE80::201:C9FF:FE40:8001   ------    -------   -------------
1     FF12::3   FE80::201:C9FF:FE40:8002   te1                 1
19    FF12::3   FE80::201:C9FF:FE40:8003   te2                 1
19    FF12::8   FE80::201:C9FF:FE40:8004   te9                 2
19    FF12::8   FE80::201:C9FF:FE40:8005   te1       te2       2
      FF12::8                              te10      te3       2
MLD Reporters that are forbidden statically:
VLAN  Group     Source Address             Ports
----  Address   ---------------------      -------
1     -------   FE80::201:C9FF:FE40:8001   te8
19    FF12::3   FE80::201:C9FF:FE40:8001   te9
      FF12::8
```

```
console# show ipv6 mld snooping interface 1000
MLD Snooping is globally enabled
MLD Snooping Querier is globally enabled
MLD Snooping Querier election is enabled
MLD Snooping Querier is enabled on the VLAN
MLD Snooping Querier version: 1
MLD Snooping admin: Enabled
MLD snooping oper mode: Enabled
Routers MLD version: 2
Groups that are in MLD version 1 compatibility mode:
FF12::3, FF12::8
MLD snooping robustness: admin 2  oper 2
MLD snooping query interval: admin 125 sec  oper 125 sec
MLD snooping query maximum response: admin 10 sec  oper 10 sec
MLD snooping last member query counter: admin 2  oper 2
MLD snooping last member query interval: admin 1000 msec  oper 600 msec
MLD snooping last immediate leave: enable
Automatic learning of multicast router ports is enabled
```

```
console# show ipv6 mld snooping mrouter interface 1000
VLAN Static Dynamic Forbidden
1000 te1    te2       te3-23
```

Unregistered Multicast

Multicast frames are generally forwarded to all ports in the VLAN. If IGMP Snooping is enabled, the device learns about the existence of Multicast groups and tracks which ports have joined what Multicast group.

Multicast groups can also be statically enabled. This enables the device to forward the Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

Traffic from unregistered Multicast groups, which are the groups that are not known to the device, can either be filtered or forwarded. After a port has been set to Forwarding/Filtering, its configuration is valid for any VLAN of which it is a member (or will be a member of).

To set the action for unregistered Multicast groups on a port or LAG:

1. Click **Switching** > **Multicast Support** > **Unregistered Multicast** in the tree view to display the **Unregistered Multicast: Summary** page.

   The action for each port is displayed.

2. To modify the forwarding action for an interface, click **Edit,** and enter the fields.

   - **Interface** — Select a port or LAG.
   - **Unregistered Multicast** — Select the forwarding status of the selected interface. The possible options are:
     - **Forwarding** — Enables forwarding of unregistered Multicast frames on the selected port or port-channel.
     - **Filtering** — Enables filtering of unregistered Multicast frames on the selected VLAN interface.

Configuring Unregistered Multicast Using CLI Commands

The following table summarizes the CLI commands for configuring unregistered Multicast on the device:

Table 16-7. Unregistered Multicast CLI Commands

CLI Command	Description
bridge multicast unregistered {*forwarding* | *filtering*} **no bridge multicast unregistered**	Configures the forwarding state of unregistered Multicast addresses on a port or LAG. Before using this command, enter the Interface Configuration mode as shown in the example. Use the no format of the command to restore the default configuration.
show bridge multicast unregistered [interface-id]	Displays the unregistered multicast filtering configuration.

The following is an example of the CLI commands:

```
console(config)# interface gi0/1
console(config-if)# bridge multicast unregistered filtering
console # show bridge multicast unregistered
Port      Unregistered
-------   --------
gi0/1     Forward
gi0/2     Filter
gi0/3     Filter
```

Multicast TV VLAN

This section describes the Multicast TV VLAN feature.

It contains the following sections:

- Multicast TV VLAN Overview
- Multicast TV VLAN Membership
- Multicast TV VLAN Mapping

Multicast TV VLAN Overview

The Multicast TV VLAN feature provides the ability to supply Multicast transmissions to Layer 2-isolated subscribers, without replicating the Multicast transmissions for all subscriber VLANs. The subscribers are the only receivers of the Multicast transmissions.

- A Multicast TV VLAN can be defined for an Access port (a port that is in Access mode for VLAN membership).
- All static VLANs are permitted to be a Multicast-TV VLAN.
- The configuration is performed per port.

One or more IP Multicast address groups can be associated with a Multicast VLAN. The source port must belong to the Multicast VLAN. Source and receiver ports do not have to be members of the same VLAN.

An end port is defined as a receiver port for the Multicast VLAN. Receiving ports can belong to a single user VLAN and additionally to one Multicast VLAN. The receiver port can be an access member in any VLAN, but not in the defined Multicast VLAN. In Multicast VLAN, the receiver port can only receive traffic and not send traffic on it. Receivers of same Multicast VLAN are isolated in different User (Access port) VLANs and therefore isolated from each other.

If a Multicast-TV VLAN is defined on an access port, then:

- The access port joins the Multicast-TV VLAN.
- The Multicast-TV VLAN on the receiver port is always untagged.
- The acceptable frame type of the port is set to Admit Untagged Only.

Multicast TV VLAN Membership

To view Multicast TV VLANs:

- Click **Switching > Multicast Support > Multicast TV VLAN Membership** in the tree view to display the **Multicast TV VLAN Membership** page.

  The receiver and transceiver ports in the selected TV VLAN are displayed.

Displaying Multicast TV VLAN Membership Using CLI Commands

The following table summarizes the CLI command for displaying Multicast TV VLAN membership:

Table 16-8. Multicast TV VLAN Membership CLI Commands

CLI Command	Description
`show vlan multicast-tv vlan` *`vlan-id`*	Displays information on the source ports and receiver ports of multicast-TV VLAN.

The following is an example of the CLI commands:

```
console # show vlan multicast-tv vlan 1
Source Ports
-------------------------------------
gi0/8, gi0/4
Receiver Ports
-------------------------------------
gi2/1-4, gi3/1-4, gi4/1-4
```

Multicast TV VLAN Mapping

To set the Multicast Group IP address for a TV VLAN:

1 Click **Switching** > **Multicast Support** > **Multicast TV VLAN Mapping** in the tree view to display the **Multicast TV VLAN Mapping: Summary** page.

   The Multicast Group IP addresses for the selected TV VLAN are displayed.

2 To add the Multicast Group IP address for a VLAN, click **Add**, and enter the fields:

   - **VLAN ID** — Enter a VLAN ID.
   - **Multicast Group IP Address** — Enter the Multicast group IP address for which the IGMP Snooping is enabled.

Mapping Multicast TV VLANs to IP Addresses Using CLI Commands

The following table summarizes the CLI command for mapping Multicast TV VLANs to Multicast IP addresses:

Table 16-9. Unregistered Multicast CLI Commands

CLI Command	Description
ip igmp snooping vlan vlan-id **multicast-tv** *ip-multicast-address* [***count*** *number*]	Defines the Multicast IP addresses that are associated with a Multicast-TV VLAN.
no **ip igmp snooping vlan** *vlan-id* **multicast-tv** *ip-multicast-address* [***count*** *number*]	Use the no form of this command to remove all associations.
show ip igmp snooping multicast-tv [***vlan*** *vlan-id*]	Displays the IP addresses associated with Multicast TV VLANs.

The following is an example of the CLI commands:

```
console# show ip igmp snooping multicast-tv
VLAN IP Address
---- -----------
1000 239.255.0.0
1000 239.255.0.1
1000 239.255.0.2
1000 239.255.0.3
1000 239.255.0.4
1000 239.255.0.5
```

17

LLDP

The section describes the Link Layer Discovery Protocol (LLDP).

It contains the following topics:

- Overview
- LLDP Properties
- LLDP Port Settings
- MED Network Policy
- MED Port Settings
- Neighbors Information

Overview

The Link Layer Discovery Protocol (LLDP) enables network managers to troubleshoot and enhance network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing methods for network devices to advertise themselves to other systems, and to store discovered information. Discovery information includes:

- Device identification
- Device capabilities
- Device configuration

The advertising device transmits multiple advertisement message sets in a single LAN packet. The multiple advertisement message sets are sent in the packet's Type Length Value (TLV) field.

LLDP devices must support chassis and port ID advertisements, as well as system name, system ID, system description, and system capability advertisements.

LLDP Media Endpoint Discovery (LLDP-MED) increases network flexibility by enabling various IP systems to co-exist on a single network, and provides the following features:

- Detailed network topology information, including information on which devices are located on the network and where the devices are located, for example, which IP phone is connect to which port, which software is running on which switch, and which port is connected to which device.
- Automatic deployment of policies over networks for:
  - QoS Policies
  - Voice VLANs
- Emergency Call Service (E-911) via IP phone location information.
- Troubleshooting information. LLDP MED sends network managers alerts for:
  - Port speed and duplex mode conflicts
  - QoS policy misconfigurations

LLDP Properties

To enable and configure LLDP:

1. Click **Switching > LLDP > LLDP Properties** in the tree view to display the **LLDP Properties** page.

   The current LLDP properties are displayed.

2. Enter the fields:
   - **Enable LLDP —** Enable/disable LLDP on the device.
   - **Updates Interval (5-32768) —** Enter the rate at which LLDP advertisement updates are sent.

- **Hold Multiplier (2-10) —** Enter the hold time to be sent in the LLDP update packets, as a multiple of the timer value.
- **Reinitializing Delay (1-10)** — Enter the minimum time, in seconds, that an LLDP port waits before reinitializing LLDP transmission.
- **Transmit Delay (1-8192)** — Enter the amount of time that passes between successive LLDP frame transmissions, due to changes in the LLDP local systems MIB.

To use the default values for any field, select **Use Default**.

Configuring LLDP Using CLI Commands

The following commands are used to set the fields in the **LLDP Properties** page.

Table 17-1. LLDP Properties CLI Commands

CLI Command	Description
lldp run **no lldp run**	Enables enable LLDP. Use the no form of this command to disable LLDP.
lldp timer *seconds* **no lldp timer**	Specifies how often the software sends LLDP updates. Use the no form of this command to restore the default configuration.
lldp hold-multiplier *number* **no lldp hold-multiplier**	Specifies the time that the receiving device should hold a Link Layer Discovery Protocol (LLDP) packet before discarding it. Use the no form of this command to restore the default configuration.
lldp reinit *seconds* **no lldp reinit**	Specifies the minimum time an LLDP port will wait before reinitializing. Use the no form of this command to revert to the default setting.

Table 17-1. LLDP Properties CLI Commands *(continued)*

CLI Command	Description
lldp tx-delay *seconds* **no lldp tx-delay**	Specifies the delay between successive LLDP frame transmissions. Use the no form of this command to restore the default configuration.

The following is an example of the CLI commands:

```
console(config)# interface vlan 1
console(config-if)# lldp run
console(config)# lldp timer 30
console(config)# lldp hold-multiplier 3
console(config)# lldp reinit 4
```

LLDP Port Settings

LLDP configuration of a port includes activating LLDP notification on it, and selecting the optional TLVs that will be sent in the LLDP PDU, in addition to the mandatory ones.

By setting these properties, it is possible to provide additional types of information to those network devices that support the LLDP.

To configure LLDP per port:

1. Click **Switching > LLDP > LLDP Port Settings** in the tree view to display the **LLDP Port Settings: Summary** page.

   LLDP settings for all ports are displayed.

2. To modify the LLDP settings for a port, click **Edit** and select the port to be configured.
3. Select the transmission type on which LLDP is to be configured in the **State** field. The possible options are:
   - *Tx Only* — Enables LLDP on transmitting LLDP packets only.
   - Rx Only — Enables LLDP on receiving LLDP packets only.

- *Tx & Rx* — Enables LLDP on transmitting and receiving LLDP packets.
- *Disable* — LLDP is disabled on the port.

4 Move the optional TLVs that the switch should advertise from the **Available TLV** list to the **Optional TLV** list. The TLVs advertise the following:

   - **Port Description** — Information about the port, including manufacturer, product name, and hardware/software version.
   - **System Name** — System's assigned name (in alpha-numeric format). This value equals the sysName object.
   - **System Description** — Description of the network entity (in alpha-numeric format). This includes the system's name and versions of the hardware, operating system, and networking software supported by the switch. This value equals the sysDescr object.
   - **System Capabilities** — Primary functions of the switch, and whether or not these functions are enabled in the switch. The capabilities are indicated by two octets. Bits 0 through 7 indicate Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and station respectively. Bits 8 through 15 are reserved.
   - **802.3 MAC-PHY** — Duplex and bit rate capability and the current duplex and bit rate settings of the sending device. It also advertises whether the current settings are due to auto-negotiation or manual configuration.

   An alternative way to select the TLVs is to select the **Use Default** field, in which case only mandatory TLVs are used. These are: Chassis subtype (MAC address), Port subtype (port number), and TTL (time-to-leave).

5 Enter the **Management IP Address** that is advertised from the interface. Check **Use Default** to use the default Management IP address.

Configuring LLDP Port Settings Using CLI Commands

The following commands are used to configure LLDP on ports.

Table 17-2. LLDP Port Settings CLI Commands

CLI Command	Description
lldp transmit **no lldp transmit**	Enables transmitting LLDP on an interface. Use the no form of this command to stop transmitting LLDP on an interface.
lldp receive **no lldp receive**	Enables receiving LLDP on an interface. Use the no form of this command to stop receiving LLDP on an interface.
lldp optional-tlv *tlv1 [tlv2 … tlv5*|***none]***	Specifies which optional TLVs from the basic set should be transmitted

The following is an example of the CLI commands:

```
console(config)# interface gi0/1
console(config-if)# lldp transmit
console(config-if)# lldp receive
console(config-if)# lldp optional-tlv port-desc
```

MED Network Policy

An LLDP-MED network policy is a set of configuration settings that is identified by a network policy number. Policies are loaded into LLDP-MED TLVs, and sent to devices connected to the switch. A network policy instructs the connected device as to how to send traffic, for example, a policy can be created for VoIP phones that instructs them to:

- Send voice traffic on VLAN 10
- Tag voice traffic with DSCP=63
- Transmit data-traffic to the switch (from the PC connected to the switch through the VoIP phone) without modification to traffic sent by the PC (typically, Untagged).

For network policies to be implemented, they must be created and then associated with ports.

Before policies are defined, the administrator must create the VLANs, and configure memberships in the VLANs, based on the specification in the LLDP-MED network policies.

To add a MED network policy:

1. Click **Switching > LLDP > MED Network Policy** in the tree view to display the **MED Network Policy: Summary** page.

   Previously-defined network policies are displayed.

2. To add a network policy, click **Add**, and enter the fields:
   - **Network Policy Number** — Select an available network policy number.
   - **Application** — Select the application (type of traffic) for which the network policy is defined.
   - **VLAN ID** — Enter the VLAN ID to which the traffic should be sent.
   - **VLAN Type** —Select whether the traffic is Tagged or Untagged.
   - **User Priority** — Select the traffic priority assigned to the network application.
   - **DSCP Value** — Select the value to be used by neighbors to mark the traffic sent to the switch.

Configuring MED Network Policies Using CLI Commands

The following commands are used to configure MED network policies.

Table 17-3. LLDP MED Network Policies CLI Commands

CLI Command	Description

`lldp med network-policy number application [vlan vlan-id] [vlan-type {tagged|untagged}] [up priority][dscp value]`
`no lldp med network-policy number`
	Defines an LLDP MED network policy.
	Use the no form of this command to remove an LLDP MED network policy.

The following is an example of the CLI commands:

```
console(config)# lldp med network-policy 1 voice-
signaling vlan 1
```

MED Port Settings

To assign MED network policies to ports:

1. Click **Switching** > **LLDP** > **MED Port Settings** in the tree view to display the **MED Port Settings: Summary** page.
2. All ports are displayed along with the following fields:
   - **LLDP MED Status** — Specifies if LLDP-MED is enabled on the selected port.
   - **Network Policy** — Specifies whether a network policy is assigned to the port.
   - **Location** — Specifies whether the location is advertised.
   - **PoE** — Specifies whether PoE is enabled on the port
3. To modify network policies on a port, click **Edit**.
4. Select the port to be configured, and enter the fields for the port:
   - **Enable LLDP-MED** — Enable/disable LLDP-MED on the port.
   - **Available TLVs** — Contains a list of available TLVs that can be advertised by the port. The possible options are:
     - **Network Policy** — Advertises the network policy attached to the port.
     - **Location** — Advertises the port's location.

     Move the TLVs to be published to the **Tx Optional TLVs** list.
   - **Available Network Policy** — Contains a list of network policies that can be assigned to a port. Move the network policies to be assigned to the port to the **Network Policy** list.
   - **Location Coordinate (16 Bytes in Hex)** — Displays the device's location map coordinates.
   - **Location Civic Address (6-160 Bytes in Hex)** — Displays the device's civic or street address location, for example 414 23rd Ave E.

- **Location ECS ELIN (10-25 Bytes in Hex)** — Displays the device’s ECS ELIN location.

5 To view MED details for a port, click **Detail** and select a port.

The following fields are displayed for the port:

- **Auto-Negotiation Status** — Enabled specifies that auto-negotiation is enabled on the port; Disabled indicates that it is not.
- **Advertised Capabilities** — The list of port capabilities advertised for the port.
- **MAU Type** — The Media Attachment Unit type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network, for example, 100BASE-TX full duplex mode.
- **System Name** — The system's assigned name (in alpha-numeric format). This value equals the sysName object.
- **System Description** — A description of the network entity (in alpha-numeric format). This includes the system's name and versions of the hardware, operating system, and networking software supported by the switch. This value equals the sysDescr object.
- **Device ID** — The device ID advertised, for example, the device MAC address.
- **Device Type** — The type of device.
- **LLDP MED Capabilities** — The TLVs that are advertised by the port.
- **LLDP MED Device Type** — Specifies whether a sender is a network connectivity device or an endpoint device.
- **Application** — The following fields are displayed for each possible application type:
  - **Application Type** — The application type.
  - **Flags** — The VLAN tagging status for the application type: Tagged or Untagged.
  - **VLAN ID** — The VLAN number for the application type.
  - **User Priority** — The user priority for the application type.
  - **DSCP** — The DSCP value assigned to the network policy.

- **Location Type** — Displays the port’s LLDP location type:
  - **Coordinates** — Device’s location map coordinates.
  - **Civic Address** — Device’s civic or street address location, for example 414 23rd Ave E.
  - **ECS ELIN** — Device’s ECS ELIN location.
- **Location Address** — Displays the port’s LLDP location, according to the **Location Type**.

Configuring MED on Ports Using CLI Commands

The following commands are used to set the fields in the **MED Port Settings** pages.

Table 17-4. LLDP Properties CLI Commands

CLI Command	Description
lldp med {enable [*tlv … tlv4*]|**disable}** **no lldp med**	Enables LLDP MED on an interface. Use the no form of this command to disable LLDP MED on an interface.
lldp med network-policy {***add***|***remove***} *number* **no lldp med network-policy** *number*	Attaches or removes an LLDP MED network policy on an interface. Use the no form of this command to remove all the LLDP MED network policies from the interface
lldp med location {{***coordinate*** *data*}|{***civic-address*** *data*}|{***ecs-elin*** *data*}} **no lldp med location** {***coordinate***|***civic-address***|***ecs-elin***}	configure the LLDP MED for an interface. Use the no form of this command to delete location information for an interface.
show lldp med configuration **[**interface-*id* |***detailed]***	Displays the LLDP MED configuration for all interfaces or for a specific interface.
show lldp local interface-*id*	Displays the LLDP information that is advertised from a specific port.

The following is an example of the CLI commands:

```
console(config)# interface gi0/3

console(config)# lldp med location civic-address
6162636465

console# show lldp med configuration

Fast Start Repeat Count: 4.

Network policy 1

-------------------

Application type: voiceSignaling

VLAN ID: 1 untagged

Layer 2 priority: 0

DSCP: 0

Port Capabil- Network Location Notif-   Inventory
     ities    Policy           ications

---- ------- -------- ------- -------   --------

gi0/1 Yes    Yes      Yes      Enabled   No

gi0/2 Yes    Yes      No       Enabled   No
```

Neighbors Information

Use the **Neighbors Information** page to view information that was received in LLDP advertisements from neighboring devices.

The neighbor's information is deleted after timeout. Timeout is the maximum interval that can pass without receiving an LLDP PDU from a neighbor. The timeout value is computed from the neighbor's Time to Live TLV.

To view neighbors information:

1 Click **Switching** > **LLDP** > **Neighbors Information** in the tree view to display the **Neighbors Information** page.

The following fields are displayed for each port on the device that has a discovered neighbor:

- **Port** — Port number for which neighboring information is displayed
- **Device ID** — Neighboring device ID
- **System Name** — Name of the neighboring system
- **Port ID** — Neighboring port ID
- **Capabilities** — Neighboring device capabilities

2 Click **Clear Neighbors Table** to delete all the entries or select **Remove** to delete a specific port entry.

3 Click the **Details** button of a port to display the **Neighbors Information: Details** page for that port.

In addition to the fields displayed in the **MED Port Settings: Details Advertise Information** page and the **Green Ethernet Configuration** pages, the following fields are displayed for the neighbors of the selected port:

- **Power Type** — Port's power type
- **Power Source** — Port's power source
- **Power Priority** — Port's power priority
- **Power Value** — Port's power value, in Watts
- **Hardware revision** — Hardware revision
- **Firmware revision** — Firmware revision
- **Software revision** — Software revision
- **Serial number** — Device serial number
- **Manufacturer name** — Device manufacturer name
- **Model name** — Device model name
- **Asset ID** — Asset ID

Configuring LLDP Neighbors Using CLI Commands

The following commands are used to configure LLDP neighbors.

Table 17-5. LLDP Neighbors Information CLI Commands

CLI Command	Description

`show lldp neighbors`
`[interface-`*`id`*`]`
	Displays information about neighboring devices discovered using LLDP

The following is an example of the CLI commands:

```
console# show lldp neighbors
Port     Device ID     Port ID System Capabili TTL
                                Name   ties

--------- ------------ -------- ----- ------ -------

gi2/4 00:75:73:71:72:55 gi0/1          B,R      91

gi3/4 00:12:cf:7c:63:a0 gi0/2           0       92

gi4/4 00:11:22:11:22:33 gi0/3           0       107
```

18

UDLD

NOTE: This feature is only supported on the R1-2210 device.

This section describes how the Unidirectional Link Detection (UDLD) feature.

It covers the following topics:

- Overview
- UDLD Global Settings
- UDLD Interface Settings
- UDLD Neighbors

Overview

Unidirectional Link Detection (UDLD) is a Layer 2-protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to detect unidirectional links. A unidirectional link occurs whenever traffic from a neighboring device is received by the local device, but traffic from the local device is not received by the neighbor.

The purpose of UDLD is to detect ports on which the neighbor does not receive traffic from the local device (unidirectional link) and to shut down those ports.

All connected devices must support UDLD for the protocol to successfully detect unidirectional links. If only the local device supports UDLD, it is not possible for the device to detect the status of the link. In this case, the status of the link is set to undetermined. The user can configure whether ports in the undetermined state are shut down or merely trigger notifications.

UDLD States and Modes

Under the UDLD protocol, ports are assigned the following states:

- **Detection**—System is attempting to determine whether the link is bidirectional or unidirectional. This is a temporary state.

- **Bidirectional**—Traffic sent by a local device is known to be received by its neighbor, and traffic from the neighbor is received by the local device.
- **Shutdown**—The link is unidirectional. Traffic sent by a local device is received by its neighbor, but traffic from the neighbor is not received by the local device.
- **Undetermined**—The system cannot determine the state of the port, because of one of the following is occurring:
  - The neighbor does not support UDLD.

  or

  - The neighbor does not receive traffic from the local device.

  The UDLD action in this case depends on the UDLD mode of the device as explained below.

UDLD supports the following modes of operation:

- **Normal**
  - If the link is unidirectional, the port is shut down.
  - If the link is undetermined, the port is not shut down. Its status is changed to undetermined and a notification is sent.
- **Aggressive**

  If the link is unidirectional or undetermined, the port is shut down.

UDLD is enabled on a port when one of the following occurs:

- The port is a fiber port and UDLD is enabled globally.
- The port is a copper port and you specifically enable UDLD on it.

How UDLD Works

When UDLD is enabled on a port, the following actions are performed:

- UDLD initiates the detection state on the port.

  In this state, UDLD periodically sends messages on every active interface to all neighbors. These messages contain the device ID of all known neighbors. It sends these messages according to a user-defined message time.

- UDLD receives UDLD messages from neighboring devices. It caches these messages until the expiration time (3 times message time) has passed. If a new message is received before the expiration time, the information in that message replaces the previous one.
- When the expiration time expires, the device does the following with the information received:
  - **If the neighbor message contains the local device ID**—The link status of the port is set to bidirectional.
  - **If the neighbor message does not contain the local device ID**—The link status of the port is set to unidirectional, and the port is shut down.
- If UDLD messages are not received from a neighboring device during the expiration time frame, the link status of the port is sent to undetermined and the following occurs:
  - **Device is in normal UDLD mode:** A notification is issued.
  - **Device is in aggressive UDLD mode.** The port is shut down.

While the interface is in the bidirectional or the undetermined state, the device periodically sends a message each message time seconds. The above steps are performed over and over.

A port that was shut down can be reactivated manually in the **Port Management > Error Recovery Settings** page. For more information, see Reactivating a Shutdown Port.

If an interface is down and UDLD is enabled, the device removes all neighbor information and sends at least one ULDL message to the neighbors informing them that the port is down. When the port is brought up, the UDLD state is changed to detection.

UDLD Not Supported or is Disabled on a Neighbor

If UDLD is not supported or disabled on a neighbor, then no UDLD messages are received from that neighbor. In this case, the device cannot determine whether the link is unidirectional or bidirectional. The status of the interface is then set to undetermined. The actions taken by the device depend on whether the UDLD mode is normal or aggressive.

Inconsistent UDLD Mode in Local and Neighboring Device

It is possible for the local device and its neighbor to be set to a different UDLD mode (normal, aggressive). The UDLD mode is not contained in the UDLD messages, so that the local device does not know the UDLD mode of the neighbor and vice versa.

If the UDLD modes are different on the local and neighbor devices, the devices act as follows:

- When the UDLD state of the link is bidirectional or unidirectional, both devices shut down their ports.
- When the UDLD state of the port is undetermined, the side with the normal UDLD mode merely issues a notification, while the side with the aggressive UDLD mode shuts down the port.

If both devices are in normal mode, the port is not shut down when its state is undetermined.

Reactivating a Shutdown Port

You can reactivate a port that was shut down by UDLD in one of the following ways:

- **Automatically**—Configure the system to automatically reactivate ports shut down by UDLD in the **Port Management > Error Recovery Settings** page. In this case, when a port is shut down by UDLD, it is automatically reactivated when the automatic recovery interval expires. UDLD again begins running on the port. If the link is still unidirectional, UDLD shuts it down again after the UDLD expiration time expires, for instance.
- **Manually**—Reactivate a port in the **Port Management > Error Recovery Settings** page.

Usage Guidelines

Dell does not recommend enabling UDLD on ports that are connected to devices on which UDLD is not supported or disabled. Sending UDLD packets on a port connected to a device that does not support UDLD simply causes more traffic on the port without providing benefits.

In addition, take the following into consideration when configuring UDLD:

- Set the message time according to how urgent it is to shut down ports with a unidirectional link. The lower the message time, the more UDLD packets are sent and analyzed, but the sooner the port is shut down if the link is unidirectional.
- If you want UDLD to be enabled on a copper port, you must enable it per port. When you globally enable UDLD, it is only enabled on fiber ports.
- Set the UDLD mode to normal when you do not want to shut down ports unless it is known for sure that the link is unidirectional.
- Set the UDLD mode to aggressive when you want to shut down any port whenever there is even a chance that the link is undetermined.

Dependencies On Other Features

- UDLD and Layer 1.

  When UDLD is enabled on a port, UDLD actively runs on that port while the port is up. When the port is down, UDLD goes into UDLD shutdown state. In this state, UDLD removes all learned neighbors. When the port is changed from down to up, UDLD resumes actively running.

- UDLD and Layer 2 Protocols

  UDLD runs on a port independently from other Layer 2 protocols running on the same port, such as STP or LACP. For example, UDLD assigns the port a status regardless of the STP status of the port or regardless of whether the port belongs to a LAG or not.

Default Settings and Configuration

The following defaults exist for this feature:

- UDLD is disabled by default on all ports of the device.
- Default message time is 15 seconds.
- Default expiration time is 45 seconds (3 times the message time).
- Default port UDLD state:
  - Fiber interfaces are in the global UDLD state.
  - Non-fiber interfaces are in the disable state.

Common UDLD Tasks

This section describes some common tasks to setup UDLD.

Workflow1: To globally enable UDLD on fiber ports, perform the following steps:

- Open the **Switching > UDLD > UDLD Global Settings** page.
  - Enter the Message Time.
  - Select either **Disabled**, **Normal** or **Aggressive** as the global UDLD status.
  - Click **Apply**

Workflow2: To change the UDLD configuration of a fiber port or to enable UDLD on a copper port, perform the following steps:

1. Open the **Switching > UDLD > UDLD Global Settings** page.
   - Select a port.
   - Select either **Default**, **Disabled**, **Normal** or **Aggressive** as the port's UDLD status. If you select Default, the port receives the global setting.
2. Click **Apply**.

UDLD Global Settings

The UDLD feature can be configured for all fiber ports at one time (in the UDLD Global Settings page) or per port (in the UDLD Interface Settings page).

The Fiber Port UDLD Default State is only applicable to fiber ports.

The Message Time field is applicable to both copper and fiber ports.

To configure UDLD globally:

1. Click **Switching > UDLD > UDLD Global Settings**.
2. Enter the following fields:
   - **Message Interval**—Enter the timeout interval between two sent UDLD messages. This field is relevant for both fiber and copper ports.

- **Fiber Port UDLD Default State**—This field is only relevant for fiber ports. The UDLD state of copper ports must be set individually in the UDLD Interface Settings page. The possible states are:
  - *Disabled*—UDLD is disabled on all ports of the device.
  - *Normal*—Device shuts down an interface if the link is unidirectional. If the link is undetermined, a notification is issued.
  - *Aggressive*—Device shuts down an interface if the link is unidirectional or undetermined.

3 Click **Apply** to save the settings to the Running Configuration file.

Defining UDLD Global Parameters Using CLI Commands

The following table summarizes the CLI commands for defining and displaying UDLD global parameters as displayed in the **UDLD Global Settings** pages.

Table 18-1. UDLD Global Parameter CLI Commands

CLI Command	Description

`udld aggressive | normal`
`no udld`
	Enables UDLD functionality and sets its mode on fiber interfaces only.
	Use the no form of this command to disable UDLD functionality.

`udld message time seconds`
`no udld message time`
	Configures a global timeout value of the interval between two sent probe messages.
	Use the no form of this command to restore the default configuration.

`show udld [interface-id] [neighbors]`	Displays the administrative and operational UDLD status.

The following is an example of the CLI commands:

```
console(config)# udld normal
console(config)# udld message time 40
console(config)# exit
console(config)# show udld
Global UDLD mode: normal
Message Time: 15 sec(default)
Interface te0/1
  Port UDLD mode: aggressive
  Port Current state: Bidirectional
  Number of detected neighbors: 1
  Port Neighbor Table
    Neighbor Device ID: 1234567893
      Neighbor MAC: 00:00:01:22:33:dd
      Neighbor Device name: switch A
      Neighbor Port ID: te0/1
      Neighbor Message Time: 20 sec
      Neighbor Current State: Bidirectional
      Neighbor Expiration Time: 7 sec
Interface te0/2
  Port UDLD mode: normal (default)
  Port Current state: Undetermined
  Number of detected neighbors: 1
    Neighbor Device ID: 1234567753
      Neighbor MAC: 00:00:01:22:33:fe
      Neighbor Device name: switch A
      Neighbor Port ID: te0/2
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 11 sec
Port Current state: detection
```

UDLD Interface Settings

Use the UDLD Interface Settings page to change the UDLD state for a specific port. Here the state can be set for copper or fiber ports.

To copy a particular set of values to more than one port, set that value for one port and use the **Copy** button to copy it to the other ports.

To configure UDLD for an interface:

1. Click **Switching > UDLD > UDLD Interface Settings**.

   Information is displayed for all ports on which UDLD is enabled, or, if you have filtered only a certain group of ports, information is displayed for that group of ports.

   – **Port**—The port identifier.

   – **UDLD State**—The possible states are:

     - **Disabled**—UDLD is disabled on all fiber ports of the device.
     - **Normal**—Device shuts down an interface if it detects that the link is unidirectional. It issues a notification if the link is undetermined.
     - **Aggressive**—Device shuts down a port if the link is unidirectional or undetermined.

   – **Bidirectional State**—Bidirectional state for the selected port. The possible states are:

     - **Detection**—The latest UDLD state of the port is in the process of being determined. Expiration time has not yet expired since the last determination (if there was one), or since UDLD began running on the port, so that the state is not yet determined.
     - **Bidirectional**—Traffic sent by the local device is received by its neighbor, and traffic from the neighbor is received by the local device.
     - **Undetermined**—The state of the link between the port and its connected port cannot be determined either because no UDLD message was received or the UDLD message did not contain the local device ID in it.
     - **Disabled**—UDLD has been disabled on this port.

        - **Shutdown**—The port has been shut down because its link with the connected device is unidirectional or undetermined in aggressive mode.

    - **Number of Neighbors**—Number of connected devices detected.

2 To modify the UDLD state for a specific port, select the **Edit** tab and select the port.

3 Modify the value of the UDLD state. If you select **Default**, the port receives the value of the Fiber Port UDLD Default State in the Global UDLD Settings page.

4 Click **Apply** to save the settings to the Running Configuration file.

Defining UDLD Parameters on a Port Using CLI Commands

The following table summarizes the CLI command for defining UDLD parameters on a port as displayed in the **UDLD Interface Settings** pages.

Table 18-1. UDLD Port CLI Commands

CLI Command	Description
`udld port [aggressive | normal | disable]`	Enables UDLD functionality on an Ethernet port
`no udld port`	Use the no form of this command to disable UDLD functionality on the port.

The following is an example of the CLI commands:

```
console(config)# interface te0/1
console(config-interface) udld port normal
```

UDLD Neighbors

To view all devices connected to the local device:

1 Click **Switching > UDLD > UDLD Neighbors**.

The following fields are displayed for all UDLD-enabled ports.

- **Interface Name**—Name of the local UDLD-enabled port.
- **Neighbor Information**:
    - **Device ID**—ID of the remote device.

    - **Device MAC**—MAC address of the remote device.
    - **Device Name**—Name of the remote device.
    - **Port ID**—Name of the remote port.
  - **State**—State of the link between the local and neighboring device on the local port. The following values are possible:
    - **Detection**—The latest UDLD state of the port is in the process of being determined. Expiration time has not yet expired since the last determination (if there was one), or since UDLD began running on the port, so that the state is not yet determined.
    - **Bidirectional**—Traffic sent by the local device is received by its neighbor, and traffic from the neighbor is received by the local device.
    - **Undetermined**—The state of the link between the port and its connected port cannot be determined either because no UDLD message was received or the UDLD message did not contain the local device ID in it.
    - **Disabled**—UDLD has been disabled on this port.
    - **Shutdown**—The port has been shut down because its link with the connected device is unidirectional or undetermined in aggressive mode.
  - **Neighbor Expiration Time (Sec)**—Displays the time that must pass before determining the port UDLD status. This is three times the Message Time.
  - **Neighbor Message Time (Sec)**—Displays the time between UDLD messages.

Viewing UDLD Neighbors Using CLI Commands

The following table displays the CLI command for viewing all devices connected to the local device as displayed in the **UDLD Neighbor** pages

Table 18-1. Viewing UDLD Neighbors CLI Commands

CLI Command	Description
`show udld [interface-id] [neighbors]`	Displays the administrative and operational UDLD status and status of devices connected to the local device.

The following is an example of the CLI commands:

```
console# show udld
Global UDLD mode: normal
Message Time: 15 sec(default)
Interface te0/1
  Port UDLD mode: aggressive
  Port Current state: Bidirectional
  Number of detected neighbors: 1
  Port Neighbor Table
    Neighbor Device ID: 1234567893
      Neighbor MAC: 00:00:01:22:33:dd
      Neighbor Device name: switch A
      Neighbor Port ID: te0/2
      Neighbor Message Time: 20 sec
      Neighbor Current State: Bidirectional
      Neighbor Expiration Time: 7 sec
Interface te0/2
  Port UDLD mode: normal (default)
  Port Current state: Undetermined
  Number of detected neighbors: 1
    Neighbor Device ID: 1234567753
      Neighbor MAC: 00:00:01:22:33:fe
      Neighbor Device name: switch A
      Neighbor Port ID: te0/2
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 11 sec
Port Current state: detection
```

19

Dynamic ARP Inspection

This section describes dynamic ARP inspection.

It contains the following topics:

- Overview
- Global Settings
- Dynamic ARP Inspection List
- Dynamic ARP Inspection Entries
- VLAN Settings
- Trusted Interfaces

Overview

ARP Inspection eliminates man-in-the-middle attacks, where false ARP packets are inserted into the subnet. ARP requests and responses are inspected, and their MAC-address-to-IP-address binding is checked according to the ARP Inspection List defined by the user (in the *Dynamic ARP Inspection List* and *Dynamic ARP Inspection Entries* pages). If the packet's IP address was not found in the ARP Inspection List, and DHCP Snooping is enabled for a VLAN, a search of the DHCP Snooping database is performed.

See Binding Database for an explanation of the DHCP Snooping database. If the IP address is found the packet is valid, and is forwarded.

Packets with invalid ARP Inspection bindings are logged and dropped.

Ports are classified as follows:

- Trusted — Packets are not inspected.
- Untrusted —Packets are inspected as described above.

The following additional validation checks may be configured by the user:

- Source MAC — Compares the packet's source MAC address in the Ethernet header against the sender's MAC address in the ARP request. This check is performed on both ARP requests and responses.
- Destination MAC — Compares the packet's destination MAC address in the Ethernet header against the destination interface's MAC address. This check is performed for ARP responses.
- IP Addresses — Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP Multicast addresses.

Global Settings

To enable ARP inspection on the device:

1 Click **Switching** > **Dynamic ARP Inspection** > **Global Settings** in the tree view to display the **Global Settings** page.

2 Enter the fields:

  - **Enable ARP Inspection** — Enable/disable ARP inspection.
  - **ARP Inspection Validate** — Enable/disable the following checking source MAC address, destination MAC address and IP addresses against the respective addresses in the ARP body.
  - **Minimal Syslog Interval** (0 – 86400) — Enter the minimum time interval between successive ARP SYSLOG messages.

Setting Dynamic ARP Inspection Global Settings Using CLI Commands

The following table summarizes the CLI commands for configuring the fields in the **Global Settings** pages.

Table 19-1. ARP Inspection Global Settings CLI Commands

CLI Command	Description
`ip arp inspection`	Enables ARP inspection.
`no ip arp inspection`	Use the no form of this command to disable ARP inspection.

Table 19-1. ARP Inspection Global Settings CLI Commands ***(continued)***

CLI Command	Description
ip arp inspection validate **no ip arp inspection validate**	Performs specific checks for dynamic ARP inspection. Use the no form of this command to restore the default configuration.
ip arp inspection logging interval {*seconds* | ***infinite***} **no ip arp inspection logging interval**	Sets the minimum time interval between successive ARP SYSLOG messages. Use the no form of this command to restore the default configuration.

The following is an example of some of the CLI commands:

```
console(config)# ip arp inspection
console(config)# ip arp inspection validate
```

Dynamic ARP Inspection List

An ARP inspection list consists of entries where each entry is a pair of MAC/IP addresses.

To create a new ARP inspection list and add the first entry to it:

1 Click **Switching** > **Dynamic ARP Inspection** > **Dynamic ARP Inspection List** in the tree view to display the **Dynamic ARP Inspection List: Summary** page.

The dynamic ARP lists are displayed.

2 To create a new list and enter the first address pair in it, click **Add**, and enter the fields:

- **List Name** — Create and enter a list name.
- **IP Address** — Enter the IP address that will be mapped to the MAC address entered below.
- **MAC Address** — Enter the MAC address that will be mapped to the IP address entered above.

Creating a Dynamic ARP Inspection List Using CLI Commands

The following table summarizes the CLI commands for configuring the fields in the **Dynamic ARP Inspection List** pages.

Table 19-2. Dynamic ARP Inspection List CLI Commands

CLI Command	Description
ip arp inspection list create *name*	Creates a static ARP binding list and enters the ARP list configuration mode.
no ip arp inspection list create *name*	Use the no form of this command to delete the list.

The following is an example of some of the CLI commands:

```
console(config)# ip arp inspection list create
servers

console(config-ARP-list)#
```

Dynamic ARP Inspection Entries

To add additional addresses to the lists defined in the **Dynamic ARP Inspection List** page:

1. Click **Switching** > **Dynamic ARP Inspection** > **Dynamic ARP Inspection Entries** in the tree view to display the **Dynamic ARP Inspection Entries: Summary** page.

   The dynamic ARP entries for the selected list are displayed.

2. To add a new address pair to a list, click **Add** and select the list.
3. Enter the fields:
   - **IP Address** — Enter the IP address that will be mapped to the MAC address entered below.
   - **MAC Address** — Enter the MAC address that will be mapped to the IP address entered above.

Adding Entries to a Dynamic ARP Inspection List Using CLI Commands

The following table summarizes the CLI commands for configuring the fields in the **Dynamic ARP Inspection Entries** pages.

Table 19-3. Dynamic ARP Inspection List Entries CLI Commands

CLI Command	Description

`ip` *`ip-address`* `mac` *`mac-address`*
`no ip` *`ip-address`* `mac` *`mac-address`*
	Creates a static ARP binding.
	Use the no form of this command to delete a static ARP binding..

`show ip arp inspection list`	Displays the static ARP binding list.

The following is an example of some of the CLI commands:

```
console(config)# ip arp inspection list create
servers

console(config-arp-list)# ip 172.16.1.1 mac
0060.704c.7321

console(config-arp-list)# ip 172.16.1.2 mac
0060.704c.7322

console(config-arp-list)# do show ip arp inspection
list

List name: servers

Assigned to VLANs:

IP               MAC

--------------- ------------------

172.16.1.1      00:60:70:4c:73:21

172.16.1.2      00:60:70:4c:73:22

console(config-arp-list)#
```

VLAN Settings

To assign a list of IP/MAC address pairs, defined in the **Dynamic ARP Inspection List** pages, to a VLAN:

1. Click **Switching** > **Dynamic ARP Inspection** > **VLAN Settings** in the tree view to display the **VLAN Settings: Summary** page.

   The VLANs and their associated lists of IP/MAC address pairs are displayed.

2. To designate a VLAN to be associated with an ARP inspection list, click **Add VLAN** and enter the VLAN ID.
3. Click **Assign** and select the **List Name** to be associated with the VLAN.

Assigning IP/MAC Address Pairs to VLANs Using CLI Commands

The following table summarizes the CLI commands for configuring the fields in the **VLAN Settings** pages.

Table 19-4. Assigning IP/MAC Address Pairs to VLANs CLI Commands

CLI Command	Description
ip arp inspection vlan *vlan-id*	Enables ARP inspection on a VLAN, based on the DHCP Snooping database. Use the no form of this command to disable ARP inspection on a VLAN.
ip arp inspection list assign *vlan-id name*	Assigns a static ARP binding list to a VLAN.
no ip arp inspection list assign *vlan-id*	Use the no form of this command to delete the assignment.

The following is an example of some of the CLI commands:

```
console(config)# ip arp inspection list assign 37
servers
```

Trusted Interfaces

Interfaces are untrusted if the packet is received from an interface outside the network or from an interface beyond the network firewall. Trusted interfaces receive packets only from within the network or the network firewall.

To configure an interface to be trusted:

1 Click **Switching** > **Dynamic ARP Inspection** > **Trusted Interfaces** in the tree view to display the **Trusted Interfaces: Summary** page.

  The ports and their trusted status are displayed.

2 To modify the status of an interface, click **Edit.**

3 Select the interface and enable/disable its **Trust Status**, which is the DHCP Snooping Trust mode.

Configuring Trusted Interfaces Using CLI Commands

The following table summarizes the CLI commands for configuring the fields in the **Trusted Interface** pages.

Table 19-5. Configuring Trusted Interface Parameters CLI Commands

CLI Command	Description
ip arp inspection trust **no ip arp inspection trust**	Configures an interface trust state that determines if incoming ARP packets are inspected. Use the no form of this command to restore the default configuration.
show ip arp inspection [interface-id]	Displays the ARP inspection configuration for all interfaces or a specific interface.

The following is an example of some of the CLI commands:

```
console(config)# interface gi0/3
console(config-if)# ip arp inspection trust
```

20

DHCP

This section describes DHCP snooping.

It contains the following topics:

- DHCP Snooping
- DHCP Relay

DHCP Snooping

This section describes DHCP Snooping.

It contains the following sections:

- Overview
- Global Parameters
- VLAN Settings
- Trusted Interfaces
- Binding Database

Overview

DHCP snooping expands network security by providing layer security between untrusted interfaces and DHCP servers. By enabling DHCP snooping, network administrators can differentiate between trusted interfaces connected to end-users or DHCP Servers, and untrusted interfaces located beyond the network firewall.

DHCP snooping filters untrusted messages, and stores these messages in a database. Interfaces are untrusted if the packet is received from an interface outside the network, or from an interface beyond the network firewall. Trusted interfaces receive packets only from within the network or the network firewall.

The DHCP Snooping Binding database contains the untrusted interfaces' MAC address, IP address, Lease Time, VLAN ID, and interface information.

Table 20-1 describes how DHCP packets are handled when DHCP snooping is enabled on an interface.

Table 20-1. DHCP Packet Handling when DHCP Snooping is Enabled

Packet Type	Arriving from Untrusted Ingress Interface	Arriving from Trusted Ingress Interface
DHCPDISCOVER	Forward to trusted interfaces only.	Forwarded to trusted interfaces only.
DHCPOFFER	Filter.	Forward the packet according to DHCP information. If the destination address is unknown the packet is filtered.
DHCPREQUEST	Forward to trusted interfaces only.	Forward to trusted interfaces only.
DHCPACK	Filter.	Same as DHCPOFFER and an entry is added to the Binding database.
DHCPNAK	Filter.	Same as DHCPOFFER. Remove entry if exists.

Table 20-1. DHCP Packet Handling when DHCP Snooping is Enabled *(continued)*

Packet Type	Arriving from Untrusted Ingress Interface	Arriving from Trusted Ingress Interface
DHCPDECLINE	Check if there is information in the database. If the information exists and does not match the interface on which the message was received, the packet is filtered. Otherwise the packet is forwarded to trusted interfaces only, and the entry is removed from database.	Forward to trusted interfaces only
DHCPRELEASE	Same as DHCPDECLINE.	Same as DHCPDECLINE.
DHCPINFORM	Forward to trusted interfaces only.	Forward to trusted interfaces only.
DHCPLEASEQUERY	Filtered.	Forward.

As shown in Table 20-1, the DHCP Snooping Binding database is updated by interception of DHCPACK, DHCPDECLINE and DHCPRELEASE packets, and is stored in non-volatile memory.

Even if a port is down, its entries are not deleted.

NOTE: Only DHCP requests on untrusted ports are maintained in the Binding database.

Limitations

The following limitations apply:

- Enabling DHCP snooping uses TCAM resources.
- The switch writes changes to the binding database only when the switch system clock is synchronized with SNTP.
- The switch does not update the Binding database when a station moves to another interface.

Global Parameters

Use the **Global Parameters** page to:

- Enable/disable DHCP snooping globally.
- Determine whether to forward or filter DHCP packets received from untrusted interfaces, whose source MAC address and the DHCP client MAC address do not match.
- Determine whether to forward or filter DHCP packets, received from untrusted interfaces, with option-82 information.
- Set Binding database update interval.

To configure DHCP snooping on the device:

1. Click **Switching > DHCP Snooping > Global Parameters** in the tree view to display the **Global Parameters** page.
2. Enable/disable DHCP snooping on the device in the **DHCP Snooping Status** field.
3. If DHCP snooping is enabled, enter the fields:
   - **Option 82 Passthrough** — Enable/disable whether to forward (enable) or filter (disable) DHCP packets, received from untrusted interfaces, with option-82 information.
   - **Verify MAC Address** — Enable/disable MAC addresses verification. This determines whether to forward (enable) or filter (disable) DHCP packets received from untrusted interfaces, whose source MAC address and the DHCP client MAC address do not match.
   - **Save Binding Database to File** — Enable/disable saving the DHCP snooping database to flash memory.
   - **Save Binding Database Internal (600-86400)** — Enter how often, in seconds, the Binding database is updated.

Configuring DHCP Snooping Global Parameters Using CLI Commands

The following table summarizes the CLI commands for configuring DHCP snooping global parameters.

Table 20-2. DHCP Snooping Global Parameters CLI Commands

CLI Command	Description

`ip dhcp snooping`
`no ip dhcp snooping`
	Globally enables DHCP snooping.
	Use the no form of this command to return to the default setting.

`ip dhcp snooping information option allowed-untrusted`
`no ip dhcp snooping information option allowed-untrusted`
	Allows a device to accept DHCP packets with option-82 information from an untrusted port.
	Use the no form of this command to return to the default setting.

`ip dhcp snooping verify`
`no ip dhcp snooping verify`
	Configures the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address.
	Use the no form of this command to configure the switch to not verify the MAC addresses.

`ip dhcp snooping database`
`no ip dhcp snooping database`
	Configures the DHCP snooping binding file.
	Use the no form of this command to delete the binding file.

`ip dhcp snooping database update-freq` *`seconds`*
`no ip dhcp snooping database update-freq`
	Configures the update frequency of the DHCP snooping binding file.
	Use the no form of this command to return to default.

`show ip dhcp snooping` `[interface-id]`	Displays the DHCP snooping configuration.

The following is an example of some of the CLI commands:

```
console(config)# ip dhcp snooping
console(config)# ip dhcp snooping information option
allowed-untrusted
console(config)# ip dhcp snooping verify
console(config)# ip dhcp snooping database
console(config)# ip dhcp snooping database frequency 1200
console# show ip dhcp snooping
DHCP snooping is enabled
DHCP snooping database: enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
DHCP snooping file update frequency is configured to: 1200
seconds
       Interface  Trusted
       ---------  ----------
       gi2/1      yes
       gi2/2      yes
```

VLAN Settings

To separate ports in a VLAN, enable DHCP snooping on it.

Before you enable DHCP snooping on a VLAN, you must globally enable DHCP snooping on the device.

When DHCP snooping is disabled for a VLAN, the Binding entries that were collected for that VLAN are removed from the Binding database.

To enable/disable DHCP snooping on a VLAN:

1. Click **Switching > DHCP Snooping > VLAN Settings** in the tree view to display the **VLAN Settings** page.

   The list of existing VLANs are displayed in the **VLAN ID** list.

2 Click **Add** to move the VLANs, for which you want to enable DHCP snooping, from the **VLAN ID** list to the **Enabled VLANs** list. To remove a VLAN, click **Remove** to move it from the **Enabled VLANs** list to the **VLAN ID** list.

Configuring DHCP Snooping on VLANs Using CLI Commands

The following table summarizes the CLI commands for configuring DHCP snooping on VLANs .

Table 20-3. DHCP Snooping on VLANs CLI Commands

CLI Command	Description
ip dhcp snooping vlan *vlan-id*	Enables DHCP snooping on a VLAN.
no ip dhcp snooping *vlan-id*	Use the no form of this command to disable DHCP snooping on a VLAN.

The following is an example of some of the CLI commands:

```
console(config)# ip dhcp snooping vlan 1
```

Trusted Interfaces

To define a trusted interface:

1 Click **Switching > DHCP Snooping > Trusted Interfaces** in the tree view to display the **Trusted Interface: Summary** page.

A list of the interfaces is displayed.

2 To change the trust status of an interface, click **Edit**, and enter the fields:

- **Interface** — Select a port or LAG.
- **Trust Status** — Enable/disable DHCP Snooping Trust mode on the selected port or LAG.

Configuring DHCP Snooping Trusted Interfaces Using CLI Commands

The following table summarizes the CLI commands for configuring DHCP snooping trusted interfaces.

Table 20-4. DHCP Snooping Trusted Interfaces CLI Commands

CLI Command	Description
ip dhcp snooping trust **no ip dhcp snooping trust**	Configures an interface as trusted for DHCP snooping purposes. Use the no form of this command to return to the default setting.

The following is an example of some of the CLI commands:

```
console(config)# interface gi0/5
console(config-if)# ip dhcp snooping trust
```

Binding Database

Entries in the DHCP Snooping Binding database consist of pairs of MAC/IP addresses.

In addition to the entries added by DHCP snooping, entries to the Snooping Binding database can be manually added or deleted. These entries are added to the Snooping Binding database and Snooping Binding file, if it exists, but they are not added to the configuration files.

A manually-added entry can be either dynamic or a static. When configuring a dynamic entry, an expiration date must be assigned.

The refresh time (in seconds) of the binding table is added in the **Global Parameters** pages.

To query and add IP addresses to the Binding database:

1 Click **Switching > DHCP Snooping > Binding Database** in the tree view to display the Binding Database: Summary page.

A list of the database entries is displayed.

2 To query the database, enter query criteria and click **Query**. Database entries matching the query are displayed.

3 To add an entry, click **Add**, and enter the fields:

- **Type** — Select the entry type. The possible options are:
  - **Static** —IP address was statically configured.
  - **Dynamic** —IP address was dynamically configured.
- **MAC Address** — Enter the MAC address to be recorded in the entry.
- **VLAN ID** — Select the VLAN ID to which the IP address is associated in the entry.
- **IP Address** — Enter the IP address to be recorded in the entry.
- **Interface** — Select the type and port or LAG to be recorded in the entry.
- **Lease Time** — If the entry is dynamic, enter the amount of time that the entry will be active in the DHCP Database. If there is no Lease Time, check **Infinite**.

Configuring DHCP Snooping Binding Database Using CLI Commands

The following table summarizes the CLI commands for configuring the DHCP Snooping Binding database.

Table 20-5. DHCP Snooping Binding Database CLI Commands

CLI Command	Description
ip dhcp snooping database **no ip dhcp snooping database**	Enables the DHCP Snooping binding database file. Use the no form of this command to delete the DHCP Snooping binding database file.
ip dhcp snooping database update-freq *seconds* **no ip dhcp snooping database update-freq**	Enables the DHCP Snooping binding database file. Use the no form of this command to delete the DHCP Snooping binding database file.
ip dhcp snooping binding *mac-address vlan-id ip-address interface-id* **expiry** {*seconds*|***infinite***} **no ip dhcp snooping binding** *mac-address vlan-id*	Configures the DHCP snooping binding database and adds binding entries to the database. Use the no form of this command to delete entries from the binding database.

Table 20-5. DHCP Snooping Binding Database CLI Commands *(continued)*

CLI Command	Description
`clear ip dhcp snooping database`	Clears the DHCP binding database.
show ip dhcp snooping binding [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan-id*][interface-*id*]]	Displays the DHCP snooping binding database and configuration information for all interfaces or some interfaces on a switch.

The following is an example of some of the CLI commands:

```
console(config)# ip dhcp snooping database
console(config)# ip dhcp snooping update-freq 3600
console# show ip dhcp snooping binding
Update frequency: 3600
Total number of binding: 2

MAC Address        IP Address    Lease     Type         VLAN     Interface
                                 (sec)
-----------        ----------    ------    --------     -----    ----------
0060.704C.73FF     10.1.8.1      7983      snooping     3        gi0/3
0060.704C.7BC1     10.1.8.2      92332     snooping     3        gi0/4
```

DHCP Relay

This section describes DHCP relay.

It contains the following sections:

- Overview
- Option 82
- Global Settings
- Interface Settings

Overview

The device can act as a DHCP Relay agent that listens for DHCP messages, and relays them between DHCP servers and clients, which reside in different VLANs or IP subnets.

This functionality is intended to be used when the client ingress VLAN is different than the VLAN on which DHCP servers are connected.

The switch can relay DHCP messages received from its IPv4 interfaces to one or more configured DHCP servers. It uses the switch’s IPv4 address of the interface where the message is received. The switch uses the address from the response to determine how to forward the response back to the DHCP client.

DHCP Relay must be enabled globally and per VLAN.

Limitations

The following limitations exist for DHCP Relay:

- It is not supported on IPv6.
- It is not relayed to servers on the client’s VLAN.
- Packets that have option-82 information, added by other devices, are discarded.
- It does not support Option 82 on non-VLAN interfaces.
- It can be enabled only on a VLAN/Port/LAG that has an IP address defined on it.

Option 82

The relay agent information option (Option 82) in the DHCP protocol enables a DHCP relay agent to send additional client information when requesting an IP address. Option 82 specifies the relaying switch's MAC address, the port identifier, and the VLAN that forwarded the packet.

Both DHCP snooping and DHCP relay can insert option 82 into traversing packets.

DHCP snooping with option 82 insertion provides transparent Layer 2 relay agent functionality when the DHCP server is on the same VLAN as the clients.

To enable Option 82 insertion:

1 Click **Switching** > **DHCP Relay** > **Option 82** in the tree view to display the **Option 82** page.
2 Enable/disable Option 82 insertion.

Configuring Option 82 Using CLI Commands

The following table summarizes the CLI commands for defining fields displayed in the **Option 82** page.

Table 20-6. CLI Option 82 Commands

CLI Command	Description
`ip dhcp information option`	Enables DHCP option-82 data insertion.
`no ip dhcp information option`	Use the no form of this command to disable DHCP option-82 data insertion.

The following is an example of the CLI command:

```
console(config)# ip dhcp information option
```

Global Settings

To set the DHCP Relay global settings:

1 Click **Switching** > **DHCP Relay** > **Global Settings** in the tree view to display the **Global Settings: Summary** page.

   The currently-define DHCP servers are displayed.

2 Enable/disable DHCP relay.
3 To add a DHCP server, click **Add**.
4 Enter the IP address of the DHCP server in the **DHCP Server IP Address** field.

Defining Global Parameters Using CLI Commands

The following table summarizes the CLI commands for defining fields displayed in the **Global Settings** pages.

Table 20-7. Global Parameters CLI Commands

CLI Command	Description
ip dhcp relay enable **no ip dhcp relay enable**	Enables DHCP relay features on the device. Use the no form of this command to disable the DHCP relay agent.
ip dhcp relay address *ip-address*	Defines the DHCP servers available for the DHCP relay.
no ip dhcp relay address [*ip-address*]	Use the no form of this command to remove servers from the list.
show ip dhcp relay	Displays the server addresses on the DHCP relay.

The following is an example of the CLI commands:

```
console(config-if)# ip dhcp relay enable
console(config)# ip dhcp relay address 176.16.1.1
console(config)# do show ip dhcp relay
DHCP relay is Enabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any VLAN.
Servers: 176.16.1.1
console(config)#
```

Interface Settings

NOTE: For DHCP Relay to function on an interface, it also must be activated globally in the Global Settings page.

To enable DHCP relay on a port, LAG, or VLAN:

1 Click **Switching > DHCP Relay > Interface Settings** in the tree view to display the **Interface Settings: Summary** page.

  The currently-define DHCP interfaces are displayed.

2 To enable DHCP relay on an interface, click **Add**.

3 Select the interface.

Defining Interface Settings Using CLI Commands

The following table summarizes the CLI commands for defining fields displayed in the **Interface Settings** pages.

Interface Settings Parameters CLI Commands

CLI Command	Description

`ip dhcp relay enable`
`no ip dhcp relay enable`
	Enables the DHCP relay features on the interface (in Interface Configuration mode).
	Use the no form of this command to disable the DHCP relay agent feature on the interface.

`ip dhcp relay address` *`ip-address`*
`no ip dhcp relay address`
	Defines a DHCP servers available for DHCP relay.
	Use the no form of this command to remove servers from the list.

The following is an example of the CLI commands that enable DHCP Relay on VLAN 2, assign it an IP address and show the DHCP Relay status:

```
console(config)# interface vlan 2
console(config-if)# ip dhcp relay enable
console(config)# ip dhcp relay address 176.16.1.1
console> show ip dhcp relay
DHCP relay is Enabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any vlan.
No servers configured
```

21

Statistics/RMON

This section describes many of the statistics available on the device. The only exception is the QoS statistics described in QoS Statistics.

It contains the following topics:

- Table Views
- RMON
- Charts

Table Views

This section displays statistics in table form.

It contains the following topics:

- Denied ACEs Counters
- Utilization Summary
- Counter Summary
- Interface Statistics
- Etherlike Statistics
- GVRP Statistics
- EAP Statistics

Denied ACEs Counters

The Denied ACEs counters contain the number of packets that were dropped (denied) because they did not meet ACL criteria expressed in some ACE.

To display the denied ACE counters:

1 Click **Statistics/RMON** > **Table Views** > **Denied ACEs Counters** in the tree view to display the **Denied ACEs Counters** page.

   The global number of dropped packets is displayed along with the number of dropped packets on each interface.

2. To clear the counters, select either a port or LAG. The counters on all ports/LAGs are cleared.
3. Mark the counters to be cleared and click **Clear Counters**.
4. To clear all counters, click **Clear All Counters**.

Viewing Denied ACE Counters Statistics Using the CLI Commands

The following table contains the CLI commands for viewing denied ACE counters statistics.

Table 21-1. Denied ACE Counters CLI Commands

CLI Command	Description
show interfaces access-lists counters [*interface-id*|port-channel-number]	Displays Access List counters.

The following is an example of the CLI commands:

```
console# show interfaces access-lists counters
Interface Denied ACE hits
--------- ------------
gi0/1        55
gi0/2        33
gi0/3        32
```

Utilization Summary

Use the **Utilization Summary** page to display interface utilization. This page is refreshed periodically to minimize impact on performance. Display may be disrupted during this period.

To display interface utilization statistics:

1. Click **Statistics/RMON** > **Table Views** > **Utilization Summary** in the tree view to display the **Utilization Summary** page.
2. Select a port or LAG.

The following fields are displayed:

- **Port/LAG** — The port/LAG number.
- **Interface Status** — The status of the interface: **Up**, **Down** or **Not Present** when no port is attached to the LAG.
- **% Interface Utilization** — Network interface utilization percentage, based on the duplex mode of the interface. The range of this reading is from 0 to 200%. The maximum reading of 200% for a full duplex connection indicates that 100% of bandwidth of incoming and outgoing connections is used by the traffic travelling through the interface. The maximum reading for a half-duplex connection is 100%.
- **% Unicast Received** — Percentage of Unicast packets received on the interface.
- **% Non Unicast Packets Received** — Percentage of non-Unicast packets received on the interface.
- **% Error Packets Received** — Percentage of packets with errors received on the interface.

3 Select one of the **Refresh Rate** options to specify how frequently the statistics should be refreshed.

The CPU utilization chart is displayed.

Counter Summary

To display the number of received and transmitted packets on ports, as numeric figures and not percentages:

1 Click **Statistics/RMON > Table Views > Counter Summary** in the tree view to display the **Counter Summary** page.

Counters for the selected ports or LAG are displayed.

2 Select a port/LAG.

The following fields are displayed:

- **Port/LAG** — The interface number.
- **Interface Status** — Status of the interface: **Up** or **Down**.
- **Received Unicast Packets** — Number of received Unicast packets on the interface.

- **Transmitted Unicast Packets** — Number of transmitted Unicast packets from the interface.
- **Received Non Unicast Packets** — Number of received non-Unicast packets on the interface.
- **Transmitted Non Unicast Packets** — Number of transmitted non-Unicast packets from the interface.
- **Received Errors** — Number of received packets with errors on the interface.

3 Select one of the **Refresh Rate** options to specify how frequently the counters should be refreshed.

Interface Statistics

To display the number of received and transmitted packets on an interface:

1 Click **Statistics/RMON > Table Views > Interface Statistics** in the tree view to display the **Interface Statistics** page.

2 Select a port/LAG.

3 Select one of the **Refresh Rate** options to specify how frequently the counters should be refreshed.

The following fields are displayed:

Receive Statistics

- **Total Bytes (Octets)** — Amount of octets received on the selected interface.
- **Unicast Packets** — Number of Unicast packets received on the selected interface.
- **Multicast Packets** — Number of Multicast packets received on the selected interface.
- **Broadcast Packets** — Number of Broadcast packets received on the selected interface.
- **Packets with Errors** — Number of errors packets received on the selected interface.

Transmit Statistics

- **Total Bytes (Octets)** — Number of octets transmitted from the selected interface.
- **Unicast Packets** — Number of Unicast packets transmitted from the selected interface.
- **Multicast Packets** — Number of Multicast packets transmitted from the selected interface.
- **Broadcast Packets** — Number of Broadcast packets transmitted from the selected interface.

4 Click **Reset All Counters** to clear these counters.

Etherlike Statistics

To display interface error statistics:

1 Click **Statistics/RMON > Table Views > Etherlike Statistics** in the tree view to display the **Etherlike Statistics** page.

2 Select a port/LAG.

The following fields are displayed:

- **Frame Check Sequence (FCS) Errors** — Number of frames received that are an integral number of octets in length but do not pass the FCS check.
- **Single Collision Frames** — Number of frames that are involved in a single collision, and are subsequently transmitted successfully.
- **Late Collisions** — Number of collisions detected after the first 512 bits of data.
- **Excessive Collisions** — Number of frames for which transmission fails due to excessive collisions.
- **Internal MAC Transmit Errors** — Number of frames for which reception fails due to an internal MAC sublayer receive error.
- **Oversize Packets** — Number of frames received that exceed the maximum permitted frame size.
- **Received Pause Frames** — Number of MAC Control frames received with a PAUSE operation code.
- **Transmitted Pause Frames** — Number of MAC Control frames transmitted on this interface with a PAUSE operation code.

3 Select one of the **Refresh Rate** options to clears the statistics for the selected interface.

Viewing Interface Statistics Using the CLI Commands

The following table contains the CLI commands for viewing utilization, counters and interface statistics.

Table 21-2. Interface Statistics CLI Commands

CLI Command	Description
show interfaces counters [*interface-id*|**detailed**]	Displays traffic seen by the physical interface.

The following is an example of the CLI command for all ports:

```
console# show interfaces counters

Port     InUcastPkts InMcastPkts InBcastPkts InOctets
------- ------------ ----------- ----------- --------
gi2/1   0            0            0          0
gi2/2   0            0            0          0
gi2/3   0            0            0          0
gi2/4   0            0            0          0
Port      OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
--------- ------------ ------------ ------------ ------------
gi2/1   0            0            0            0
gi2/2   0            0            0            0
gi2/3   0            0            0            0
gi2/4   0            0            0            0
```

The following is an example of the CLI command for a single port:

```
console# show interfaces counters gi0/1
Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
-------- ------------- ------------ ------------ ------------
gi0/1           0            0            0            0

Port     OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
-------- ----------- ------------ ------------ ------------
gi0/1  0           0            0            0
Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
```

GVRP Statistics

To display device GVRP statistics:

1. Click **Statistics/RMON > Table Views > GVRP Statistics** in the tree view to display the **GVRP Statistics** page.
2. Select a port/LAG.

   The number of received and transmitted packets in the following counters is displayed:

   GVRP Statistics Table

   – **Join Empty** — The number of GVRP Join Empty packets.

   – **Empty** — The number of GVRP empty packets.

   – **Leave Empty** — The number of GVRP Leave Empty packets.

   – **Join In** — The number of GVRP Join In packets.

   – **Leave In** — The number of GVRP Leave In packets.

- **Leave All** — The number of GVRP Leave All packets.

GVRP Error Statistics

- **Invalid Protocol ID** — The number of GVRP Invalid Protocol ID errors.
- **Invalid Attribute Type** — The number of GVRP Invalid Attribute ID errors.
- **Invalid Attribute Value** — The number of GVRP Invalid Attribute Value errors.
- **Invalid Attribute Length** — The number of GVRP Invalid Attribute Length errors.
- **Invalid Event** — The number of GVRP Invalid Events errors.

3 Select one of the **Refresh Rate** options to specify how frequently the statistics should be refreshed.

Viewing GVRP Statistics Using the CLI Commands

The following table contains the CLI commands for viewing GVRP statistics.

Table 21-3. GVRP Statistics CLI Commands

CLI Command	Description
show gvrp statistics [interface-id]	Displays GVRP statistics.
show gvrp error-statistics [interface-id]	Displays GVRP error statistics.

The following is an example of the CLI commands:

```
console# show gvrp statistics
GVRP Statistics:
----------------
Legend:
  rJE   : Join Empty Received     rJIn: Join In Received
  rEmp  : Empty Received          rLIn: Leave In Received
  rLE   : Leave Empty Received    rLA : Leave All Received
  sJE   : Join Empty Sent         sJIn: Join In Sent
  sEmp  : Empty Sent              sLIn: Leave In Sent
  sLE   : Leave Empty Sent        sLA : Leave All Sent
Port    rJE  rJIn  rEmp  rLIn  rLE   rLA   sJE  sJIn  sEmp  sLIn  sLE   sLA
----- ----- ----- ----- ----- ----- ----- ---- ----- ----  ---   ----  ---
gi0/1  1    2     1     4     2     3     4    1     0     0     0     1
```

EAP Statistics

For information about EAP, see Dot1x Authentication.

To display EAP statistics:

1 Click **Statistics/RMON** > **Table Views** > **EAP Statistics** in the tree view to display the **EAP Statistics** page.

2 Select a port/LAG.

The following fields are displayed:

– **Frames Receive** — The number of valid EAPOL frames received on the port.

– **Frames Transmit** — The number of EAPOL frames transmitted via the port.

– **Start Frames Receive** — The number of EAPOL Start frames received on the port.

– **Log off Frames Receive** — The number of EAPOL Logoff frames received on the port.

– **Respond ID Frames Receive** — The number of EAP Resp/ID frames received on the port.

– **Respond Frames Receive** — The number of valid EAP Response frames received on the port.

- **Request ID Frames Transmit** — The number of EAP Req/ID frames transmitted via the port.
- **Request Frames Transmit** — The number of EAP Request frames transmitted via the port.
- **Invalid Frames Receive** — The number of unrecognized EAPOL frames received on this port.
- **Length Error Frames Receive** — The number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frame Version** — The protocol version number attached to the most recently received EAPOL frame.
- **Last Frame Source** — The source MAC address attached to the most recently received EAPOL frame.

3 Select one of the **Refresh Rate** options to specify how frequently the statistics should be refreshed.

Viewing EAP Statistics Using the CLI Commands

The following table summarizes the CLI commands for viewing EAP statistics.

Table 21-4. EAP Statistics CLI Commands

CLI Command	Description
`show dot1x statistics interface` `interface-id`	Displays 802.1X statistics for the specified interface.

The following is an example of the CLI commands:

```
console# show dot1x statistics interface gi0/1
EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 0008.3b79.8787
```

RMON

This section describes Remote Monitoring (RMON), which enables network managers to display network information from a remote location.

It contains the following topics:

- Statistics
- History Control
- History Table
- Events Control
- Events Log
- Alarms

Statistics

To display device utilization statistics and errors that occurred on the device:

1. Click **Statistics/RMON > RMON > Statistics** in the tree view to display the **Statistics** page.
2. Select a port/LAG.

   The following fields are displayed:

   - **Received Bytes (Octets)** — Number of bytes received on the selected interface.
   - **Received Packets** — Number of packets received on the selected interface.
   - **Broadcast Packets Received** — Number of good Broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
   - **Multicast Packets Received** — Number of good Multicast packets received on the interface, since the device was last refreshed.
   - **CRC&Align Errors** — Number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
   - **Undersize Packets** — Number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets), and otherwise well formed.
   - **Oversize Packets** — Number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and otherwise well formed.
   - **Fragments** — Number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets), which has either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error).

- **Jabbers** — Number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and having either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error).
- **Collisions** — Number of collisions received on the interface, since the device was last refreshed.
- **Frames of 64 Bytes** — Number of 64-byte frames received on the interface, since the device was last refreshed.
- **Frames of 65 to 127 Bytes** — Number of 65-127-byte frames received on the interface, since the device was last refreshed.
- **Frames of 128 to 255 Bytes** — Number of 128-255-byte frames received on the interface, since the device was last refreshed.
- **Frames of 256 to 511 Bytes** — Number of 256-511-byte frames received on the interface, since the device was last refreshed.
- **Frames of 512 to 1023 Bytes** — Number of 512-1023-byte frames received on the interface, since the device was last refreshed.
- **Frames of 1024 to Max Octets** — Number of 1024-Max Octet frames received on the interface, since the device was last refreshed.

3 Select one of the **Refresh Rate** options to specify how frequently the statistics should be refreshed.

Configuring RMON Statistics Using the CLI Commands

The following table contains the CLI commands for viewing and enabling RMON statistics.

Table 21-5. Configuring RMON Statistics Using CLI Command

CLI Command	Description
`show rmon statistics {interface-id}`	Displays RMON Ethernet statistics.

The following is an example of the CLI commands:

```
console# show rmon statistics gi0/1
Port te1/0/1
Dropped: 0
Octets: 0 Packets: 0
Broadcast: 0 Multicast: 0
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 0 65 to 127 Octets: 1
128 to 255 Octets: 1 256 to 511 Octets: 1
512 to 1023 Octets: 0 1024 to max Octets: 0
```

History Control

To display the requested RMON history group statistics or request a new sample of interface statistics:

1. Click **Statistics/RMON** > **RMON** > **History Control** in the tree view to display the **History Control: Summary** page.

   Previously-defined samples are displayed.

2. To add a new entry, click **Add**. The **New History Entry** number, which uniquely identifies the sample, is displayed.
3. Enter the fields for the entry:
   - **Source Interface** — Sampled Ethernet interface.
   - **Owner (0-20 characters)** — RMON station or user that configured the entry.
   - **Max No. of Samples to Keep (1-50)** — Number of samples to be saved.
   - **Sampling Interval (1-3600)** — The time interval in seconds between samples.

Configuring RMON History Control Using the CLI Commands

The following table contains the CLI commands for configuring RMON history control.

Table 21-6. RMON History Control CLI Commands

CLI Command	Description
rmon collection stats *index* [**owner** *ownername]*[**buckets** *bucket-number*][**interval** *seconds*] **no rmon collection stats** *index*	Enables and configures RMON on an interface. Use the no form of this command to remove a specified RMON history group of statistics.
show rmon history *index {**throughput**|**errors**|**other**}[**period** seconds]*	Displays RMON collection history statistics.

The following is an example of the CLI commands:

```
console(config)# interface gi0/8
console(config-if)# rmon collection stats 1 interval
2400
```

History Table

The **History Table** page displays interface-specific statistical network samplings. Each table entry represents the counter values compiled during a single sample.

To display RMON statistics for a specified sample:

1. Click **Statistics/RMON** > **RMON** > **History Table** in the tree view to display the **History Table** page.
2. Select a **History Entry No**.

   The following fields are displayed:

   - **Owner** — RMON station or user that requested the RMON information.
   - **Sample No.** — Number of the specific sample the information in the table reflects.

- **Drop Events** — Number of dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number of dropped packets, but rather the number of times dropped packets were detected.
- **Received Bytes (Octets)** — Number of data octets, including bad packets, received on the network.
- **Received Packets** — Number of packets received during the sampling interval.
- **Broadcast Packets** — Number of good Broadcast packets received during the sampling interval.
- **Multicast Packets** — Number of good Multicast packets received during the sampling interval.
- **CRC Align Errors** — Number of packets received during the sampling session, with a length of between 64-1632 octets, who had a bad Check Sequence (FCS) with an integral number of octets, or a bad FCS with a non-integral number.
- **Undersize Packets** — Number of packets, having less than 64 octets, received during the sampling session.
- **Oversize Packets** — Number of packets having more than 1632 octets, received during the sampling session.
- **Fragments** — Number of packets, having less than 64 octets and having a FCS, received during the sampling session.
- **Jabbers** — Number of packets, having more than 1632 octets and who had an FCS, received during the sampling session.
- **Collisions** — Estimated number of packet collision that occurred during the sampling session. Collisions are detected when repeater port detects two or more stations transmitting simultaneously.
- **Utilization** — Estimated main physical layer network usage on an interface during the session sampling. The value is stated in hundredths of a percent.

Viewing the RMON History Table Using the CLI Commands

The following table contains the CLI commands for viewing the RMON history table.

Table 21-7. RMON History Table CLI Commands

CLI Command	Description
show rmon history *index* **{throughput|errors|other}** **[period** *seconds***]**	Displays RMON Ethernet statistics history.

The following is an example of a CLI command:

```
console# show rmon history 1 throughput
Sample Set: 1
Interface: 1/0/1
Requested samples: 50
Owner: CLI
Interval: 1800
Granted samples: 50
Maximum table size: 500
Time
--------------------
Jan 18 2005 21:57:00
Octets
---------
303595962
Packets
--------
357568
Broadcast
---------
3289
Multicast
----------
7287
Util
--------
19%
```

Events Control

Events are actions that are performed when an alarm is generated (alarms are defined in the **Alarms** page).

An event can be any combination of logs/traps. If the action includes logging, then the events are logged in the **Events Log** page.

To define an RMON event:

1. Click **Statistics/RMON > RMON > Events Control** in the tree view to display the **Events Control: Summary** page.

   The currently-defined events are displayed. Along with the fields described in the **Events Control: Add** page, the following field is displayed for the events:

   – **Time** — The time that the event occurred.

2. To define a new event, click **Add**.
3. Enter the fields:

   – **Event Entry** — Displays a new event number.

   – **Community** — Enter the community to which the event belongs or keep the default community.

   – **Description** — Enter the event description.

   – **Type** — Select the event action. The possible options are:

   - **None** — No action is taken.
   - **Log** — When an alarm occurs, a log entry is recorded.
   - **Trap** — When an alarm occurs, a trap is generated.
   - **Log and Trap** — When an alarm occurs, a log entry is recorded and a trap is generated.

   – **Owner** — Enter the event owner.

Defining RMON Events Using the CLI Commands

The following table contains the CLI commands for defining RMON events.

Table 21-8. RMON Event Definition CLI Commands

CLI Command	Description
rmon event index {***none***|***log***|***trap***|***log-trap***} [**community** *text*] [**description** *text*] [**owner** *name*]	Configures an event. Use the no form of this command to remove an event.
no rmon event *index*	
show rmon events	Displays RMON event table.

The following is an example of the CLI commands:

```
console(config)# rmon event 1 log
console(config)# exit
console# show rmon events
Index  Descrip-  Type    Community   Owner    Last Time
       tion
                                              Sent
-----  --------  ------  --------    -----    ----------
1      Errors    Log     Default     CLI      Jan 18
                         Community            2002
                                              23:58:17
2      High      Log-    Router      Manager  Jan 18
       Broadcas  Trap                         2002
       t                                      23:59:48
```

Events Log

The Events log displays the log of events that occurred. An event is logged when the type of the event is **Log** or **Log and Trap**. The action in the event is performed when the event is bound to an alarm (see the **Alarms** page) and the conditions of the alarm have occurred.

To display the events log:

- Click **Statistics/RMON** > **RMON** > **Events Log** in the tree view to display the **Events Control** page.

  The following fields are displayed:

  – **Event** — The event identifier.

  – **Log No.** — The log number.

  – **Log Time** — Time when the log entry was entered.

  – **Description** — Description of the log entry.

Viewing Device Events Using the CLI Commands

The following table contains the CLI commands for viewing device events.

Table 21-9. Device Event Viewing CLI Commands

CLI Command	Description
show rmon log [*event*]	Displays the RMON logging table.

The following is an example of the CLI commands:

```
console(config)# rmon event 1 log

console> show rmon log

Maximum table size: 500

Event Description      Time

----- --------------   -------------

1     Errors           Jan 18 2002 23:58:17

2     High Broadcast   Jan 18 2002 23:59:48
```

Alarms

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on a counter or any other SNMP object counter maintained by the agent.

Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, another rising event is not generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when a rising threshold is crossed. One or more alarms are bound to an event. The event indicates the action to be taken when the alarm occurs.

To add an RMON alarm:

1. Click **Statistics/RMON > RMON > Alarms** in the tree view to display the **Alarms: Summary** page.

   The currently-defined alarms are displayed.

2. To add a new alarm, click **Add** and enter the fields:
   - **Alarm Entry** — Displays a new alarm entry.
   - **Port** — Select the port or LAG for which RMON statistics are displayed.
   - **Counter Name** — Select the selected MIB variable.
   - **Sample Type** — Select the sampling method for the selected variable and comparing the value against the thresholds. The possible options are:
     - **Delta** — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
     - **Absolute** — Compares the values directly with the thresholds at the end of the sampling interval.
   - **Rising Threshold** (0–2147483647) — Enter the rising counter value that triggers the rising event alarm.
   - **Rising Event** — Select one of the previously-defined events.
   - **Falling Threshold** (0–2147483647) — Enter the falling counter value that triggers the falling event alarm.
   - **Falling Event** — Select one of the previously-defined events.

- **Startup Alarm** — Select the trigger that activates the alarm. The possible options are:
  - **Rising Alarm** — A rising counter value triggers the alarm
  - **Falling Alarm** — A falling counter value triggers the alarm.
  - **Rising and Falling** — Both rising and falling counter values trigger the alarm.
- **Interval (1–2147483647)** — Enter the alarm interval time in seconds. This is the interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
- **Owner** — Enter the name of the user or network management system that receives the alarm.

Defining Device Alarms Using the CLI Commands

The following table contains the CLI commands for defining device alarms.

Table 21-10. Device Alarm CLI Commands

CLI Command	Description
rmon alarm *index MIB_Object_ID interval rising-threshold falling-threshold rising-event falling-event* [**type** {**absolute**|**delta**}][**startup** {**rising**|**rising-falling**|**falling**}][**owner** *name*]	Configures RMON alarm conditions. Use the no form of this command to remove an alarm.
no rmon alarm index	
show rmon alarm-table	Displays summary of the alarm table.
show rmon alarm *number*	Displays the RMON alarm configuration.

The following is an example of the CLI commands:

```
console(config)# rmon alarm 1000
1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20

console# show rmon alarm-table

Index

-----

123

OID

----------------------

1.3.6.1.2.1.2.2.1.10.1

1.3.6.1.2.1.2.2.1.10.1

1.3.6.1.2.1.2.2.1.10.9

Owner

-------

CLI

Manager

CLI
```

Charts

This section describes how to display statistics as charts.

It contains the following topics:

- Ports
- LAGs
- CPU Utilization

Ports

To display port statistics in chart format:

1 Click **Statistics/RMON > Charts > Ports** in the tree view to display the **Ports** page.

2 Check the type of statistics to be displayed:

  – **Interface Statistics** — Select the interface statistics to display.

  – **Etherlike Statistics** — Select the frame error statistics to display.

  – **RMON Statistics** — Select the RMON statistics to display.

  – **GVRP Statistics** — Select the GVRP statistics type to display.

  – **Refresh Rate** — Select the amount of time that passes before the statistics are refreshed.

3 To draw a chart for the selected statistics, click **Draw**. The chart for the selected statistic is displayed on the page.

Viewing Port Statistics Using the CLI Commands

The CLI commands for viewing port statistics are the same CLI commands described above. The **Ports** page simply shows the same statistics in chart form.

LAGs

To display LAG statistics in chart format:

1 Click **Statistics/RMON > Charts > LAGs** in the tree view to display the **LAGs** page.

2 Check the type of statistics to be displayed:

  – **Interface Statistics** — Select the interface statistics to display.

  – **Etherlike Statistics** — Select the frame error statistics to display.

  – **RMON Statistics** — Select the RMON statistics to display.

  – **GVRP Statistics** — Select the GVRP statistics type to display.

  – **Refresh Rate** — Select the amount of time that passes before the statistics are refreshed.

3 To draw a chart for the selected statistics, click **Draw**. The chart for the selected statistic is displayed on the page.

Viewing LAG Statistics Using the CLI Commands

The following table contains the CLI commands for viewing LAG statistics.

Table 21-11. LAG Statistic CLI Commands

CLI Command	Description
show interfaces counters [*LAG-number* |**detailed**]	Displays traffic seen by the physical interface.
show rmon statistics {*interface-id*}	Displays RMON Ethernet statistics.
show gvrp statistics [*interface-id*]	Displays GVRP statistics.
show gvrp-error statistics [*interface-id*]	Displays GVRP error statistics.

The following is an example of the CLI commands:

```
console# show rmon statistics gi0/1

Port gi0/1

Dropped: 0

Octets: 0 Packets: 0

Broadcast: 0 Multicast: 0

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 0 65 to 127 Octets: 1

128 to 255 Octets: 1 256 to 511 Octets: 1

512 to 1023 Octets: 0 1024 to max Octets: 0
```

CPU Utilization

Use the **CPU Utilization** page to display the system’s CPU utilization and percentage of CPU resources consumed by the device.

To display CPU utilization in chart format:

1. Click **Statistics/RMON** > **Charts** > **CPU Utilization** in the tree view to display the **CPU Utilization** page.
2. Select the **Refresh Rate** to specify how frequently the statistics should be refreshed.

The CPU utilization chart is displayed.

Viewing CPU Utilization Using CLI Commands

The following table summarizes the CLI commands for viewing CPU utilization.

Table 21-12. CPU Utilization CLI Commands

CLI Command	Description
show cpu utilization	Displays CPU utilization.

The following is an example of the CLI commands:

```
console# show cpu utilization

CPU utilization service is on.

CPU utilization

--------------------------

five seconds: 5%; one minute: 3%; five minutes: 3%
```

22

Quality of Service

This section provides information for configuring Quality of Service (QoS).

It contains the following topics:

- Overview
- General
- QoS Basic Mode
- QoS Advanced Mode
- QoS Statistics

Overview

The QoS feature is used to optimize network performance. It provides classification of incoming traffic into traffic classes, based on one or more attributes, including:

  – Device configuration
  – Ingress interface
  – Packet contents

QoS includes the following features:

- **Traffic Classification** — Classifies each incoming packet, as belonging to a specific traffic flow, based on the packet contents and/or interface. The classification is done by an ACL (Access Control List), and only traffic that meets the ACL criteria is subject to classification.
- **Assignment to Hardware Queues** — Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong.
- **Other Traffic Class-Handling Attribute** — Applies QoS mechanisms to various classes, including bandwidth management.

QoS Modes

A single QoS mode is selected and applies to all interfaces in the system. The modes are:

- **Basic Mode — Class of Service (CoS)**.
  - Traffic is divided into classes that determine how it is treated. All traffic in a class is treated with the same QoS action. The QoS action for the class of traffic determines the egress queue on the egress port, based on the indicated QoS value in the incoming frame.

    The QoS value in the incoming frame is:

    - **Layer 2 Packets** — VLAN Priority Tag (VPT) 802.1p value
    - **Layer 3 IPv4 Frames** — Differentiated Service Code Point (DSCP) value
    - **Layer 3 IPv6 Frames** —Traffic Class (TC) value

    When operating in Basic mode, the switch trusts this externally-assigned QoS value.

    This is the default QoS mode.
- **Advanced Mode — Per-flow Quality of Service (QoS)**.

  In Advanced mode, a per-flow QoS consists of a class map and a policer:

  - A class map defines the kind of traffic in a flow, and contains one or more ACLs. Packets that match the ACLs belong to the flow.
  - A policer applies the configured QoS to a flow. The QoS configuration of a flow may consist of the egress queue, the DSCP or CoS value, and actions on out-of-profile (excess) traffic.
- **Disable Mode (QoS is not enabled)**

  In this mode, all traffic is mapped to a single best-effort queue, so that no type of traffic is prioritized over another.

Only a single mode can be active at a time. When the system is configured to work in QoS Advanced mode, settings for QoS Basic mode are not active and vice versa.

When the QoS mode is changed, the following occurs:

- When changing from Advanced mode to any other mode, policy profile definitions and class maps are deleted. ACLs, which are bonded directly to interfaces, remain bonded.
- When changing from Basic mode to Advanced mode, the QoS Trust mode configuration in Basic mode is not retained.
- When disabling QoS, the shaper and queue setting (WRR/SP bandwidth settings) are reset to default values.

All other user configurations remain intact.

General

This section contains the following topics:

- QoS Mode
- QoS Properties
- Queue
- CoS to Queue
- DSCP to Queue
- Bandwidth
- TCP Congestion Avoidance

QoS Mode

To enable/disable the QoS mode:

1 Click **Quality of Service** > **General** > **QoS Mode** in the tree view to display the **QoS Mode** page.

2 Select the **QoS Mode**. The possible options are:

   – **Basic** — QoS is enabled in Basic mode on the switch

   – **Advanced** — QoS is enabled in Advanced mode on the switch.

   – **Disable** — QoS is not enabled on the switch.

Setting QoS Mode Using CLI Commands

The following table summarizes the CLI commands for setting the QoS mode.

Table 22-1. QoS Mode CLI Commands

CLI Command	Description
qos [***basic***|***advanced***]	Enables QoS on the device.
no qos	Use the no form of this command to disable QoS on the device
show qos	Displays the QoS mode.

The following is an example of the CLI commands:

```
console(config)# qos basic
```

QoS Properties

To set the default CoS value on incoming, untagged packets:

1. Click **Quality of Service** > **General** > **QoS Properties** in the tree view to display the **QoS Properties: Summary** page.

   The default CoS values for all interfaces are displayed.

2. To modify the CoS value for an interface, click **Edit**, and enter the fields:

   – **Interface** — Select a port or LAG if required.

   – **Set Default CoS** — Enter the default CoS tag value for untagged packets.

Configuring QoS Properties Using CLI Commands

The following table summarizes the CLI commands for configuring fields in the **QoS Properties** page.

Table 22-2. QoS Properties CLI Commands

CLI Command	Description
qos cos *default-cos*	Defines the default CoS value of a port.
no qos cos	Use the no form of this command to restore the default configuration.

The following is an example of the CLI command:

```
console(config)# interface gi0/8
console(config-if)# qos cos 3
```

Queue

The switch supports four queues for the R1-2401 device and eight queues for the R1-2210 device for each interface. Queue number four and eight is the highest priority queue for the R1-2401 and R1-2210 devices, respectively. Queue number one is the lowest priority queue.

Traffic Limitation Methods

There are two ways of determining how traffic in queues is handled, Strict Priority and Weighted Round Robin (WRR):

- **Strict Priority** — Egress traffic from the highest-priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, thus providing the highest level of priority of traffic to the lowest-numbered queue.
- **Weighted Round Robin (WRR)** — In WRR mode, the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent). The type of WRR algorithm used in the device is not the standard Deficit WRR (DWRR), but rather Shaped Deficit WRR (SDWRR).

Combination of WRR and Strict Priority

The priority for handling traffic can be selected for each queue. When the queuing mode is Weighted Round Robin for all queues, queues are serviced according to their weights. If all queues are assigned strict priority, queues are serviced according to that order.

The following is true if some queues are assigned strict priority and others are assigned WRR:

- If one queue is assigned strict priority, all higher queues are also assigned strict priority. Conversely, if a queue is assigned a WRR weight, all lower queues must also have a WRR weight assigned to them.

- In the above case, traffic for the strict priority queues is always sent before traffic from the WRR queues. Traffic from the WRR queues is forwarded only after the strict priority queues have been emptied. The relative portion from each WRR queue depends on its weight.

To select the priority method and enter WRR weights:

1 Click **Quality of Service** > **General** > **Queue** in the tree view to display the **Queue** page.

  The queues are displayed.

2 Enter the parameters for the queues:

  – **Strict Priority** — Check to indicate that traffic scheduling for the selected queue, and all higher queues, is based strictly on the queue priority.

  – **WRR** — Check to indicate that traffic scheduling for the selected queue is based on WRR. The time period is divided between the WRR queues that are not empty, meaning they have descriptors to egress. This happens only if strict priority queues are empty.

  – **Scheduling WRR Weight** — If WRR is selected, enter the WRR weight assigned to the queue.

  – **% of WRR Bandwidth** — Displays the amount of bandwidth assigned to the queue. These values represent the percent of the WRR weight.

Configuring Queue Settings Using CLI Commands

The following table summarizes the CLI commands for configuring fields in the **Queue** page.

Table 22-3. Queue Setting CLI Commands

CLI Command	Description
priority-queue out num-of-queues *number-of-queues*	Configures the number of expedite queues.
no priority-queue out num-of-queues	Use the no form of this command to restore the default configuration.
wrr-queue bandwidth *weight1 weight2 ... weight_n* **no wrr-queue bandwidth**	Assigns WRR weights to egress queues. Use the no form of this command to restore the default configuration.

The following is an example of the CLI commands:

```
console(config)# priority-queue out num-of-queues 2
console(config-if)# wrr-queue bandwidth 6 6 6 6 6 6
```

CoS to Queue

The **CoS to Queue** page maps CoS priorities to an egress queue, meaning that the egress queues of the incoming packets is based on the CoS priority in their VLAN Tags. For incoming, untagged packets, the CoS priority is the default CoS priority assigned to ingress ports.

By changing CoS to Queue mapping, Queue schedule method, and bandwidth allocation, it is possible to achieve the desired quality of services in a network.

The CoS to Queue mapping is applicable only if one of the following exists:

- The switch is in QoS Basic mode, and CoS is the trusted mode.
- The switch is in QoS Advanced mode, and the packets belong to flows that are CoS trusted.

To map CoS values to egress queues:

1. Click **Quality of Service** > **General** > **CoS to Queue** in the tree view to display the **CoS to Queue** page.

   The CoS/queue mappings are displayed.

2. Enter the fields:

   – **Class of Service** — The CoS priority tag values, where zero is the lowest priority and 7 is the highest priority.

   – **Queue** — The queue to which the CoS priority is mapped.

Mapping CoS Priorities to Queues Using CLI Commands

The following table summarizes the CLI commands for configuring fields in the **CoS to Queue** page.

Table 22-4. CoS to Queue CLI Commands

CLI Command	Description
wrr-queue cos-map *queue-id cos0 ... cos7* **no wrr-queue cos-map** [*queue-id*]	Maps CoS values to the egress queues. Use the no form of this command to restore the default configuration.

The following is an example of the CLI commands:

```
console(config)# wrr-queue cos-map 4 7
```

The following is an example of the CLI commands:

```
console(config)# wrr-queue cos-map 4 7
```

DSCP to Queue

The DSCP to Queue mapping determines the egress queues of the incoming IP packets, based on their DSCP values. The original VPT (VLAN Priority Tag) of the packet is unchanged.

By changing the DSCP to Queue mapping, the Queue schedule method, and bandwidth allocation, it is possible to achieve improved quality of service in a network.

Non-IP packets are always classified to the best-effort queue.

The DSCP to Queue mapping is applicable to IP packets when:

- The switch is in Basic mode and DSCP is the trusted mode.
- The switch is in Advanced mode and the packets belongs to flows that are DSCP trusted

To map DSCP to queues:

1 Click **Quality of Service** > **General** > **DSCP to Queue** in the tree view to display the **DSCP to Queue** page.

The DSCP values in the incoming packet and its associated queues are displayed.

2 Enter the fields:

- **DSCP In** — The values of the DSCP field in the incoming packet.
- **Queue** — The queue to which packets with the specific DSCP value is assigned. The values are 1-4 for the R1-2401 device and 1-8 for the R1-2210 device, where 1 is the lowest value, and 4 and 8 are the highest values.

Mapping DSCP Values to Queues Using CLI Commands

The following table summarizes the CLI commands for configuring fields in the **DSCP to Queue** page.

Table 22-5. DSCP to Queue CLI Commands

CLI Command	Description
`qos map dscp-queue` *`dscp-list`* `to` *`queue-id`*	Modifies the DSCP to queue mapping.
`no qos map dscp-queue [`*`dscp-list`*`]`	Use the no form of this command to restore the default configuration.

The following is an example of the CLI command:

```
console(config)# qos map dscp-queue 33 40 41 to 1
```

Bandwidth

The amount of traffic that can be received and transmitted on an interface can be limited by the following:

- **Ingress Rate Limit** — Number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded.
- **Egress Shaping Rates** is defined by the following:
  - Committed Information Rate (CIR) sets the average maximum amount of data allowed to be sent on the egress interface, measured in bits per second
  - Committed Burst Shape (CBS) sets the maximum burst of data that is allowed to be sent, even though it is above the CIR. This is defined in number of bytes of data.

To configure bandwidth limitation:

1. Click **Quality of Service > General > Bandwidth** in the tree view to display the **Bandwidth: Summary** page.

   The ingress and egress rates are displayed for all ports.

2. To set interface parameters, click **Edit**.
3. Select an interface, and enter the fields:
   - **Enable Ingress Rate Limit** — Enable/disable ingress traffic limit for the interface. If this field is selected, enter the Ingress Rate Limit.
   - **Ingress Rate Limit** — Enter the ingress traffic limit for the interface.
   - **Enable Egress Shaping Rate** — Enable/disable egress traffic limitation. If this field is selected, enter the following fields.
   - **Committed Information Rate (CIR)** — Enter the average maximum amount of data allowed to be sent on the egress interface, measured in bits per second.
   - **Committed Burst Size (CBS)** — Enter the maximum burst of data that is allowed to be sent on the egress interface, even though it is above the CIR. This is defined in number of bytes of data.

Configuring Bandwidth Using CLI Commands

The following table summarizes the CLI commands for configuring fields in the **Bandwidth** pages.

Table 22-6. Bandwidth CLI Commands

CLI Command	Description
traffic-shape *committed-rate* [*committed-burst*] **no traffic-shape**	Sets shaper on egress port. Use no form in order to disable the shaper.
rate-limit *committed-rate-kbps* [***burst*** *committed-burst-byte*] **no rate-limit**	Limits the rate of the incoming traffic. Use the **no** form to disable rate limit.

The following is an example of the CLI commands:

```
console(config)# interface gi0/5
console(config-if)# traffic-shape 124000 9600
console(config-if)# rate-limit 150000
```

TCP Congestion Avoidance

Use the **TCP Congestion Avoidance** page to activate a congestion avoidance algorithm. The algorithm breaks up or prevents TCP global synchronization in a congested node, where the congestion is due to various sources sending packets with the same byte count.

To configure TCP congestion avoidance:

1. Click **Quality of Service** > **General** > **TCP Congestion Avoidance** in the tree view to display the **TCP Congestion Avoidance** page.

> **NOTE:** TCP Congestion Avoidance increases network reliability, but it also increases network traffic. Continue only if you are sure it will improve overall network performance. For this change to be effective you must save the configuration and reboot the device.

2. Check **TCP Congestion Avoidance** to enable the algorithm.

Configuring TCP Congestion Avoidance Using CLI Commands

The following table summarizes the CLI commands for configuring fields in the **TCP Congestion Avoidance** page.

Table 22-7. TCP Congestion Avoidance CLI Commands

CLI Command	Description
`qos wrr-queue wrtd`	Enables Weighted Random Tail Drop (WRTD).
`no qos wrr-queue wrtd`	Use the no form of this command to disable WRTD.

The following is an example of the CLI commands:

```
console(config)# qos wrr-queue wrtd
This setting will take effect only after copying
running configuration to startup configuration and
resetting the device.
```

QoS Basic Mode

This section describes QoS Basic mode.

It contains the following topics:

- Overview
- Global Settings
- DSCP Rewrite
- Interface Settings

Overview

In QoS Basic mode, a specific domain in the network can be defined as trusted. Within that domain, packets are marked with CoS priority and/or DSCP values, to signal the type of service they require. Nodes within the domain use these fields to assign the packet to a specific output queue. The initial packet classification and marking of these fields is done in the ingress of the trusted domain.

Workflow to Configure Basic Mode

To configure Basic QoS mode, perform the following:

1. Select Basic mode for the system in the **QoS Mode** page.
2. Select the trust-behavior in the **Global Settings** page.
3. If there is any port that, as an exception, should not trust the incoming CoS mark, disable the QoS state on that port in the **Interface Settings** pages.

   If a port is disabled without trusted mode, all its ingress packets are forwarded in best effort. It is recommended that you disable the trusted mode at the ports where the CoS and/or DSCP values in the incoming packets are not trustworthy. Otherwise, performance in the network might be negatively affected.
4. If you selected DSCP Rewrite in the **Global Settings** page, set the DSCP in/out values in the **DSCP Rewrite** page.

Global Settings

Use the **Global Settings** page to enable Trust on all interfaces on the switch. This configuration is only active when the QoS mode is Basic. Packets entering a QoS domain are classified at the edge of the QoS domain.

For more information on setting Trust mode on an interface, see Interface Settings.

To define Trust configuration:

1. Click **Quality of Service** > **QoS Basic Mode** > **Global Settings** in the tree view to display the **Global Settings** page.
2. Enter the fields:
   - **Trust Mode** — Enable/disable Trust mode.
     - **CoS** — Traffic is mapped to queues, based on the VPT field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet). The mapping of the VPT to queue can be configured in the **CoS to Queue** page.
     - **DSCP** — All IP traffic is mapped to queues, based on the DSCP field in the IP header. The mapping of the DSCP to queue is configured in the **DSCP to Queue** page.
   - **Always Rewrite DSCP** — Check to always rewrite the DSCP values in the incoming packets with the new values set in the **DSCP to Queue** page. When this field is enabled, the switch uses the new DSCP values to select the egress queue.

Assigning Global Settings Using CLI Commands

The following table summarizes the CLI commands for configuring fields in the **Global Settings** page.

Table 22-8. Global Settings CLI Commands

CLI Command	Description

`qos trust {cos|dscp}`
`no qos trust`
	Configures the system to either the CoS or DSCP trust state.
	Use the no form of this command to return to the default configuration.

Table 22-8. Global Settings CLI Commands *(continued)*

CLI Command	Description

`qos dscp-mutation`
`no qos dscp-mutation`
	Applies the DSCP Mutation map to system DSCP trusted ports.
	Use the no form of this command to restore the trusted port with no DSCP mutation.

The following is an example of the CLI commands:

```
console(config)# qos trust dscp
console(config)# qos dscp-mutation
```

DSCP Rewrite

Use the **DSCP Rewrite** page to rewrite the DSCP tags for incoming traffic, when different DSCP values are used in the incoming and outgoing domains. Changing the DSCP value used in one domain to the DSCP value used in the other domain preserves the priority of traffic used in the first domain.

As an example, assume that there are three levels of service: Silver, Gold, and Platinum. The DSCP incoming values used to mark these levels are 10, 20, and 30 respectively. If this traffic is forwarded to another service provider that has the same three levels of service, but uses DSCP values 16, 24, and 48, the values set in the **DSCP Rewrite** page are used to change the incoming values to the outgoing values.

These settings are active globally when the system is in QoS Basic mode.

To map DSCP In values to DSCP Out values:

1 Click **Quality of Service > QoS Basic Mode > DSCP Rewrite** in the tree view to display the **DSCP Rewrite** page.

2 For each **DSCP In** value (DSCP value of the incoming packet) that needs to be rewritten to an alternative value, set a **DSCP Out** value.

Assigning DSCP Rewrite Values Using CLI Commands

The following table summarizes the CLI commands for configuring fields in the **DSCP Rewrite** page.

Table 22-9. DSCP Rewrite CLI Commands

CLI Command	Description
qos map dscp-mutation *in-dscp* **to** *out-dscp*	Configures the DSCP to DSCP Mutation table.
no qos map dscp-mutation [*in-dscp*]	Use the no form of this command to restore the default configuration.

The following is an example of the CLI commands:

```
 console(config)# qos map dscp-mutation 1 2 4 5 6 to
63
```

Interface Settings

QoS Trust mode can be configured on each port of the switch, as follows:

- **QoS Trust State Disabled on an Interface** — All inbound traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.
- **QoS Trust State Enabled on an Interface** — Port prioritized traffic on ingress is based on the system- wide configured trusted mode, which is either CoS Trusted mode or DSCP Trusted mode.

To define QoS Trust for an interface:

1. Click **Quality of Service > QoS Basic Mode > Interface Settings** in the tree view to display the **Interface Settings: Summary** page.

   Trust mode is displayed for all interfaces.

2. To change the QoS trust state for an interface, click **Edit**, and select an interface.
3. Enable/disable the **QoS Trust State**.

Configuring QoS Basic Mode Using CLI Commands

The following is a sample script configuring QoS Basic mode.

Table 22-10. Sample CLI Script to Configure QoS Basic Mode

CLI Command	Description
`console#configure`	Enable QoS in Basic mode.
`console(config)# qos basic`	
`console(config)#mac access-list extended MAC1`	Define an ACL named "MAC1"
`console(config-mac-a1)#deny 00:00:00:00:00:11 00:00:00:00:00:ff any`	MAC1 discards all traffic with source MAC 00:00:00:00:00:XX addresses.
`console(config-mac-a1)# permit any any`	MAC1 permits all other traffic.
`console(config-mac-a1)#exit`	Exit ACL mode.
`console(config)#interface gi0/1`	Enter Interface mode on port gi0/1.
`console(config-if)#service-acl input mac1`	Bind MAC1 to port gi0/1.

QoS Advanced Mode

This section describes QoS Advanced mode.

It contains the following topics:

- Overview
- DSCP Mapping
- Class Mapping
- Aggregate Policer
- Policy Table
- Policy Class Maps
- Policy Binding

Overview

In Advanced mode, the switch uses policies to support per-flow QoS. A policy and its components have the following characteristics and relationships:

- A policy contains one or more class maps.
- A class map defines a flow with one or more associated ACLs. Packets that match the ACL rules (ACEs) in a class map with Permit (forward) action, belong to the same flow, and are subject to the same quality of service action. A policy can contain one or more flows, each with a user-defined QoS action.
- The QoS of a class map (flow) may be enforced by the associated policer. There are two type of policers, as described in Defining Class Mapping Using CLI Commands.
- Per-flow QoS actions are applied to flows by binding the policy maps to the desired ports. A policy map and its class maps can be bound to one or more ports, but each port is bound with, at the most, one policy map.

The following points should be considered:

- An ACL can be configured to one or more class maps, regardless of policies.
- A class map can belong to only one policy map.
- When a class map, using a single policer, is bound to multiple ports, each port has its own instance of the policer. Each instance applies the QoS actions on the class map (flow) at a port independent of each other.
- If you bind a policy map to more than one port and one of its classes contains a single policer, all policy map rules will be multiplied per port (using up more TCAM resources).
- An aggregate policer applies the QoS to all of its flows in aggregation, regardless of policies and ports.

Advanced QoS settings consist of the following elements:

- Rules — All frames matching a single group of rules are considered to be a flow.
- Actions — To be applied to frames in each flow that match the rules.
  - **Policers** — See Defining Class Mapping Using CLI Commands
  - **Aggregate Policers** — Defining Class Mapping Using CLI Commands

  - **Trust** —Interface Settings, Policy Class Maps
  - **Set DSCP/CoS** — Policy Class Maps
  - **Set Queue** — DSCP Mapping
- Binding — Combination of rules and actions that are bound to one or more interfaces.

Workflow to Configure Advanced QoS Mode

To configure Advanced QoS mode, perform the following:

1. Select Advanced mode for the system in the **QoS Mode** page.
2. If external DSCP values are different from those used on incoming packets, map the external values to internal values in the **DSCP Rewrite** page.
3. Create ACLs, as described in ACLs.
4. When ACLs are defined, create class maps and associate the ACLs with them in the **Class Mapping** pages.
5. Create a policy map in the **Policy Class Maps** pages, and associate the policy map with one or more class maps. Specify the QoS action, if needed, for example by assigning a policer to a class map, when you associate the class map to the policy.
   - a **Single Policer** — Create a policy that associates a class map with a single policer in the **Policy Table** pages and the **Class Mapping** pages. Within the policy, define the single policer.
   - b **Aggregate Policer** — Create a QoS action for each flow. This action sends all matching frames to the same policer (aggregate policer), defined in the **Aggregate Policer** pages. Create a policy that associates a class map with the aggregate policer in the **Policy Table** pages.
6. Bind the policy to an interface in the **Policy Binding** pages.

DSCP Mapping

When a policer is assigned to a class map (flow), you can specify the action to take when the amount of traffic in the flow(s) exceeds the QoS-specified limits. The portion of the traffic that causes the flow to exceed its QoS limit is referred to as **out-of-profile packet***s*.

If the exceed action is **Remark DSCP** (as opposed to **Drop**), the switch rewrites the original DSCP value of the out-of-profile IP packets to a new value, based on the values entered in the **DSCP Mapping** page. The switch uses the new values to assign resources and egress queues to these packets. The switch physically replaces the original DSCP value in the out-of-profile packets with the new DSCP value.

To use the **Remark DSCP** exceed action, set the DSCP Out value in the **DSCP Mapping** page. Otherwise the action is null, because the DSCP value in the packet is rewritten to the original DSCP value, set by factory default.

To set new DSCP values:

1. Click **Quality of Service > QoS Advanced Mode > DSCP Mapping** to display the **DSCP Mapping** page.
2. If the **Exceed Action** is **Out-of-Profile** (in the *Policy Class Maps* page) or **Remark DSCP** (in the *Aggregate Policy* page), the **DSCP In** values are rewritten with the **DSCP Out** values. Set the **DSCP Out** values as required.

Configuring DSCP Mapping Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **DSCP Mapping** page.

Table 22-11. DSCP Mapping CLI Commands

CLI Command	Description
`qos map policed-dscp` *`dscp-list`* **`to`** *`dscp-mark-down`*	Configures the policed-DSCP map for remarking purposes.
`no qos map policed-dscp` `[`*`dscp-list`*`]`	Use the no form of this command to restore the default configuration.

The following is an example of the CLI commands:

```
console(config)# qos map policed-dscp 3 to 43
```

Class Mapping

A Class Map defines a traffic flow associated with ACL(s). A MAC-based ACL, IP-based ACL, and an IPv6-based ACL can be combined into a class map. Class maps are configured to match packet criteria on a match-all or match-any basis. They are matched to packets on a first-fit basis, meaning that the action associated with the first-matched class map is the action performed by the system. Packets that match the same class map belong to the same flow.

There are two possible types of matching:

- **match-all** — Traffic matches class map if it matches IP/IPV6 and MAC ACLs
- **match-any** — Traffic matches class map if it matches at least one of the ACLs

If a more complex set of rules is needed, several class maps can be grouped into a super-group called a policy (see Defining Class Mapping Using CLI Commands).

To define a class map:

1. Click **Quality of Service** > **QoS Advanced Mode** > **Class Mapping** to display the **Class Mapping: Summary** page.

   The previously-defined class maps are displayed.

2. To add a class map, click **Add**.

   A new class map is added by selecting one or two ACLs and assigning them a class map name. If a class map has two ACLs, specify that a frame must match both ACLs, or that it must match either one or both of the ACLs selected.

3. Enter the parameters.

   – **Class Map Name** — Enter the name of a new class map.

- **Match ACL Type** — Enter the criteria that a packet must match in order to belong to the flow defined by the class map. The possible options are:
  - **IP** — A packet must match either of the IP-based ACLs in the class map.
  - **MAC** — A packet must match the MAC-based ACL in the class map.
  - **IP and MAC** — A packet must match the IP-based ACL and the MAC-based ACL in the class map (match-all).
  - **IP or MAC** — A packet must match either the IP-based ACL or the MAC-based ACL in the class map (match-any).
- **IP ACL** — Select the IPv4-based ACL or the IPv6-based ACL for the class map.
- **MAC ACL** — Select the MAC-based ACL for the class map.
- **Preferred ACL** — Select whether packets are first matched to an IP-based ACL or a MAC-based ACL.

Defining Class Mapping Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **Class Mapping** pages.

Table 22-12. Class Mapping CLI Commands

CLI Command	Description
class *class-map-name* [***access-group*** *acl-name*] **no class** *class-map-name*	Defines a traffic classification and enters the Policy-map Class Configuration mode. Use the no form of this command to detach a class map from the policy map.
class-map *class-map-name* [***match-all***|***match-any***] **no class-map** *class-map-name*	Creates or modifies a class map and enters the Class-map Configuration mode. Use the no form of this command to delete a class map.

Table 22-12. Class Mapping CLI Commands *(continued)*

CLI Command	Description
match access-group *acl-name* **no match access-group** *acl-name*	Defines the match criteria for classifying traffic. Use the no form of this command to delete the match criteria.
show class-map [*class-map-name*]	Displays information about the class map.

The following is an example of the CLI commands:

```
console(config)# qos advanced
console(config)# class-map class1 match-all
console(config-cmap)# match access-group enterprise
console(config-cmap)# do show class-map class1
Class Map matchAll class1
Match access-group enterprise
```

Aggregate Policer

The rate of traffic that matches a pre-defined set of rules can be measured, and limits, such as limiting the rate of file-transfer traffic that is allowed on a port, can be enforced.

This is done by using the ACLs in the class map(s) to match the desired pattern of traffic, and by using a policer to apply QoS on the matching traffic.

A policer is configured with a QoS specification. There are two kinds of policers:

- **Single Policer** — A single policer applies the QoS to a single class map, and to a single flow, based on the policer's QoS specification. When a class map, using a single policer, is bound to multiple ports, each port has its own instance of the single policer; each applying the QoS on the class map (flow) at ports that are otherwise independent of each other. A single policer is created in the **Policy Table** and **Policy Class Maps** pages.

- **Aggregate Policer** — An aggregate policer applies QoS to one or more class maps, and to one or more flows. An aggregation policer can support class maps from various policies. An aggregate policer applies QoS to all its flow(s) in aggregation, regardless of policies and ports. An aggregate policer is created in the **Aggregate Policer** pages.

  An aggregate policer is defined if the policer is to be shared with more than one class.

Each policer is defined with its own QoS specification, and is composed of a combination of the following parameters:

- **Committed Information Rate (CIR)** — A maximum allowed rate of traffic, measured in Kbps.
- **Committed Burst Size (CBS)** — An amount of traffic, measured in bytes, which is allowed to pass as a temporary burst, even if it is above the defined maximum rate.
- **Exceed Action** — An action to be applied to frames that are over the limits (called out-of-profile traffic). These frames can be forwarded as is, dropped, or forwarded, after rewriting their DSCP value with a value that marks them as lower-priority frames for all subsequent handling within the device.

A policer is assigned to a class map when a class map is added to a policy**.**

To define an aggregate policer:

1. Click **Quality of Service > QoS Advanced Mode > Aggregate Policer** to display the **Aggregate Policer: Summary** page.

   The existing aggregate policers are displayed.

2. To add an aggregate policer, click **Add**, and enter the fields.
   - **Aggregate Policer Name** — Enter the name of the Aggregate Policer.
   - **Committed Information Rate (CIR)** — Enter the maximum bandwidth allowed in bits per second. See the description of this field in Bandwidth.
   - **Committed Burst Size (CBS)** — Enter the maximum burst size (even if it goes beyond the CIR) in bytes. See the description of this in the Bandwidth.

- **Exceed Action** — Select the action to be performed on incoming packets that exceed the CIR. The possible options are:
  - **None** — No action is performed on packets exceeding the defined CIR value.
  - **Drop** — Packets exceeding the defined CIR value are dropped.
  - **Remark DSCP** — The DSCP values of packets exceeding the defined CIR value are rewritten to a value entered in the **DSCP Mapping** pages.

Defining Aggregate Policers Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **Aggregate Policer** pages.

Table 22-13. Aggregate Policer CLI Commands

CLI Command	Description
qos aggregate-policer *aggregate-policer-name committed-rate-kbps excess-burst-byte*[**exceed-action** {**drop**|**policed-dscp-transmit**}] **no qos aggregate-policer** *aggregate-policer-name*	Defines the policer parameters that can be applied to multiple traffic classes within the same policy map. Use the no form of this command to remove an existing aggregate policer.

The following is an example of the CLI commands:

```
console(config)# qos aggregate-policer policer1
124000 9600 exceed-action drop
```

Policy Table

To create a single policer:

1. Create a policy in the **Police Table** pages
2. Configure the policy in the **Policy Class Maps** pages. Here the policy class can be designated as containing a single policer, or it can be designated as containing Aggregate policers.

A policy can consist of one of the following:

- One or more class maps of ACLs that define the traffic flows in the policy.

- One or more aggregate policers that apply the QoS to the traffic flows in the policy.

Only those policies that are bound to an interface are active (see the **Policy Binding** pages).

After a policy has been added, class maps can be added in the **Policy Table** pages.

To create a QoS policy:

1. Click **Quality of Service > QoS Advanced Mode > Policy Table** to display the **Policy Table: Summary** page.

   The previously-defined policies are displayed.

2. To create a policy, click **Add**.
3. Enter the name of the new policy in the **Policy Name** field.
4. Add class maps to the new policy in the **Policy Class Maps** page.

Defining Policies Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **Policy Table** page.

Table 22-14. Policy Table CLI Commands

CLI Command	Description
policy-map *policy-map-name* **no policy-map** *policy-map-name*	Creates a policy map and enters the Policy-map Configuration mode. Use the no form of this command to delete a policy map.

The following is an example of the CLI commands:

```
console(config)# policy-map policy1
```

Policy Class Maps

One or more class maps can be added to a policy. A class map defines the type of packets that are considered to belong to the same traffic flow.

To add a class map to a policy:

1. Click **Quality of Service** > **QoS Advanced Mode** > **Policy Class Maps** to display the **Policy Class Maps: Summary** page.
2. Select a policy in the **Policy Name** field. The class maps in that policy are displayed.
3. To add a class map, click **Add**.
4. Enter the parameters.
   - **Policy Name** — Select the policy to which the class map is being added.
   - **Class Map Name** — Select an existing class map to be associated with the policy. Class maps are created in the **Class Mapping** pages.
   - **Action Type** — Select the action regarding the ingress CoS and/or DSCP value of all the matching packets.
     - **None** — Ignore the ingress CoS and/or DSCP value. The matching packets are sent as best effort.
     - **Trust CoS-DSCP** — If this option is selected, the switch will trust the CoS or DSCP value of the matching packet. If a packet is an IP packet, the switch will put the packet in the egress queue, based on its DSCP value and the DSCP to Queue mapping. Otherwise, the egress queue of the packet is based on the packet's CoS value and the CoS to Queue mapping.
     - **Set** — See the description of this field below.
   - **Set** — If this option is selected, enter a **New Value**, which determines the egress queue of the matching packets:
     - **DSCP** — If DSCP is selected, the new DSCP value and the DSCP to Queue mapping determines the egress queue of the matching packets.
     - **Queue** — If Queue is selected, the new value is the egress queue number for all matching packets.
     - **CoS** — If CoS is selected, the CoS priority value and the CoS to Queue mapping determines the egress queue of the matching packets.

- **Police Type (Only in L2 and R1-2210)**— Available in Layer 2 Mode only. Select the policer type for the policy. The possible options are:
  - **None** — No policy is used.
  - **Single** — The policer for the policy is a single policer.
  - **Aggregate** — The policer for the policy is an aggregate policer.
- **Aggregate Policer (Only in L2 and R1-2210)** — Available in Layer 2 Mode only. If Police Type is **Aggregate**, select a previously-defined aggregate policer.

If **Police Type** is Single, enter the following QoS parameters:

- **Ingress Committed Information Rate (CIR) (3 - 10485760) (Only in L2 and R1-2210)** — Enter the CIR in Kbps. See its description in the **Bandwidth** pages.
- **Ingress Committed Burst Size (CBS) (3000 - 16769020) (Only in L2 and R1-2210)** — Enter the CBS in bytes. See its description in the **Bandwidth** pages.
- **Exceed Action (Only in L2 and R1-2210)** — Select the action assigned to incoming packets exceeding the CIR. The possible options are:
  - **None** — No action.
  - **Drop** — Packets exceeding the defined CIR value are dropped.
  - **Out-of-Profile DSCP** — Packets, exceeding the defined CIR, are forwarded with a new DSCP, derived from the **DSCP Mapping** pages.

Defining Policy Class Maps Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **Policy Class Maps** pages.

Table 22-15. Policy Class Maps CLI Commands

CLI Command	Description

`class` *`class-map-name`* `[access-group` *`acl-name`*`]`
`no class class-map-name`
	Defines a traffic classification and enters the Policy-map Class Configuration mode.
	Use the no form of this command to detach a class map from the policy map.

`trust [`*`cos-dscp`*`]`
`no trust`
	Configures the trust state, which selects the value that QoS uses as the source of the internal DSCP value.
	Use the no form of this command to return to the default trust state.

`set {dscp` *`new-dscp`*`|queue` *`queue-id`*`|cos` *`new-cos`*`}`
`no set`
	Sets new values in the IP packet.
	Use the no form of this command to return to the default values.

`police` *`committed-rate-kbps committed-burst-byte`* `[exceed-action {`*`drop`*`|`*`policed-dscp-transmit`*`}]`
`no police`
	Defines the policer for classified traffic.
	Use the no form of this command to remove a policer.

`qos aggregate-policer` *`aggregate-policer-name committed-rate-kbps excess-burst-byte`* `[exceed-action {`*`drop`*`|`*`policed-dscp-transmit`*`}]`
`no qos aggregate-policer` *`aggregate-policer-name`*
	Defines the policer parameters that can be applied to multiple traffic classes.
	Use the no form of this command to remove an existing aggregate policer.

`show policy-map [`*`policy-map-name`*`]`	Displays all policy maps or a specific policy map.

The following is an example of the CLI commands:

```
console(config)# policy-map policy1

console(config-pmap)# class class1 access-group
enterprise

console(config-pmap)# trust cos-dscp

console(config-pmap)# set dscp 56

console(config-pmap)# class class1

console(config-pmap-c)# police 124000 9600 exceed-
action drop

console(config)# qos aggregate-policer policer1
124000 9600 exceed-action drop
```

Policy Binding

After policies are created, they must be bound to interfaces (ports or LAGs).When a policy is bound to a specific interface, it becomes active on it (subject to time range restrictions). Only one policy can be active on a single interface, but a single policy can be bound to more than one interface.

When a policy is bound to an interface, it filters and applies QoS to ingress traffic that belongs to the flows defined in the policy. The policy does not apply to traffic egress to the same port.

To edit a policy, it must first be removed (unbound) from all those ports to which it is bound.

To define policy binding:

1. Click **Quality of Service > QoS Advanced Mode > Policy Binding** to display the **Policy Binding: Summary** page.

   Previously-defined policy bindings are displayed.

2. To bind a policy to an interface, click **Add**.
3. Select the interface assigned to the policy.
4. Select the **Policy Name** to be activated on the interface.

Defining Policy Binding Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **Policy Binding** pages.

Table 22-16. Policy Binding CLI Commands

CLI Command	Description
service-policy input *policy-map-name*	Applies a policy map to the input of a particular interface.
no service-policy input	Use the no form of this command to detach a policy map from an interface.

The following is an example of the CLI commands:

```
console(config-if)# service-policy input policy1
```

QoS Statistics

This section describes how to view and manage QoS statistics.

It contains the following topics:

- Policer Statistics
- Aggregated Policer
- Queues Statistics

Policer Statistics

A Single Policer is bound to a class map from a single policy. An Aggregate Policer is bound to one or more class maps from one or more policies.

Use the **Policer Statistics** pages to view the number of in-profile and out-of-profile packets received from an interface that meet the conditions defined in the class map of a policy.

To view policer statistics:

1 Click **Quality of Service** > **QoS Statistics** > **Policer Statistics** to display the **Policer Statistics: Summary** page.

  The following statistics for the previously-defined counters are displayed:

  – **Interface** — Statistics are displayed for this interface.

- **Policy** — Statistics are displayed for this policy.
- **Class Map** — Statistics are displayed for this class map.
- **In-Profile Bytes** — Number of in-profile bytes received.
- **Out-of-Profile Bytes** — Number of out-of-profile bytes received.

2 Click **Add** to add a new counter that applies to another policy-class map.

3 Enter the fields:

- **Interface** — Select the interface for which the counter is defined.
- **Policy - Class Map Name** — Select a policy class map pair.

Defining Policer Statistics Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **Policer Statistics** pages.

Table 22-17. Policer Statistics CLI Commands

CLI Command	Description
qos statistics policer policy-map-name class-map-name	Enables counting in-profile and out-of-profile bytes vis-a-vis a policer.
no qos statistics policer policy-map-name class-map-name	Use the no form of this command to disable counting.
clear qos statistics	Clears the statistics
show qos statistics	Displays the statistics

The following is an example of the CLI commands:

```
console(config-if)# qos statistics policer policy1
class1
```

Aggregated Policer

To view aggregated policer statistics:

1 Click **Quality of Service** > **QoS Statistics** > **Aggregate Policer** to display the **Aggregate Policer: Summary** page.

The following statistics for the previously-defined counters are displayed:

- **Aggregate Policer Name** — Policer on which statistics are based.

- **In-Profile Bytes** — Number of in-profile packets that were received.
- **Out-of-Profile Bytes** — Number of out-of-profile packets that were received.

2 To add a new counter that applies to another aggregate policer, click **Add**.

3 Select an aggregate policer in the Aggregate Policer Name field.

Defining Aggregate Policer Statistics Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **Aggregate Policer Statistics** pages.

Table 22-18. Aggregate Policer Statistics CLI Commands

CLI Command	Description

`qos statistics aggregate-policer` *`aggregate-policer-name`*
`no qos statistics aggregate-policer` *`aggregate-policer-name`*
	Enables counting in-profile and out-of-profile bytes vis-a-vis an aggregate policer.
	Use the no form of this command to disable counting.

`clear qos statistics`	Clears the statistics
`show qos statistics`	Displays the statistics

The following is an example of the CLI commands:

```
console (config)# qos statistics aggregate-policer policer1
```

Queues Statistics

Queue statistics include statistics of forwarded and dropped packets, based on interface, queue, and drop precedence. Lowest drop precedence has the lowest probability of being dropped.

To view Queue Statistics:

1 Click **Quality of Service** > **QoS Statistics** > **Queues Statistics** to display the **Queues Statistics: Summary**.

The statistics for previously-defined counters are displayed.

- **Counter Set** —Number of counter.
- **Port** —Number of port.

- **Queue** —Number of queue.
- **Total Packets** —Number of packets forwarded or tail dropped.
- **Tail Drop Packets** —Percentage of packets that were tail dropped.

2. To add a new counter, click **Add**, and enter the fields:
   - **Counter Set**—Select the counter set. The possible options are:
     - **Set 1** — Displays the statistics that contains all interfaces and queues with a high DP (Drop Precedence).
     - **Set 2** — Displays the statistics that contains all interfaces and queues with a low DP.
   - **Interface** — Select the interface for which Queue statistics are displayed.
   - **Queue** — Select the queue on which packets were forwarded or tail dropped.

Defining QoS Statistics Using CLI Commands

The following table summarizes the CLI commands for setting the fields in the **QoS Statistics** pages.

Table 22-19. QoS Statistics CLI Commands

CLI Command	Description
qos statistics queues *set-number {queue|**all**} {dp|**all**}* {interface_id|***all***} **no qos statistics queues** *set-number*	Enables QoS statistics for output queues. Use the no form of this command to disable QoS statistics for output queues.
clear qos statistics	Clears the statistics
show qos statistics	Displays the statistics

The following is an example of the CLI commands:

```
console(config)# qos statistics queues 1 all all all
```

23

Getting Help

Contacting Dell

NOTE: Dell provides several online and telephone-based support and service options. If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog. Availability varies by country and product, and some services may not be available in your area.

To contact Dell for sales, technical support, or customer-service issues:

1. Go to **dell.com/support**.
2. For customized support:
   - a. Enter your system service tag in the **Enter your Service Tag** field.
   - b. Click **Submit**.

     The support page that lists the various support categories is displayed.
3. For general support:
   - a. Select your product category.
   - b. Select your product segment.
   - c. Select your product.

     The support page that lists the various support categories is displayed.

Locating Your System Service Tag

Your system is identified by a unique Express Service Code and Service Tag number. The Express Service Code and Service Tag are found on the front of the system by pulling out the information tag. Alternatively, the information may be on a sticker on the chassis of the system. This information is used by Dell to route support calls to the appropriate personnel.

Downloading Drivers, Firmware, and Software

1. Go to **dell.com/support**.
2. Enter your system service tag in the **Enter your Service Tag** field.
3. Click **Submit**.

   The support page that lists the various support categories is displayed.
4. From the left pane, select **Get drivers and downloads**.
5. Select your **filters**.
6. View by **Category**, **Importance**, or **Release Date**.

Related Documentation

⚠ **WARNING: See the safety and regulatory information that shipped with your system. Warranty information may be included within this document or as a separate document.**

NOTE: Ensure that all the component software are upgraded to the latest versions.

NOTE: Always check for updates on dell.com/support/manuals and read the updates first because they often supersede information in other documents.

Any media that ships with your system provides documentation and tools for configuring and managing your system, including those pertaining to the operating system, system management software, system updates, and system components that you purchased with your system.

The following guides are provided:

- *The Dell PowerEdge VRTX R1-2401 and R1-2210 Getting Started Guide* shipped with your system provides an overview of product features, setting up your product, and technical specifications.
- The *Dell PowerEdge VRTX R1-2401 CLI Reference Guide* and *Dell PowerEdge VRTX R1-2210 CLI Reference Guide* provide a description of all the CLI commands revelevant to the devices.

These documents are available online at dell.com/support/my-support/us/en/19/product-support/product/poweredge-vrtx/manuals.

Documentation Feedback

If you have feedback for this document, write to documentation_feedback@dell.com. Alternatively, you can click on the **Feedback** link in any of the Dell documentation pages, fill out the form, and click **Submit** to send your feedback.

Glossary

This glossary contains key technical words of interest.

A B C D E F G H I L M N O P Q

R S T U V W

A

Access Mode

Specifies the method by which user access is granted to the system.

Access Profiles

Allows network managers to define profiles and rules for accessing the switch module. Access to management functions can be limited to user groups, which are defined by the following criteria:

- Ingress interfaces
- Source IP address or Source IP subnets

ACL

Access Control List. Allow network managers to define classification actions and rules for specific ingress ports.

Aggregated VLAN

Groups several VLANs into a single aggregated VLAN. Aggregating VLANs enables routers to respond to ARP requests for nodes located on different sub-VLANs belonging to the same Super VLAN. Routers respond with their MAC address.

ARP

Address Resolution Protocol. A protocol that converts IP addresses into physical addresses.

ASIC

Application Specific Integrated Circuit. A custom chip designed for a specific application.

Asset Tag

Specifies the user-defined switch module reference.

Authentication Profiles

Sets of rules which that enables login to and authentication of users and applications.

Auto-negotiation

Allows 10/100 Mpbs or 10/100/1000 Mbps Ethernet ports to establish for the following features:

- Duplex/Half Duplex mode
- Flow Control
- Speed

B

Back Pressure

A mechanism used with Half Duplex mode that enables a port not to receive a message.

Backplane

The main BUS that carries information in the switch module.

Backup Configuration Files

Contains a backup copy of the switch module configuration. The Backup file changes when the Running Configuration file or the Startup Configuration file is copied to the Backup file.

Bandwidth

Bandwidth specifies the amount of data that can be transmitted in a fixed amount of time. For digital switch modules, bandwidth is defined in Bits per Second (bps) or Bytes per Second.

Bandwidth Assignments

The amount of bandwidth assigned to a specific application, user, or interface.

Baud

The number of signaling elements transmitted each second.

Best Effort

Traffic is assigned to the lowest priority queue, and packet delivery is not guaranteed.

Boot Version

The boot version.

BootP

Bootstrap Protocol. Enables a workstation to discover its IP address, an IP address of a BootP server on a network, or a configuration file loaded into the boot of a switch module.

BPDU

Bridge Protocol Data Unit. Provide bridging information in a message format. BPDUs are sent across switch module information with in Spanning Tree configuration. BPDU packets contain information on ports, addresses, priorities, and forwarding costs.

Bridge

A device that connect two networks. Bridges are hardware specific, however they are protocol independent. Bridges operate at Layer 1 and Layer 2 levels.

Broadcast Domain

device sets that receive Broadcast frames originating from any device within a designated set. Routers bind Broadcast domains, because routers do not forward Broadcast frames.

Broadcasting

A method of transmitting packets to all ports on a network.

Broadcast Storm

An excessive amount of Broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, overloading network resources or causing the network to time out.

C

CDB

Configuration Data Base. A file containing a device's configuration information.

Class of Service

Class of Service (CoS). Class of Service is the 802.1p priority scheme. CoS provides a method for tagging packets with priority information. A CoS value between 0-7 is added to the Layer II header of packets, where zero is the lowest priority and seven is the highest.

A overlapping transmission of two or more packets that collide. The data transmitted cannot be used, and the session is restarted.

CLI

Command Line Interface. A set of line commands used to configure the system. For more information on using the CLI, see **Using the CLI**.

Communities

Specifies a group of users which retains the same system access rights.

CPU

Central Processing Unit. The part of a computer that processes information. CPUs are composed of a control unit and an ALU.

D

DHCP Client

A device using DHCP to obtain configuration parameters, such as a network address.

DHCP Snooping

DHCP Snooping expands network security by providing firewall security between untrusted interfaces and DHCP servers.

DSCP

DiffServe Code Point (DSCP). DSCP provides a method of tagging IP packets with QoS priority information.

Domain

A group of computers and devices on a network that are grouped with common rules and procedures.

Duplex Mode

Permits simultaneous transmissions and reception of data. There are two different types of duplex mode:

- **Full Duplex Mode** — Permits for bisynchronous communication, for example, a telephone. Two parties can transmit information at the same time.
- **Half Duplex Mode** — Permits asynchronous communication, for example, a walkie-talkie. Only one party can transmit information at a time.

Dynamic VLAN Assignment (DVA)

Allows automatic assignment of users to VLANs during the RADIUS server authentication. When a user is authenticated by the RADIUS server, the user is automatically joined to the VLAN configured on the RADIUS server.

E

Egress Ports

Ports from which network traffic is transmitted.

End System

An end user device on a network.

Ethernet

Ethernet is standardized as per IEEE 802.3. Ethernet is the most common implemented LAN standard. Supports data transfer rates of Mpbs, where 10, 100 or 1000 Mbps is supported.

EWS

Embedded Web Server. Provides device management via a standard web browser. Embedded Web Servers are used in addition to or in place of a CLI or NMS.

F

FFT

Fast Forward Table. Provides information about forwarding routes. If a packet arrives to a device with a known route, the packet is forwarded via a route listed in the FFT. If there is not a known route, the CPU forwards the packet and updates the FFT.

FIFO

First In First Out. A queuing process where the first packet in the queue is the first packet out of the packet.

Flapping

Flapping occurs when an interfaces state is constantly changing. For example, an STP port constantly changes from listening to learning to forwarding. This may cause traffic loss.

Flow Control

Enables lower speed devices to communicate with higher speed devices, that is, that the higher speed device refrains from sending packets.

Fragment

Ethernet packets smaller than 576 bits.

Frame

Packets containing the header and trailer information required by the physical medium.

G

GARP

General Attributes Registration Protocol. Registers client stations into a Multicast domain.

Gigabit Ethernet

Gigabit Ethernet transmits at 1000 Mbps, and is compatible with existing 10/100 Mbps Ethernet standards.

GVRP

GARP VLAN Registration Protocol. Registers client stations into a VLANs.

H

HOL

Head of Line. Packets are queued. Packets at the head of the queue are forwarded before packets at the end of the line.

Host

A computer that acts as a source of information or services to other computers.

HTTP

HyperText Transport Protocol. Transmits HTML documents between servers and clients on the internet.

I

IC

Integrated Circuit. Integrated Circuits are small electronic devices composed from semiconductor material.

ICMP

Internet Control Message Protocol. Allows gateway or destination host to communicate with a source host, for example, to report a processing error.

IEEE

Institute of Electrical and Electronics Engineers. An Engineering organization that develops communications and networking standards.

IEEE 802.1d

Used in the Spanning Tree Protocol, IEEE 802.1d supports MAC bridging to avoid network loops.

IEEE 802.1p

Prioritizes network traffic at the data-link/MAC sublayer.

IEEE 802.1Q

Defines the operation of VLAN Bridges that permit the definition, operation, and administration of VLANs within Bridged LAN infrastructures.

IGMP Snooping

IGMP Snooping examines IGMP frame contents, when they are forwarded by the device from work stations to an upstream Multicast router. From the frame, the device identifies work stations configured for Multicast sessions, and which Multicast routers are sending Multicast frames.

Image File

System images are saved in two Flash sectors called images (Image 1 and Image 2). The active image stores the active copy; while the other image stores a second copy.

Ingress Port

Ports on which network traffic is received.

IP

Internet Protocol. Specifies the format of packets and there addressing method. IP addresses packets and forwards the packets to the correct port.

IP Address

Internet Protocol Address. A unique address assigned to a network device with two or more interconnected LANs or WANs.

IP Version 6 (IPv6)

A version of IP addressing with longer addresses than the traditional IPv4. IPv6 addresses are 128 bits long, whereas IPv4 addresses are 32 bits; allowing a much larger address space.

ISATAP

*Intra-Site Automatic Tunnel Addressing Protoco*l.
ISATAP is an automatic overlay tunneling mechanism that uses the underlying IPv4 network as a non-Broadcast/multicast access link layer for IPv6. ISATAP is designed for transporting IPv6 packets within a site where a native IPv6 infrastructure is not yet available.

L

LAG

Link Aggregated Group. Aggregates ports or VLANs into a single virtual port or VLAN.

For more information on LAGs, see **Defining LAG Membership**.

LAN

Local Area Networks. A network contained within a single room, building, campus or other limited geographical area.

Layer 2

Data Link Layer or MAC Layer. Contains the physical address of a client or server station. Layer 2 processing is faster than Layer 3 processing because there is less information to process.

Layer 3

Establishes a connections and ensures that all data arrives to their destination. Packets inspected at the Layer 3 level are analyzed and forwarding decisions, based on their applications.

LLDP-MED

Link Layer Discovery Protocol - Media Endpoint Discovery. LLDP allows network managers to troubleshoot and enhance network management by discovering and maintaining network topologies over multi-vendor environments. MED increases network flexibility by allowing different IP systems to co-exist on a single network LLDP.

Load Balancing

Enables the even distribution of data or processing packets across available network resources. For example, load balancing may distribute the incoming packets evenly to all servers, or redirect the packets to the next available server.

M

MAC Address

Media Access Control Address. The MAC Address is a hardware specific address that identifies each network node.

MAC Address Learning

MAC Address Learning characterizes a learning bridge, in which the packet's source MAC address is recorded. Packets destined for that address are forwarded only to the bridge interface on which that address is located. Packets addressed to unknown addresses are forwarded to every bridge interface. MAC Address Learning minimizes traffic on the attached LANs.

MAC Layer

A sub-layer of the *Data Link Control* (DTL) layer.

Mask

A filter that includes or excludes certain values, for example parts of an IP address.

MD5

Message Digest 5. An algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

MDI

Media Dependent Interface. A cable used for end stations.

MDIX

Media Dependent Interface with Crossover (MDIX). A cable used for hubs and switches.

MIB

Management Information Base. MIBs contain information describing specific aspects of network components.

Multicast

Transmits copies of a single packet to multiple ports.

Multicast TV VLAN

Multicast Television Vlan or TV VLAN, is used for television applications with a PC or with televisions equipped with a "Set-Top Box" device.

N

NA

Neighbor Advertisement.

ND

Neighbor Discovery.

NS

Neighbor Solicitation.

NMS

Network Management System. An interface that provides a method of managing a system.

Node

A network connection endpoint or a common junction for multiple network lines. Nodes include:

- Processors
- Controllers
- Workstations

O

OID

Organizationally Unique Identifiers. Identifiers associated with a Voice VLAN.

OUI

Object Identifier. Used by SNMP to identify managed objects. In the SNMP Manager/Agent network management paradigm, each managed object must have an OID to identify it.

P

Packets

Blocks of information for transmission in packet switched systems.

PDU

Protocol Data Unit. A data unit specified in a layer protocol consisting of protocol control information and layer user data.

PING

Packet Internet Groper. Verifies if a specific IP address is available. A packet is sent to another IP address and waits for a reply.

Port

Physical ports provide connecting components that allow microprocessors to communicate with peripheral equipment.

Port Mirroring

Monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

For more information on port mirroring, see **Defining Port Mirroring Sessions**.

Protocol

A set of rules that governs how devices exchange information across networks.

PVE

Protocol VLAN Edge. A port can be defined as a Private VLAN Edge (PVE) port of an uplink port, so that it will be isolated from other ports within the same VLAN.

Q

QoS

Quality of Service. QoS allows network managers to decide how and what network traffic is forwarded according to priorities, application types, and source and destination addresses.

Query

Extracts information from a database and presents the information for use.

R

RA

RADIUS Advertisement.

RD

RADIUS Discovery.

RS

Router Solicitation.

RADIUS

Remote Authentication Dial-In User Service. A method for authenticating system users, and tracking connection time.

RMON

Remote Monitoring. Provides network information to be collected from a single workstation.

Router

A device that connects to separate networks. Routers forward packets between two or more networks. Routers operate at a Layer 3 level.

RSTP

Rapid Spanning Tree Protocol. Detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops.

Running Configuration File

Contains all startup configuration file commands, as well as all commands entered during the current session. After the switch module is powered down or rebooted, all commands stored in the Running Configuration file are lost.

S

Segmentation

Divides LANs into separate LAN segments for bridging. Segmentation eliminates LAN bandwidth limitations.

Server

A central computer that provides services to other computers on a network. Services may include file storage and access to applications.

SNMP

Simple Network Management Protocol. Manages LANs. SNMP based software communicates with network devices with embedded SNMP agents. SNMP agents gather network activity and device status information, and send the information back to a workstation.

SNTP

Simple Network Time Protocol. SNTP assures accurate network switch clock time synchronization up to the millisecond.

SoC

System on a Chip. An ASIC that contains an entire system. For example, a telecom SoC application can contain a microprocessor, digital signal processor, RAM, and ROM.

Spanning Tree Protocol

Prevents loops in network traffic. The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP provides one path between end stations on a network, eliminating loops.

SSH

Secure Shell. Permits logging to another computer over a network, execute commands on a remote machine, and move files from one machine to another. Secure Shell provides strong authentication and secure communications methods over insecure channels.

Startup Configuration

Retains the exact switch module configuration when the switch module is powered down or rebooted.

Subnet

Sub-network. Subnets are portions of a network that share a common address component. On TCP/IP networks, devices that share a prefix are part of the same subnet. For example, all devices with a prefix of 157.100.100.100 are part of the same subnet.

Subnet Mask

Used to mask all or part of an IP address used in a subnet address.

Switch

Filters and forwards packets between LAN segments. Switches support any packet protocol type.

T

TCP/IP

Transmissions Control Protocol. Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order their sent.

Telnet

Terminal Emulation Protocol. Enables system users to log in and use resources on remote networks.

TFTP

Trivial File Transfer Protocol. Uses User Data Protocol (UDP) without security features to transfer files.

Trap

A message sent by the SNMP that indicates that system event has occurred.

Trunking

Link Aggregation. Optimizes port usage by linking a group of ports together to form a single trunk (aggregated groups).

TV VLAN

Multicast Television Vlan or *TV VLAN*, is used for television applications with a PC or with televisions equipped with a "Set-Top Box" device.

U

UDP

User Data Protocol. Transmits packets but does not guarantee their delivery.

Unicast

A form of routing that transmits one packet to one user.

V

VLAN

Virtual Local Area Networks. Logical subgroups with a Local Area Network (LAN) created via software rather than defining a hardware solution.

VoIP

Voice over IP.

W

WAN

Wide Area Networks. Networks that cover a large geographical area.

Wildcard Mask

Specifies which IP address bits are used, and which bits are ignored. A wild switch module mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important.

Printed in the U.S.A.

dell.com/support

5MM18A00