Part No. 060202-10 , Rev. D
June 2007

Alcatel OS-LS-6200

User Guide

ALCATEL

www.alcatel.com

An Alcatel service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners. Additionally, with 24-hour-a-day access to Alcatel's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel's technical support, open a new case or access helpful release notes, technical bulletins, and manuals. For more information on Alcatel's Service Programs, see our web page at www.ind.alcatel.com, call us at 1-800-995-2696, or email us at support@ind.alcatel.com.

This Manual documents Alcatel 6200 hardware and software.
The functionality described in this Manual is subject to change without notice.

ALCATEL

26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505
info@ind.alcatel.com
US Customer Support-(800) 995-2696
International Customer Support-(818) 878-4507
Internet-http://eservice.ind.alcatel.com

Warning

This equipment has been tested and found to comply with the limits for Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this guide, may cause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user’s authority to operate this equipment. It is suggested that the user use only shielded and grounded cables to ensure compliance with FCC Rules.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of the Canadian department of communications.

Le present appareil numerique níemet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la Class A prescrites dans le reglement sur le brouillage radioelectrique edicte par le ministere des communications du Canada.

Utilice sólo adaptadores con las siguientes características eléctricas y que estén debidamente certificados de acuerdo a la legislación vigente. El uso de otros adaptadores podría dañar el dispositivo y anular la garantía además de provocar riesgos al usuario.

	Características de entrada:	Características de salida:
OS-LS-6224P	AC100/115/220/230V; 50/60Hz; 2.0/1.7/0.9/0.9A; Clase I	DC 12V, 4.0A; -50V, 3.6A
OS-LS-6248P	AC100/115/220/230V; 50/60Hz; 4.0/3.4/1.8/1.8A; Clase I	DC 12V, 7.5A; -50V, 7.5A
OS-LS-6224	AC 100/115/220/230V; 50/60Hz; 0.4/0.4/0.2/0.2A; Clase I	DC 12V, 4.5A
OS-LS-6248	AC100/115/220/230V; 50/60Hz; 0.6/0.6/0.4/0.4A; Clase I	DC 12V, 4.5A
OS-LS-6224U	AC 100/115/220/230V 50/60Hz 1.0/1.0/0.5/0.5A Clase I	DC 12V , 4.5A

Adaptador:

	Modelo:	Marca comercial:
OS-LS-6224P	OS-LS-62BP-P	3Y Power
OS-LS-6248P	OS-LS-62BP-P	Alcatel
OS-LS-6248	OS-LS-62BP-DC & OS-LS-62BP	Accton & 3Y Power
OS-LS-6224	OS-LS-62BP-DC & OS-LS-62BP	Accton & 3Y Power

Contents

Figures

Chapter 1: Introduction

The OmniStack® 6200 series has seven platforms:

- **OS-LS-6212 –** Ethernet based switch with 12 RJ-45 10/100Base-TX ports, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking
- **OS-LS-6212P –** Ethernet based switch with 12 RJ-45 10/100Base-TX ports providing standard-based Power over Ethernet, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking
- **OS-LS-6224** – Ethernet based switch with 24 RJ-45 10/100Base-TX ports, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking (optional DC power source)
- **OS-LS-6224P** – Ethernet based switch with 24 RJ-45 10/100Base-TX ports providing standard-based Power over Ethernet, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking
- **OS-LS-6248** – Ethernet based switch with 48 RJ-45 10/100Base-TX ports, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking (optional DC power source)
- **OS-LS-6248P** – Ethernet based switch with 48 RJ-45 10/100Base-TX ports providing standard-based Power over Ethernet, two Gigabit combo uplink ports (with SFP or 10/100/1000Base-TX interfaces) and two ports full-duplex Gigabit stacking
- **OS-LS-6224U** – Ethernet based switch with 24 100Base-FX external SFP ports, two Gigabit combo ports with assicuated Mini-GBIC slots or RJ-45 ports and two 1000Base-T stacking ports

All devices have a management port which is used for debugging and management purposes.

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

Key Features

Table 1-1. Key Features

Feature	Description
Configuration Backup and Restore	Backup to TFTP server

Table 1-1. Key Features

Feature	Description
Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – HTTPS; Telnet – SSH SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Port – IEEE 802.1x
Access Control Lists	Supports up to 1K IP or MAC ACLs
DHCP Client	Supported
DNS Server	Supported
Port Configuration	Speed, duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports up to 8 trunks using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Static Address	Up to 16K MAC addresses in the forwarding table
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Protocol	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Trees (MSTP).
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, protocol-based, or private VLANs GVRP
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP) and TCP/UDP Port
STP Root Guard	Prevents devices outside the network core from being assigned the spanning tree root.
STP BPDU Guard	Used as a security mechanism to protect the network from invalid configurations.
802.1x - MAC Authentication	MAC authentication ensures that end-user stations meet security policies criteria, and protects networks from viruses.
DHCP Snooping	Expands network security by providing a firewall security between untrusted interfaces and DHCP servers.
DHCP Option 82	Enables to add information for the DHCP server on request.
IP Source Address Guard	Restricts IP traffic on non-routed, Layer 2 interfaces by filtering traffic. This feature is based on the DHCP snooping binding database and on manually configured IP source bindings.
ARP Inspection	Classic Address Resolution Protocol is a TCP/IP protocol that translates IP addresses into MAC addresses.

Table 1-1. Key Features

Feature	Description
LLDP-MED	Increases network flexibility by allowing different IP systems to co-exist on a single network.
QoS	Supports Quality of Service (QoS).
Multicast Filtering	Supports IGMP snooping and query.
Power over Ethernet	Enables PoE support.
Multicast TV VLAN	Supplies multicast transmissions to L2-isolated subscribers, without replicating the multicast transmissions for each subscriber VLAN.
IP Subnet-Based VLANs	Packets are classified according to the packet's source IP subnet in its IP header
MAC-Based VLANs	Packets are classified according to MAC address
Jumbo Frames	Support of mini jumbo frames allows forwarding of packets up to 1632 bytes.
QinQ	Allows network managers to add an additional tag to previously tagged packets

Description of Software Features

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Port-based and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications. Some of the management features are briefly described below.

Configuration Backup and Restore – You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

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

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP version 3, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access.

MAC Address Capacity Support – The device supports up to 16K MAC addresses. The device reserves specific MAC addresses for system use.

Self-Learning MAC Addresses – The device enables automatic MAC addresses learning from incoming packets.

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.

Static MAC Entries – User defined static MAC entries are stored in the *Bridging Table*, in addition to the Self Learned MAC addresses.

VLAN-Aware MAC-based Switching – Packets arriving from an unknown source address are sent to the CPU. When source addresses are added to the *Hardware Table*, packets addressed to this address are then forwarded straight to corresponding port.

MAC Multicast Support – Multicast service is a limited broadcast service, which allows one-to-many and many-to-many connections for information distribution. Layer 2 multicast service is where a single frame is addressed to a specific multicast address, and copies of the frame transmitted to relevant all relevant ports.

Address Resolution Protocol – IP routing generally utilizes routers and Layer 3 switches to inter-communicate using various routing protocols to discover network topology and define Routing tables. Device Next-Hop MAC addresses are automatically derived by ARP. This includes directly attached end systems. Users can override and supplement this by defining additional ARP Table entries.

QinQ tagging – QinQ tagging allows network managers to add an additional tag to previously tagged packets. Adding additional tags to the packets helps create more VLAN space. The added tag provides an VLAN ID to each customer, this ensures private and segregated network traffic.

Port Configuration – You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

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

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

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3ad Link Aggregation

Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 6 trunks.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static MAC address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

STP BPDU Guard – Bridge Protocol Data Units (BPDU) Guard expands network adminstrator’s ablility to enforce STP borders and maintain STP topologies realibility. BPDU is utilized when Fast Link ports is enabled and/or if the Spanning Tree Protocol is disabled on ports. If a BPDU message is sent to a port on which STP is disabled, BPDU Guard shuts down the port, and generates a SNMP message.

STP Root Guard – Spanning Tree Root Guard is used to prevent an unauthorized device from becoming the root of a spanning tree. Root guard functionality enables detection and resolution of misconfigurations, while preventing loops or loss of connectivity.

802.1x - MAC Authentication – MAC authentication like the 802.1X allows network access to a device, for example, printers and IP phones, that do not have the 802.1X supplicant capability. MAC authentication uses the MAC address of the connecting device to grant or deny network access.

To support MAC authentication, the RADIUS authentication server maintains a database of MAC addresses for devices that require access to the network. In order for the feature to be active, 802.1x must be in auto-mode.

User then can enable the MAC authentication feature in one of following modes:

- MAC Only – Where only MAC authentication is enabled
- MAC + 802.1x (In that case 802.1x takes precedence)

The feature can be enabled per port. The port must be a member of a guest VLAN prior of activating the feature.

DHCP Snooping – DHCP Snooping expands network security by providing a firewall security between untrusted interfaces and DHCP servers. By enabling DHCP Snooping network administrators can identify between trusted interfaces connected to end-users or DHCP Servers, and untrusted interface located beyond the network firewall. DHCP Snooping creates and maintains a DHCP Snooping Table which contains information received from untrusted packets. Interfaces are untrusted if the packet is received from an interface from outside the network or from a interface beyond the network firewall.

DHCP Option 82 – DHCP server can insert information into DHCP requests. The DHCP information is used to assign IP addresses to network interfaces.

IP Source Address Guard – IP source guard stops malignant network users from using unallocated network IP addresses. IP Source Guard ensures that only packets with an IP address stored in the DHCP Database are forwarded. IP address stored in the DHCP Snooping Database are either statically configured by the network administrator or are retrieved using DHCP. IP source guard can be enabled only on DHCP snooping untrusted interface.

Dynamic ARP Inspection – 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. Packets with invalid ARP Inspection Bindings are logged and dropped. Packets are classified as:

- Trusted — Indicates that the interface IP and MAC address are recognized, and recorded in the ARP Inspec-tion List. Trusted packets are forward without ARP Inspection.
- Untrusted — Indicates that the packet arrived from an interface that does not have a recognized IP and MAC addresses. The packet is checked for:
  - Source MAC — Compares the packet’s source MAC address 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 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. 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. If the IP address is found the packet is valid, and is forwarded. ARP inspection is performed only on untrusted interfaces.

LLDP - The Link Layer Discovery Protocol (LLDP) allows 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 system, and to store discovered information. Device 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 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-MED – LLDP Media Endpoint Discovery (LLDP-MED) increases network flexibility by allowing different IP systems to co-exist on a single network. Provides detailed network topology information, including what device are located on the network, and where the devices are located. For example, which IP phone is connect to what port, which software is running on what switch, and which port is connected to what PC.

Spanning Tree Protocol – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol adds a level of fault tolerance by allowing two or more redundant connections to be created between a pair of LAN segments. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

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

Virtual LANs – The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same broadcast domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

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

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

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration.

Virtual Cable Testing (VCT) – VCT detects and reports copper link cabling occurrences, such as open cables and cable shorts.

MDI/MDIX Support – The device supports auto-detection between crossed and straight-through cables. Standard wiring for end stations is Media-Dependent Interface (MDI) and the *s*tandard wiring for hubs and switches is known as Media-Dependent Interface with Crossove**r** (MDIX).

Quality of Service (QoS) Support – Network traffic is usually unpredictable, and the only basic assurance that can be offered is Best Effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance. The device supports the following QoS modes:

- Basic
- Advanced

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.

Quality of Service Basic Mode – In the Basic QoS mode, it is possible to activate a trust mode (to trust VPT, DSCP, TCP/UDP or none). In addition, a single Access Control List can be attached to an interface.

Web Based Management – With web based management, the system can be managed from any web browser. The system contains an Embedded Web Server (EWS), which 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.

Remote Monitoring – Remote Monitoring (RMON) is an extension to SNMP, which provides comprehensive network traffic monitoring capabilities (as opposed to SNMP which allows network device management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.

VLAN Groups – Provides VLAN classification by MAC address, subnet, and protocol groups.

Multicast TV – Supplies multicast transmissions to L2-isolated subscribers, without replicating the multicast transmissions for each subscriber VLAN

Port Based Authentication – 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).

System Defaults

The device is configured with default settings. To reset the device to the default settings, delete the startup configuration. The following table lists some of the basic system defaults.

Table 1-2. System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	0
	Local Console Timeout	10
Authentication	Privileged Exec Level	no password
	Normal Exec Level	no password
	Enable Privileged Exec from Normal Exec Level	no password
	RADIUS Authentication	disabled
	TACACS Authentication	disabled
	802.1x Port Authentication	disabled
	HTTPS	disabled
	SSH	disabled
	Port Security	disabled

Table 1-2. System Defaults

Function	Parameter	Default
SNMP	Community Strings	no SNMP communities
	Traps	disabled
	SNMP V3 View:	local engine ID of device is comprised of IANA Private Enterprise number & MAC address of device
Port Configuration	Admin Status	enabled
	Auto-negotiation	on
	Flow Control	off
	Port Capability	list of all capabilities on port
AMAP	Status	enabled
	Common Phase Timeout Interval	300 sec.
	Discovery Phase Timeout Interval	30 sec.
Rate Limiting	Input and output limits	disabled
Port Trunking	Static Trunks	up to 8 port in 8 trunks can be defined
	LACP system priority	1
	LACP Port-priority	1
	LACP	long
Broadcast Storm Protection	Status	disabled
	Broadcast Limit Rate	100 kbps
Spanning Tree Protocol	Status	enabled
	Spanning Tree Mode	STP
	Fast Forwarding (Edge Port)	enabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	all
	Ingress Filtering	on
	Switchport Mode (Egress Mode)	hybrid (tagged/untagged)
	GVRP (global)	disabled
	GVRP (port interface)	disabled

Table 1-2. System Defaults

Function	Parameter	Default
Quality of Service	QoS Mode	disabled
	CoS Mapping	Cos 0 - queue 1; CoS 1 - queue 1; Cos 2 - queue 1 Cos 3 - queue 1; CoS 4 - queue 2; Cos 5 - queue 2 Cos 6 - queue 3; CoS 7 - queue 3;
	Scheduling	all queues are expedite queues
IP Settings	IP Address	none
	Subnet Mask	none
	Default Gateway	none
	DHCP	disabled
	BOOTP	enabled if configuration is empty and there is no command line activity within 60 seconds
DNS Server	Domain Lookup	enabled
Multicast Filtering	IGMP Snooping	disabled
System Log	Status	on
	Messages Logged	200
	Messages Logged to Flash	200
SNTP	Clockset	0:00 Jan 1, 2000
	Clock source	internal
	Daylight Savings	disabled
	SNTP	no servers defined
Port Security	Port Lock	disabled
	DHCP Snooping	disabled
	DHCP Option 82	disabled
	STP BPDU Guard	disabled
	ARP Inspection	disabled
	IP Source Address Guard	disabled
	Root Guard	disabled
Multicast Forwarding	IGMP Snooping (Global)	disabled
	IGMP Snooping (Interface)	disabled
	Multicast TV VLAN	disabled
SSH	Server	enabled

Table 1-2. System Defaults		
Function	Parameter	Default
SSL	Server	enabled
RADIUS	RADIUS server	none defined
TACACS+	TACACS+ server	none defined

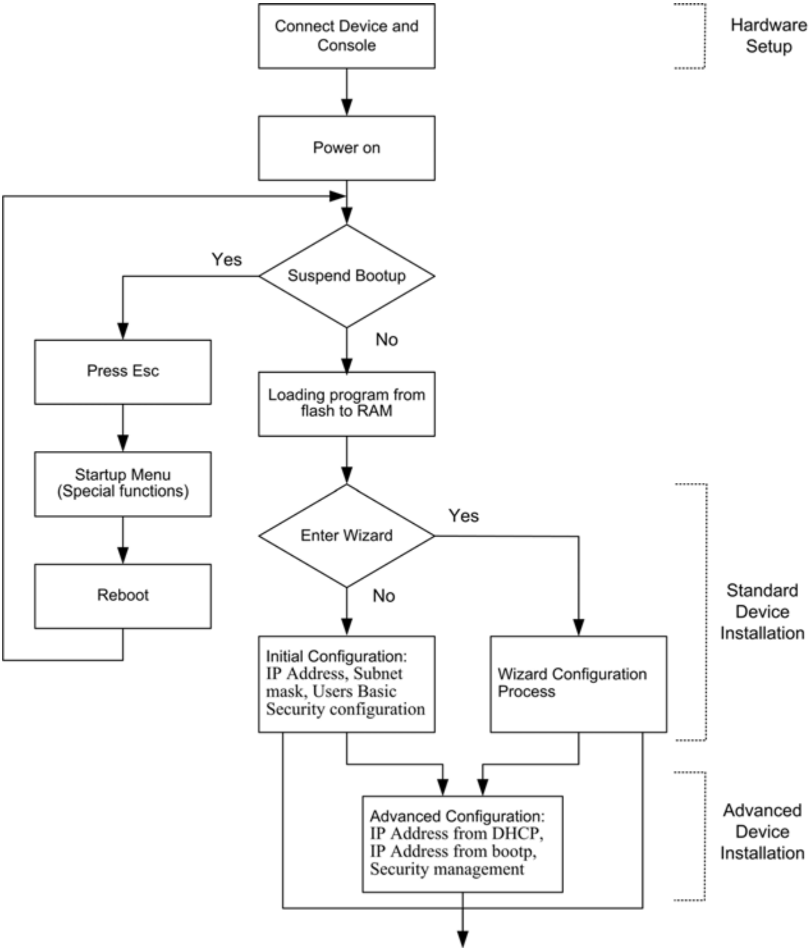
Chapter 2: Initial Configuration

This section describes the initial device configuration and includes the following topics:

- General Configuration Information
- Booting the Switch
- Configuration Overview
- Advanced Configuration
- Software Download and Reboot
- Startup Menu Functions

After completing all external connections, connect a terminal to the device to monitor the boot and other procedures. The order of installation and configuration procedures is illustrated in the following figure. For the initial configuration, the standard device configuration is performed. Other functions can be performed, but doing so suspends the installation process and causes a system reboot.

Performing other functions is described later in this section.



Connect Device and Console
Power on
Suspend Bootup
Yes
No
Press Esc
Startup Menu (Special functions)
Reboot
Loading program from flash to RAM
Enter Wizard
Yes
No
Initial Configuration: IP Address, Subnet mask, Users Basic Security configuration
Wizard Configuration Process
Advanced Configuration: IP Address from DHCP, IP Address from bootp, Security management
Hardware Setup
Standard Device Installation
Advanced Device Installation

Figure 2-1. Installation and Configuration

General Configuration Information

Your device has predefined features and setup configuration.

Auto-Negotiation

Auto-negotiation allows a device to advertise modes of operation and share information with another device that shares a point-to-point link segment. This automatically configures both devices to take maximum advantage of their abilities.

Auto-negotiation is performed completely within the physical layers during link initiation, without any additional overhead to either the MAC or higher protocol layers. Auto-negotiation allows the ports to do the following:

- Advertise their abilities
- Acknowledge receipt and understanding of the common modes of operation that both devices share
- Reject the use of operational modes that are not shared by both devices
- Configure each port for the highest-level operational mode that both ports can support

If connecting a port of the switch to the network interface card (NIC) of a terminal that does not support auto-negotiation or is not set to auto-negotiation, both the device port and the NIC must be manually set with the Web browser interface or CLI commands to the same speed and duplex mode.

Note: If the station on the other side of the link attempts to auto-negotiate with a port that is manually configured to full duplex, the auto-negotiation results in the station attempting to operate in half duplex. The resulting mismatch may lead to significant frame loss. This is inherent in the auto-negotiation standard.

Device Port Default Settings

The following table describes the device port default settings.

Function	Default Settings
Port speed and mode	100 M or 1000M Auto-negotiation
Port forwarding state	Enabled
Head of line blocking prevention	On (Enabled)
Flow Control	Off
Back Pressure	Off

Note: These default settings can be modified once the device is installed.

The following is an example for changing the port speed on port g1 using CLI commands:

```
Console (config)# interface ethernet g1                    4-376
Console (config-if)# speed 100                             4-380
```

The following is an example for enabling flow control on port e1 using CLI commands:

```
Console (config)# interface ethernet e1                        4-376
Console (config-if)# flowcontrol on                            4-383
```

The following is an example for enabling back pressure on port e1 using CLI commands.

```
Console (config)# interface ethernet e1                        4-376
Console (config-if)# speed 10                                  4-380
Console (config-if)# back-pressure                             4-384
```

Booting the Switch

To boot the switch, perform the following:

1. Ensure that the device console is connected to a VT100 terminal device or VT100 terminal emulator.
2. Deactivate the AC power receptacle.
3. Connect the device to the AC receptacle.
4. Activate the AC power receptacle.

When the power is turned on with the local terminal already connected, the switch goes through Power On Self Test (POST). POST runs every time the device is initialized and checks hardware components to determine if the device is fully operational before completely booting. If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure.

As the switch boots, the bootup test first counts the device memory availability and then continues to boot. The following screen is an example of the displayed POST.

```
------ Performing the Power-On Self Test (POST) ------

Boot1 Checksum Test...............................PASS

Boot2 Checksum Test...............................PASS

Flash Image Validation Test.......................PASS

BOOT Software Version x.x.x.xx Built 07-Jan-200x 10:53:05
Processor: xxxxxx xxxxx xxxx, xx MByte SDRAM.
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

The boot process runs approximately 30 seconds.

The auto-boot message that appears at the end of POST (see the last lines) indicates that no problems were encountered during boot.

During boot, the Startup menu can be accessed if necessary to run special procedures. To enter the Startup menu, press <Esc> or <Enter> within the first two seconds after the auto-boot message is displayed. For information on the Startup menu, see "Startup Menu Functions."

If the system boot is not interrupted by pressing <Esc> or <Enter>, the system continues operation by decompressing and loading the code into RAM. The code starts running from RAM and the list of numbered system ports and their states (up or down) are displayed.

Note: The following screen is an example configuration. Items such as addresses, versions, and dates may differ for each device.

```
Preparing to decompress...

Decompressing SW from image-1
638000
OK
Running from RAM...

**********************************************************************
*** Running SW Ver. x.x.x.x Date 11-Jan-200x Time 15:43:13 ***
**********************************************************************

HW version is
Base Mac address is: 00:00:b0:24:11:80
Dram size is: xxM bytes
Dram first block size is: 47104K bytes
Dram first PTR is: 0x1200000
Flash size is: xM
Devices on SMI BUS:
-------------------
smi dev id = 16, dev type=0xd0411ab, dev revision=0x1

Device configuration:
Prestera based - Back-to-back system
Slot 1 - DB-DX240-24G HW Rev. xx.xx
Tapi Version: xx.x.x-x
Core Version: xx.x.x-x
01-Jan-200x 01:01:22 %INIT-I-InitCompleted: Initialization task is
completed

Console> 01-Jan-200x 01:01:23 %LINK-I-Up:  e1
01-Jan-200x 01:01:23 %LINK-W-Down:  e2
01-Jan-200x 01:01:23 %LINK-I-Up:  Vlan 1
01-Jan-200x 01:01:23 %LINK-W-Down:  e4
.
.
.
01-Jan-200x 01:01:23 %LINK-W-Down:  e46
01-Jan-200x 01:01:23 %LINK-W-Down:  e47
01-Jan-200x 01:01:23 %LINK-W-Down:  e48
```

After the switch boots successfully, a system prompt appears (console>) and the local terminal can be used to begin configuring the switch. However, before configuring the switch, ensure that the software version installed on the device is the latest version. If it is not the latest version, download and install the latest version. See "Software Download and Reboot."

Configuration Overview

Before assigning a static IP address to the device, obtain the following information from the network administrator:

- A specific IP address allocated by the network administrator for the switch to be configured
- Network mask for the network

There are two types of configuration: Initial configuration consists of configuration functions with basic security considerations, whereas advanced configuration includes dynamic IP configuration and more advanced security considerations.

After making any configuration changes, the new configuration must be saved before rebooting. To save the configuration, enter the following CLI command:

```
Console# copy running-config startup-config                4-365
```

Initial Configuration

Initial configuration, which starts after the device has booted successfully, includes static IP address and subnet mask configuration, and setting user name and privilege level to allow remote management. If the device is to be managed from an SNMP-based management station, SNMP community strings must also be configured. The following configurations are completed:

- Static IP Address and Subnet Mask
- Static Route Configuration
- User Name
- SNMP Community strings

Static IP Address and Subnet Mask

IP interfaces can be configured on each interface of the device. After entering the configuration command, it is recommended to check if a interface was configured with the IP address by entering the `show ip interface` command.

The commands to configure the device are interface specific.

To manage the switch from a remote network, a static route must be configured, which is an IP address to where packets are sent when no entries are found in the device tables. The configured IP address must belong to the same subnet as one of the device IP interfaces.

To configure a static route, enter the command at the system prompt as shown in the following configuration example where 101.1.1.2 is the specific management station:

```
Console# configure
Console(config)# interface vlan 1                                       4-664
Console(config-if)# ip address 100.1.1.1 255.255.255.0                  4-418
Console(config-if)# exit                                                4-656
Console(config)# ip default-gateway 100.1.1.10                          4-420
```

.

```
Gateway IP Address
Gateway IP       Type                     Activity Status
Address
10.7.1.1         Static                   Active
IP Address       Interface                Type
-----------      -----------              -------------
10.7.1.192/24    VLAN1                    static
10.7.2.192/24    VLAN2                    DHCP
```

User Name

A user name is used to manage the device remotely, for example through SSH, Telnet, or the Web interface. To gain complete administrative (super-user) control over the device, the highest privilege level 15 must be specified.

Note: Only the administrator (super-user) with the highest privilege level (15) is allowed to manage the device through the Web browser interface.

For more information about the privilege level, see the *Command Line Interface*.

The configured user name is entered as a login name for remote management sessions. To configure user name and privilege level, enter the command at the system prompt as shown in the configuration example:

```
Console> enable
Console# configure
Console(config)# username admin password lee privilege 15
```

SNMP Community Strings

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Devices supporting SNMP run a local software (agent). The SNMP agents maintain a list of variables, used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. 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 and SNMP community strings.

The device is SNMP-compliant and contains an SNMP agent that supports a set of standard and private MIB variables. Developers of management stations require the exact structure of the MIB tree and receive the complete private MIBs information before being able to manage the MIBs.

All parameters are manageable from any SNMP management platform, except the SNMP management station IP address and community (community name and access rights). The SNMP management access to the switch is disabled if no community strings exist.

Note: The device switch is delivered with no community strings configured.

The following screen displays the default device configuration:

```
Console# show snmp                                                  4-531

Community-String      Community-Access      IP address
----------------      ----------------      ----------

System Contact:
System Location:
```

The community-string, community-access, and IP address can be configured through the local terminal during the initial configuration procedure.

The SNMP configuration options for the Community String are as follows:

- Access rights options: ro (read only), rw (read-and-write) or su (super).
- An option to configure IP address or not: If an IP address is not configured, it means that all community members having the same community name are granted the same access rights.

Common practice is to use two community strings for the switch one (public community) with read-only access and the other (private community) with read-write access. The public string allows authorized management stations to retrieve MIB objects, while the private string allows authorized management stations to retrieve and modify MIB objects.

During initial configuration, it is recommended to configure the device according to the network administrator requirements, in accordance with using an SNMP-based management station.

To configure SNMP station IP address and community string(s) perform the following:

1. At the console prompt, enter the command **Enable**. The prompt is displayed as #.
2. Enter the command **configure** and press **<Enter>**.
3. In the configuration mode, enter the SNMP configuration command with the parameters including community name (private), community access right (read and write) and IP address, as shown in the following example:

```
Console# configure
Config(config)# snmp-server community private rw 11.1.1.2 type
router                                                          4-519
Config(config)# exit                                            4-656
Console(config)# show snmp                                      4-531

Community-String     Community-Access     IP address
----------------     ----------------     ----------

private readWrite 11.1.1.2
Traps are enabled.
Authentication-failure trap is enabled.

Trap-Rec-Address     Trap-Rec-Community     Version
----------------     ------------------     -------

System Contact:
System Location:
```

This completes the initial configuration of the device from a local terminal. The configured parameters enable further device configuration from any remote location.

Advanced Configuration

This section provides information about dynamic allocation of IP addresses and security management based on the authentication, authorization, and accounting (AAA) mechanism, and includes the following topics:

- Configuring IP Addresses through DHCP
- Configuring IP Addresses through BOOTP
- Security Management and Password Configuration

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

Retrieving an IP Address From a DHCP Server

When using the DHCP protocol to retrieve an IP address, the device acts as a DHCP client. 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, in order to retrieve the IP address.

2. Enter the following commands to use the selected port for receiving the IP address. In the following example, the commands are based on the port type used for configuration.

- Assigning Dynamic IP Addresses:

```
console# configure
console(config)# interface ethernet e1                       4-376
console(config-if)# ip address dhcp hostname sales           4-419
console(config-if)# exit                                     4-656
console(config)#
```

The interface receives the IP address automatically.

3. To verify the IP address, enter the show ip interface command at the system prompt as shown in the following example.

```
Console# show ip interface


Gateway IP        Type         Activity status
Address

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

10.7.1.1          Static       Active




IP address        Interface    Type               Directed Broadcast

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

10.7.1.192/24     VLAN 1       Static
```

Notes: **1.** The device configuration does not have to be deleted to retrieve an IP address for the DHCP server.

2. 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 switch 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 again.

Receiving an IP Address From a BOOTP Server

The standard BOOTP protocol is supported and enables the switch to automatically download its IP host configuration from any standard BOOTP server in the network. In this case, the device acts as a BOOTP client.

To retrieve an IP address from a BOOTP server:

1. Select and connect any port to a BOOTP server or subnet containing such a server, to retrieve the IP address.

2. At the system prompt, enter the delete startup configuration command to delete the startup configuration from flash. The device reboots with no configuration

and in 60 seconds starts sending BOOTP requests. The device receives the IP address automatically.

Note: When the device reboot begins, any input at the ASCII terminal or keyboard automatically cancels the BOOTP process before completion and the device does not receive an IP address from the BOOTP server.

The following example illustrates the process:

```
Console> enable                                                   4-368
Console# delete startup-config                                    4-368
Startup file was deleted
Console# reload                                                   4-612
You haven’t saved your changes. Are you sure you want to continue (y/
n)[n]?
This command will reset the whole system and disconnect your current
session.Do you want to continue (y/n)[n]?
*****************************************************
/*the device reboots */
```

To verify the IP address, enter the show ip interface command. The device is now configured with an IP address.

Security Management and Password Configuration

System security is handled through the AAA (Authentication, Authorization, and Accounting) 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.

The system is delivered with no default password configured; all passwords are user-defined. If a user-defined password is lost, a password recovery procedure can be invoked from the Startup menu. The procedure is applicable for the local terminal only and allows a one-time access to the device from the local terminal with no password entered.

Configuring Security Passwords Introduction

The security passwords can be configured for the following services:

- Console
- Telnet
- SSH
- HTTP
- HTTPS

Passwords are user-defined.

When creating a user name, the default priority is "1," which allows 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.

Configuring an Initial Console Password

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

```
Console(config)# aaa authentication login default line     4-288
Console(config)# aaa authentication enable default line    4-290
Console(config)# line console                              4-437
Console(config-line)# login authentication default         4-291
Console(config-line)# enable authentication default        4-292
Console(config-line)# password george                      4-296
```

When initially logging on to a device through a console session, enter `george` at the password prompt.

When changing a device’s mode to enable, enter `george` at the password prompt.

Configuring an Initial Telnet Password

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

```
Console(config)# aaa authentication login default line     4-288
Console(config)# aaa authentication enable default line    4-290
Console(config)# line telnet                               4-437
Console(config-line)# login authentication default         4-291
Console(config-line)# enable authentication default        4-292
Console(config-line)# password bob                         4-296
```

When initially logging onto a device through a Telnet session, enter `bob` at the password prompt.

When changing a device mode to enable, enter `bob`.

Configuring an Initial SSH password

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

```
Console(config)# aaa authentication login default line     4-288
Console(config)# aaa authentication enable default line    4-290
Console(config)# line ssh                                  4-437
Console(config-line)# login authentication default         4-291
Console(config-line)# enable authentication default        4-292
Console(config-line)# password jones                       4-296
```

When initially logging onto a device through a SSH session, enter `jones` at the password prompt.

When changing a device mode to enable, enter `jones`.

Configuring an Initial HTTP Password

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

```
Console(config)# ip http authentication local                   4-293
Console(config)# username admin password user1 level 15         4-297
```

Configuring an initial HTTPS Password

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

```
Console(config)# ip https authentication local                  4-294
Console(config)# username admin password user1 level 15         4-297
```

Enter the following commands once when configuring to use a console, a Telnet, or an SSH session in order to use an HTTPS session.

In the Web browser enable SSL 2.0 or greater for the content of the page to appear.

```
Console(config)# crypto certificate generate key_generate       4-695
Console(config)# ip https server                                4-693
```

When initially enabling an http or https session, enter `admin` for user name and `user1` for password.

Note: HTTP and HTTPS services require level 15 access and connect directly to the configuration level access.

Software Download and Reboot

Software Download through XModem

This section contains instructions for downloading device software (system and boot images) using XModem, which is a data transfer protocol for updating back-up configuration files.

To download a boot file using XModem:

1. Enter the command “xmodem:boot”. The switch is ready to receive the file via the XModem protocol and displays text similar to the following:

   ```
   Console# copy xmodem:boot                                    4-365
   Please download program using XMODEM.
   console#
   ```

2. Specify the path of the source file within 20 seconds. If the path is not specified within 20 seconds, the command times out.

To download a software image file using XModem:

1. Enter the command “xmodem:image”. The switch is ready to receive the file via

the XModem protocol.

2. Specify the path of the source file to begin the transfer process. The following is an example of the information that appears:

```
Console# copy xmodem:image                                          4-365
Please download program using XMODEM
console#
```

Software Download Through TFTP Server

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.

The switch boots and runs when decompressing the system image from the flash memory area where a copy of the system image is stored. When a new image is downloaded, it is saved in the other area allocated for the additional system image copy.

On the next boot, the switch decompresses and runs the currently active system image unless chosen otherwise.

To download an image through the TFTP server:

1. Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.

2. Ensure that the file to be downloaded is saved on the TFTP server (the Image file).

3. Enter the command “show version” to verify which software version is currently running on the device. The following is an example of the information that appears:

```
Console# show version                                               4-619
SW version x.xx.xx (date xx-xxx-2004 time 13:42:41)Boot version
x.xx.x (date x-xxx-2003 time 15:12:20) HW version
```

4. Enter the command “show bootvar” to verify which system image is currently active. The following is an example of the information that appears:

```
Console# show bootvar                                               4-374
Images currently available on the Flash Image-1 active (selected
for next boot)Image-2 not active
Console#
```

5. Enter the command “copy tftp://{tftp address}/{file name} image” to copy a new system image to the device. When the new image is downloaded, it is saved in

the area allocated for the other copy of system image (image-2, as given in the example). The following is an example of the information that appears:

```
Console# copy tftp://176.215.31.3/file1 image Accessing file
file1 on 176.215.31.3...                                       4-365
Loading file1 from
176.215.31.3:!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Exclamation symbols indicate that a copying process is in progress. A period indicates that the copying process is timed out. Many periods in a row indicate that the copying process failed.

6. Select the image for the next boot by entering the `boot system` command. After this command, enter the command `show bootvar` 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 appears:

```
Console# boot system image-2                                   4-372
Console# show bootvar                                          4-374
Images currently available on the Flash
Image-1 active Image-2 not active (selected for next boot)
```

If the image for the next boot is not selected by entering the boot system command, the system boots from the currently active image (image-1,as given in the example).

7. Enter the command “reload”. The following message is displayed:

```
Console# reload                                                4-612
This command will reset the whole system and disconnect your
current session.Do you want to continue (y/n)[n]?
```

8. Enter “Y” to reboot the switch.

Note: For information on downloading software to stacking units, see *"Configuring Stacking".*

Boot Image Download

Loading a new boot image from the TFTP server and programming it into the flash updates the boot image. The boot image is loaded when the switch is powered on.

To download a boot file through the TFTP server:

1. Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.
2. Ensure that the file to be downloaded (the .rfb file) is saved on the TFTP server.

3. Enter the command “show version” to verify which boot version is currently running on the device. The following is an example of the information that appears:

```
Console# show version                                                4-619
SW version x.xx.xx (date xx-xxx-2004 time 13:42:41)Boot version
x.xx.xx (date xx-xx-2004 time 15:12:20)HW version xx.xx.xx (date
xx-xxx-2004 time 12:12:20)
```

4. Enter the command “copy tftp://{tftp address}/{file name} boot” to copy the boot image to the switch. The following is an example of the information that appears:

```
Console# copy tftp://176.215.31.3/6024_boot-10013.rfb                4-365
boot
Erasing file
...done.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!Copy:393232 bytes copied in 00:00:05 [hh:mm:ss]
```

5. Enter the command “reload”. The following message is displayed:

```
Console# reload                                                      4-612
This command will reset the whole system and disconnect your
current session. Do you want to continue (y/n)[n]?
```

6. Enter “Y” to reboot the switch.

Startup Menu Functions

Additional configuration functions can be performed from the Startup menu.

To display the Startup menu:

1. During the boot process, after the first part of the POST is completed press **<Esc>** or **<Enter>** within two seconds after the following message is displayed:

```
Autoboot in 2 seconds -press RETURN or Esc.to abort and enter prom.
```

The Startup menu is displayed and contains the following configuration functions:

```
[1]Download Software
[2]Erase Flash File
[3]Erase Flash Sectors
[4]Password Recovery Procedure
[5]Enter Diagnostic Mode
[6]Back Enter your choice or press 'ESC' to exit:
```

The following sections describe the Startup menu options. If no selection is made within 25 seconds (default), the switch times out and the device continues to load normally.

Only technical support personnel can operate the Diagnostics Mode. For this reason, the **Enter Diagnostic Mode** option of the Startup menu is not described in this guide.

Download Software

Use the software download option when a new software version must be downloaded to replace corrupted files, update, or upgrade the system software.

To download software from the Startup menu:

1. On the Startup menu, press “1”.

   The following prompt is displayed:

   ```
   Downloading code using XMODEM
   ```

2. When using HyperTerminal, click **Transfer** on the HyperTerminal menu bar.
3. From the Transfer menu, click **Send File**. The **Send File** window is displayed.

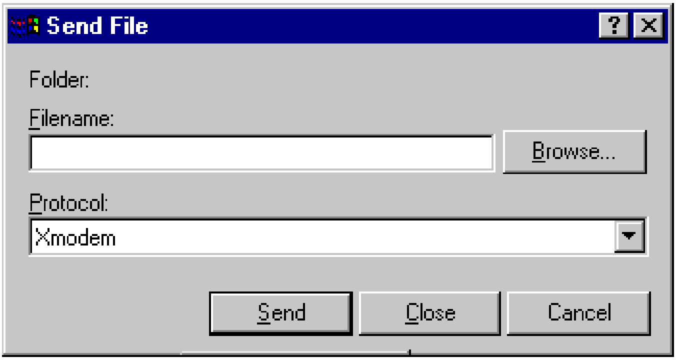

Send File
Folder:
Filename:
Protocol:
Xmodem

Figure 2-2. Send File window

4. Enter the file path for the file to be downloaded.
5. Ensure the protocol is defined as Xmodem.
6. Click **Send**.

   The software is downloaded. Software downloading takes several minutes. The terminal emulation application, such as HyperTerminal, may display the progress of the loading process.

After software downloads, the device reboots automatically.

Erase FLASH File

In some cases, the device configuration must be erased. If the configuration is erased, all parameters configured via CLI, Web browser interface, or SNMP must be reconfigured.

To erase the device configuration:

1. From the Startup menu, press “2” within 6 seconds to erase flash file. The following message is displayed:

```
Warning! About to erase a Flash file.
Are you sure (Y/N)?y
```

2. Press “Y”.

   Note: Do not press **<Enter>**.

   The following message is displayed.

```
Write Flash file name (Up to 8 characters, Enter for none.):config
File config (if present) will be erased after system initialization
========Press Enter To Continue ========
```

3. Enter **config** as the name of the flash file. The configuration is erased and the device reboots.
4. Perform the switch’s initial configuration.

Erase FLASH Sectors

For troubleshooting purposes, the flash sectors may need to be erased. If the flash is erased, all software files must be downloaded and installed again.

To erase the FLASH:

1. From the Startup menu, press “3” within 6 seconds. The following message is displayed:

```
Warning! About to erase Flash Memory! FLASH size =16252928.blocks =64
Are you sure (Y/N)
```

2. Confirm by pressing **<Y>**. The following message is displayed:

```
Enter First flash block (1 -63):
```

3. Enter the first flash block to be erased and press **<Enter>**. The following message is displayed:

```
Enter Last flash block (1 -63):
```

4. Enter the last flash block to be erased and press **<Enter>**. The following message is displayed:

```
Are you sure (Y/N)
```

5. Confirm by pressing **<Y>**. The following message is displayed:

```
Erasing flash blocks 1 -63: Done.
```

Password Recovery

If a password is lost, use the Password Recovery option on the Startup menu. The procedure enables the user to enter the device once without a password.

To recover a lost password for the local terminal only:

1. From the Startup menu, select “4” and press **<Enter>**. The password is deleted.

2. To ensure device security, reconfigure passwords for applicable management methods.

Chapter 3: Configuring the Switch

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 6.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 4: “Command Line Interface.”

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

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol.
2. Set user names and passwords using an out-of-band serial connection. Access to the Web agent is controlled by the same user names and passwords as the onboard configuration program.
3. After you enter a user name and password, you will have access to the system configuration program.

Notes: **1.** If you log into the CLI interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as “admin” (Privileged Exec level), you can change the settings on any page.

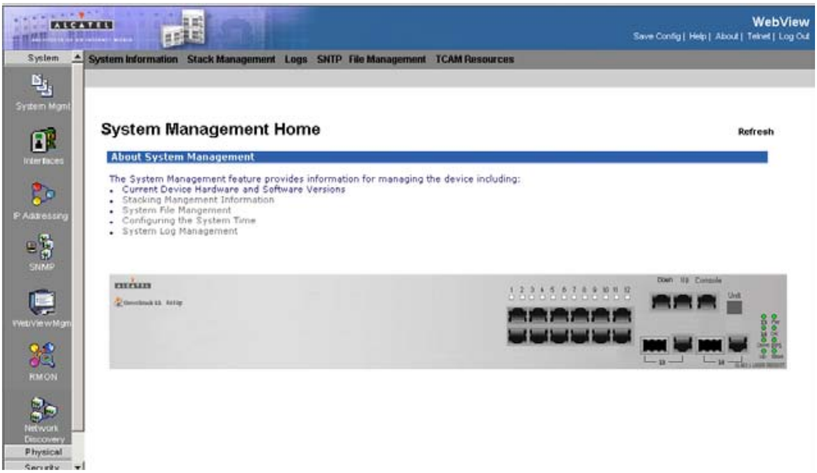
2. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch’s response time to management commands issued through the web interface.

Navigating the Web Browser Interface

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

Home Page

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



System Management Home

The System Management feature provides information for managing the device including:

- Current Device Hardware and Software Versions
- Stacking Mangement Information
- System File Mangement
- Configuring the System Time
- System Log Management

Figure 3-3. Home Page

Configuration Options

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

Table 3-1.

Add	Adds new device configuration information.
Modify	Modifies existing device configuration information.
Apply	Saves new or modified configuration information to the device.
Delete Checkbox	Deletes current device configuration information.
Test Now	Performs either copper or fiber cable tests.
Clear Counters	Clears device statistics.

Notes:

1. To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings,” the setting for item “Check for newer versions of stored pages” should be “Every visit to the page.”
2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser’s refresh button.

Panel Display

The web agent displays an image of the switch’s ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex, or Flow Control (i.e., with or without flow control). Clicking on the image of a port opens the Interface Configuration Page as described on page 3-71.

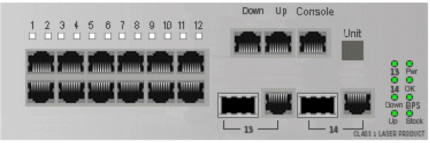


Figure 3-4. Ports Panel

Main Menu

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

Table 3-2. EWS Menu Options

System		
System Management	Provides system information including the general device information, stacking information, system logs, system time parameters, and parameters for managing system files.	
Interfaces	Provides information for configuring the device interfaces.	
IP Addressing	Provides information for configuring IP addressing. In addition, this section contains information for defining ARP, DHCP, and DNS settings.	
SNMP	Provides information for configuring SNMP.	
Web View Management	Provides information for configuring system passwords, and web access.	
RMON	Provides information for viewing RMON statistics.	
Network Discovery	Provides Information for configuring the LLDP and the AMAP protocols.	
Physical	Provides information for managing Power-over-Ethernet devices and system diagnostics.	
Ethernet	Provides information for managing PoE devices and viewing PoE statistics.	
Diagnostics	Provides information for performing copper and fiber cable tests, performing port mirroring, and viewing device health information.	
Security		

Table 3-2. EWS Menu Options

Traffic Control	Provides information for configuring Broadcast Storm Control and port security.	
802.1X	Provides information for configuring 802.1X port authentication.	
Access Control	Provides information for configuring Access Control Lists and Access Control Entries, as well as, information for binding ACLs to interfaces.	
DHCP Snooping	Builds and maintains a binding table used by DHCP Snooping, the ARP Inspection and IP Source Guard features.	
Layer 2		
Address Tables	Provides information for defining static and dynamic addresses.	
Spanning Tree	Provides information for configuring the Spanning Tree Protocol, the Rapid Spanning Tree, and Multiple Spanning Tree.	
VLAN	Provides information for defining VLANs, including VLAN groups, GARP, and GVRP.	
Multicast	Provides information for configuring Multicast Groups, Multicast Forwarding, and IGMP snooping.	
Policy		
General QoS	Provides information for configuring the QoS general mode	
Basic Mode	Provides information for configuring the QoS basic mode.	
Advanced Mode	Provides information for configuring the QoS advanced mode.	

Managing Device Information

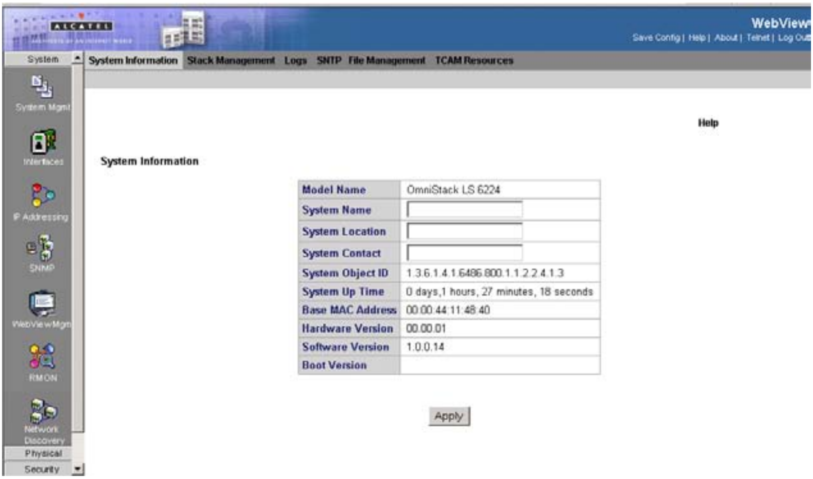
In the *System Information Page*, you can easily identify the system by displaying the device name, location and contact information.

Command Attributes

- **Model Name** — Displays the device model number and name.
- **System Name** — Defines the user-defined device name. The field range is 0-160 characters.
- **System Location** — Defines the location where the system is currently running. The field range is 0-160 characters.
- **System Contact** — Defines the name of the contact person. The field range is 0-160 characters.
- **System Object ID** — Displays the vendor's authoritative identification of the network management subsystem contained in the entity.
- **System Up Time** — Displays the amount of time since the most recent device reset. The system time is displayed in the following format: Days, Hours, Minutes, and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.
- **Base MAC Address** — Displays the device MAC address.
- **Hardware Version** — Displays the installed device hardware version number.

- **Software Version** — Displays the installed software version number.
- **Boot Version** — Displays the current boot version running on the device.

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



System Information

Model Name	OmniStack LS 6224
System Name	
System Location	
System Contact	
System Object ID	1.3.6.1.4.1.6486.800.1.1.2.2.4.1.3
System Up Time	0 days,1 hours, 27 minutes, 18 seconds
Base MAC Address	00:00:44:11:48:40
Hardware Version	00.00.01
Software Version	1.0.0.14
Boot Version	

Figure 3-5. System Information Page

CLI – The following is an example of the CLI System Information commands:

```
console# show system
4-618
```

Managing Stacking

Stacking provides multiple switch management through a single point as if all stack members are a single unit. All stack members are accessed through a single IP address through which the stack is managed. The stack is managed from the following:

- Web-based interface
- SNMP Management Station
- Command Line Interface (CLI)

Devices support stacking up to six units per stack, or can operate as stand-alone units.

During the Stacking setup, one switch is selected as the Stacking Master and another stacking member can be selected as the Secondary Master. All other devices are selected as stack members, and assigned a unique Unit ID.

Switch software is downloaded separately for each stack members. However, all units in the stack must be running the same software version.

Switch stacking and configuration is maintained by the Stacking Master. The Stacking Master detects and configures the ports with minimal operational impact in the event of:

- Unit Failure
- Inter-unit Stacking Link Failure
- Unit Insertion
- Removal of a Stacking Unit

This section provides an introduction to the user interface, and includes the following topics:

- Understanding the Stack Topology
- Stacking Failover Topology
- Stacking Members and Unit ID
- Removing and Replacing Stacking Members
- Exchanging Stacking Members
- Switching between the Stacking Master and the Secondary Master

Understanding the Stack Topology

The devices operate in a Ring topology. A stacked Ring topology is where all devices in the stack are connected to each other forming a circle. Each device in the stack accepts data and sends it to the device to which it is attached. The packet continues through the stack until it reaches its destination. The system discovers the optimal path on which to send traffic.

Most difficulties incurred in Ring topologies occur when a device in the ring becomes non-functional, or a link is severed. In a stack, the system automatically switches to a Stacking Failover topology without any system downtime. An SNMP message is automatically generated, but no stack management action is required. However, the stacking link or stacking member must be repaired to ensure the stacking integrity. After the stacking issues are resolved, the device can be reconnected to the stack without interruption, and the Ring topology is restored.

Stacking Failover Topology

If a failure occurs in the stacking topology, the stack reverts to Stacking Failover Topology. In the Stacking Failover topology, devices operate in a chain formation. The Stacking Master determines where the packets are sent. Each unit is connected to two neighboring devices, except for the top and bottom units.

Stacking Members and Unit ID

Stacking Unit IDs are essential to the stacking configuration. The stacking operation is determined during the boot process. The operation mode is determined by the Unit ID selected during the initialization process. Stacking LEDs are dual mode

LEDS. During bootup, the Stacking LEDs indicate the stacking Unit number. When the device is running, the stack ID selector displays the unit ID number. Pressing a second time displays the port speed. For example, if the user selected stand-alone mode, the device boots in the boot-up process as a stand-alone device.

The device units are shipped with a default Unit ID of the stand-alone unit. If the device is operating as a stand-alone unit, all stacking LEDs are off.

Once the user selects a different Unit ID, it is not erased, and remains valid, even if the unit is reset.

Unit ID 1 and Unit ID 2 are reserved for Master enabled units. Unit IDs 3 to 8 can be defined for stack members.

When the Master unit boots or when inserting or removing a stack member, the Master unit initiates a stacking discovering process.

Note: If two members are discovered with the same Unit ID the stack continues to function, however only the unit with the older join time joins the stack. A message is sent to the user, notifying that a unit failed to join the stack.

Removing and Replacing Stacking Members

Stacking member 1 and Stacking member 2 are Stacking Master enabled units. Unit 1 and Unit 2 are either designated as Master Unit or Secondary Master Unit. The Stacking Master assignment is performed during the configuration process. One Master enabled stack member is elected Master, and the other Master enabled stack member is elected Secondary Master, according to the following decision process:

- If only one Stacking Master enabled unit is present, it is elected Stacking Master.
- If two Stacking Masters enabled stacking members are present, and one has been manually configured as the Stacking Master, the manually configured member is elected Stacking Master.
- If two Master enabled units are present and neither has been manually configured as the Stacking Master, the one with the longer up-time is elected Stacking Master.
- If the two Master enabled stacking members are the same age, Unit 1 is elected Stacking Master.
- Two stacking member are considered the same age if they were inserted within the same ten minute interval.

For example, Stack member 2 is inserted in the first minute of a ten-minute cycle, and Stack member 1 is inserted in fifth minute of the same cycle, the units are considered the same age. If there are two Master enabled units that are the same age, then Unit 1 is elected Stacking Master.

The Stacking Master and the Secondary Master maintain a Warm Standby. The Warm Standby ensures that the Secondary Master takes over for the Stacking Master if a failover occurs. This guarantees that the stack continues to operate normally.

During the Warm Standby, the Master and the Secondary Master are synchronized with the static configuration only. When the Stacking Master is configured, the

Stacking Master must synchronize the Stacking Secondary Master. The Dynamic configuration is not saved, for example, dynamically learned MAC addresses are not saved.

Each port in the stack has a specific Unit ID, port type, and port number, which is part of both the configuration commands and the configuration files. Configuration files are managed only from the device Stacking Master, including:

- Saving to the FLASH
- Uploading Configuration files to an external TFTP Server
- Downloading Configuration files from an external TFTP Server

Whenever a reboot occurs, topology discovery is performed, and the master learns all units in the stack. Unit IDs are saved in the unit and are learned through topology discovery. If a unit attempts to boot without a selected Master, and the unit is not operating in stand-alone mode, the unit does not boot.

Configuration files are changed only through explicit user configuration. Configuration files are not automatically modified when:

- Units are Added
- Units are Removed
- Units are reassigned Unit IDs
- Units toggle between Stacking Mode and Stand-alone Mode

Each time the system reboots, the Startup Configuration file in the Master unit is used to configure the stack. If a stack member is removed from the stack, and then replaced with a unit with the same Unit ID, the stack member is configured with the original device configuration. Only ports which are physically present are displayed in the home page, and can be configured through the WebViewMgmt system. Non-present ports are configured through the CLI or SNMP interfaces.

Exchanging Stacking Members

If a stack member with the same Unit ID replaces an existing Unit ID with the same Unit ID, the previous device configuration is applied to the inserted stack member. If the new inserted device has either more than or less ports than the previous device, the relevant port configuration is applied to the new stack member.

Switching between the Stacking Master and the Secondary Master

The Secondary Master replaces the Stacking Master if the following events occur:

- The Stacking Master fails or is removed from the stack.
- Links from the Stacking Master to the stacking members fails.
- A soft switchover is performed with either via web interface or the CLI.

Switching between the Stacking Master and the Secondary Master results in a limited service loss. Any dynamic tables are relearned if a failure occurs. The running configuration file is synchronized between Stacking Master and the Secondary Master, and continues running on the Secondary Master.

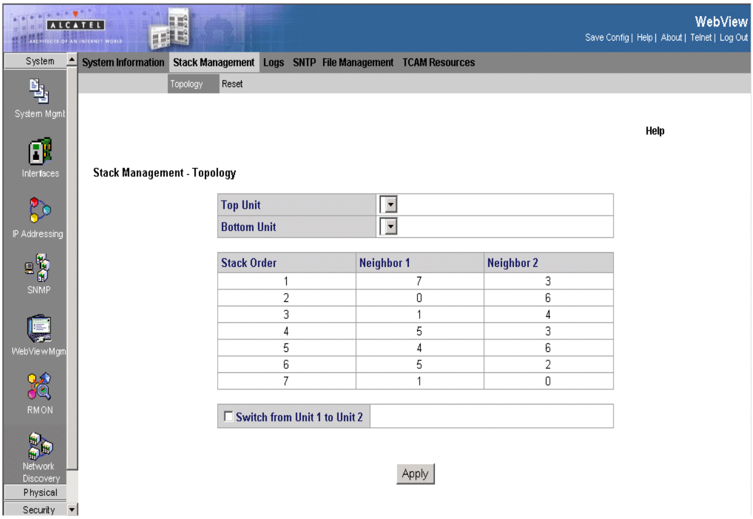
Configuring Stacking

The *Stack Management Topology Page* allows network managers to either reset the entire stack or a specific device. Device configuration changes that are not saved before the device is reset are not saved. If the Stacking Master is reset, the entire stack is reset.

Command Attributes

- **Top Unit** — Indicates the first stack member's number. Possible values are Master and 1-8.
- **Bottom Unit** — Indicates the second stack member's number. Possible values are Master and 1-8.
- **Stack Order** — Displays the number of the unit within the stack.
- **Neighbor 1** — Indicates the first stack member of the stack.
- **Neighbor 2** — Indicates the second stack member of the stack.
- **Switch Stack Control from Unit 1 to Unit 2** — Switches the stack control from the Stack Master to the Secondary Stack Master. The possible field values are:
  - *Checked* — Enables switching the stack control to the Secondary Stack Master.
  - *Unchecked* — Maintains the current stacking control.

Web – Click System, System Management, Stack Management, Topology. Specify the upper and lower stacking members, then click Apply.



Stack Management - Topology

Top Unit	
Bottom Unit	

Stack Order	Neighbor 1	Neighbor 2
1	7	3
2	0	6
3	1	4
4	5	3
5	4	6
6	5	2
7	1	0

□ Switch from Unit 1 to Unit 2

Figure 3-6. Stack Management Topology Page

It is recommended to upgrade software on all units in a stack simultaneously. Use the following steps:

1. Download the file
2. Open the *File Download Page*.
3. Select the Firmware Download field.
4. Enter full path and file name of software to be downloaded to device.
5. Select Download to all Units.
6. Reset the stack.

CLI – The following is an example of stack management commands:

```
Console(config)# stack master unit 2
4-613
Console(config)# stack display-order top 6 bottom 1
4-614
```

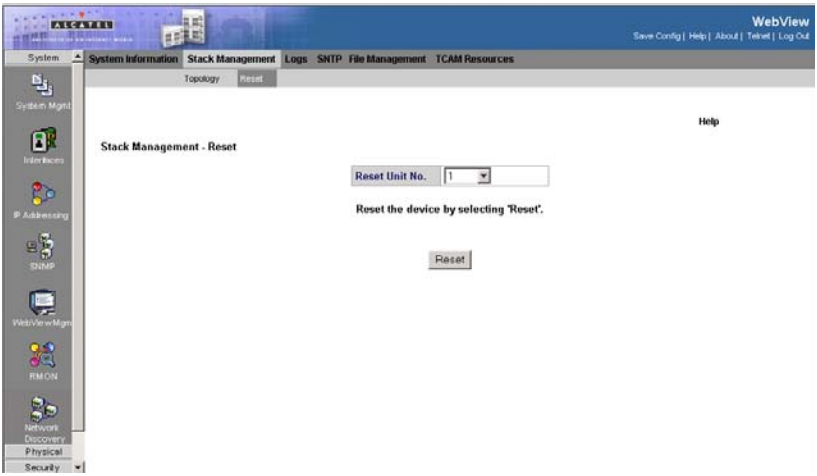
Resetting the Stack

The *Stack Management - Reset Page* resets the stack.

Command Attributes

- **Reset Unit No** — Indicates the unit to be reset.

Web – Click System, System Management, Stack Management, Reset page. Click the Reset button.



Stack Management - Reset

Reset Unit No. 1

Reset the device by selecting 'Reset'.

Figure 3-7. Stack Management - Reset Page

CLI – The following is an example of stack reset commands:

```
Console(config)# stack reload unit 2
4-614
```

Managing System Logs

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.
The default for all logs is information, with the exception of logs in the Remote Log Server, which are errors.

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

Enabling System Logs

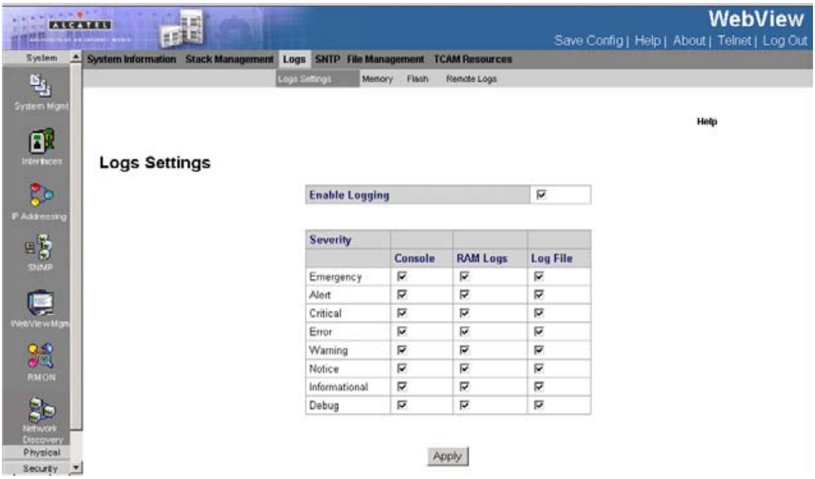
The *Logs Settings Page*contains fields for defining which events are recorded to which logs. It contains fields for enabling logs globally, and parameters for defining logs. The Severity log messages are listed from the highest severity to the lowest. When a severity level is selected, all severity level choices above the selection are selected automatically.

Command Attributes

- **Enable Logging** — Indicates if device global logs for Cache and File are enabled. Console logs are enabled by default. The possible field values are:
  - *Checked* — Enables device logs.
  - *Unchecked* — Disables device logs.
- **Severity** — The following are the available severity logs:

  - *Emergency* — Indicates the highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
  - *Alert* — Indicates the second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
  - *Critical* — Indicates the third highest warning level. 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* — Indicates that a device error has occurred, for example, if a single port is offline.
  - *Warning* — Indicates the lowest level of a device warning. The device is functioning, but an operational problem has occurred.
  - *Notice* — Provides device information, for example, a port is not operating.
  - *Informational* — Provides device information.
  - *Debug* — Provides debugging messages.
- **Console** — Defines the minimum severity level from which logs are sent to the console.
- **RAM Logs** — Defines the minimum severity level from which logs are sent to the Event Log kept in RAM (Cache).
- **Log File** — Defines the minimum severity level from which logs are sent to the Message Log kept in FLASH memory.

Web – Click System, System Management, Logs, Log Settings, and enable logs.



Logs Settings

Enable Logging ☑

Severity			
	Console	RAM Logs	Log File
Emergency	☑	☑	☑
Alert	☑	☑	☑
Critical	☑	☑	☑
Error	☑	☑	☑
Warning	☑	☑	☑
Notice	☑	☑	☑
Informational	☑	☑	☑
Debug	☑	☑	☑

Figure 3-8. Logs Settings Page

CLI – The following is an example of the CLI commands used to view system logs:

```
console# config
4-655
console(config)# logging on
4-591
console(config)# logging console errors
   4-593
console(config)# logging buffered debugging
   4-594
console(config)# logging file alert
   4-594
console(nconfig)# exit
   4-656
console# clear logging file
   4-595
Clear Logging File [y/n]y
```

Viewing Memory Logs

The system allows you to enable or disable event logging, and specify which levels are logged to the RAM (Cache).

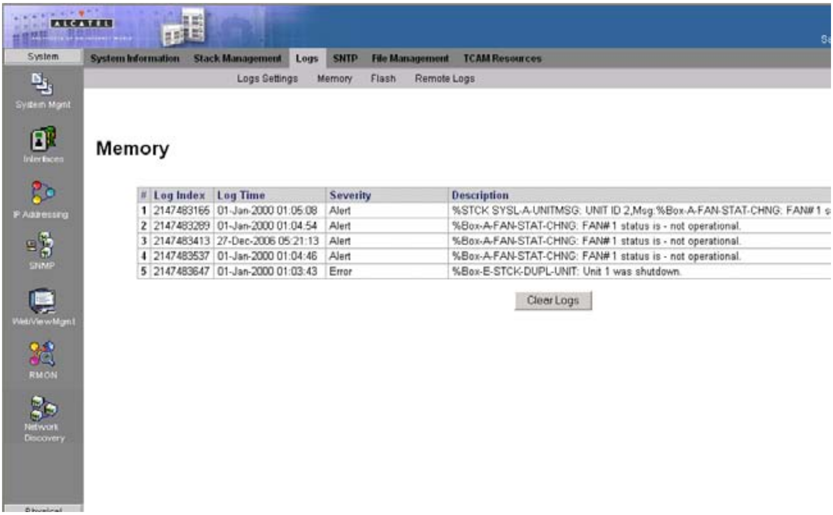
Severe error messages that are logged to the RAM are permanently stored in the switch to assist in troubleshooting network problems. When a severity level is selected, all severity level choices above the selection are selected automatically.

The *Memory Page* allows you to configure and limit system messages that are logged to the RAM.

Command Attributes

- **Log Index** — Displays the log number.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — The following are the available log severity levels:
  - *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
  - *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
  - *Critical* — The third highest warning level. 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, if 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.
  - *Informational* — Provides device information.
  - *Debug* — Provides debugging messages.
- **Description** — Displays the log message text.

Web – Click System, System Management, Logs, Memory.



Memory

#	Log Index	Log Time	Severity	Description
1	2147483166	01-Jan-2000 01:05:08	Alert	%STCK SYSL-A-UNITMSG: UNIT ID 2,Msg:%Box-A-FAN-STAT-CHNG: FAN# 1 s
2	2147483289	01-Jan-2000 01:04:54	Alert	%Box-A-FAN-STAT-CHNG: FAN# 1 status is - not operational.
3	2147483413	27-Dec-2006 05:21:13	Alert	%Box-A-FAN-STAT-CHNG: FAN# 1 status is - not operational.
4	2147483537	01-Jan-2000 01:04:46	Alert	%Box-A-FAN-STAT-CHNG: FAN# 1 status is - not operational.
5	2147483647	01-Jan-2000 01:03:43	Error	%Box-E-STCK-DUPL-UNIT: Unit 1 was shutdown.

Figure 3-9. Memory Page

CLI – The following is an example of the CLI commands used to view memory logs:

```
Console# show logging
4-599
Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped
(severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.
File logging: level notifications. File Messages: 0 Dropped (severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).
2 messages were not logged (resources)
Application filtering control
Application Event Status
----------- ----- ------
AAA Login Enabled
File system Copy Enabled
File system Delete-Rename Enabled
Management ACL Deny Enabled
Buffer log:
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/0, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/1, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/2, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/3, changed
state to up
11-Aug-2004 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/0, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/1, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/2, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

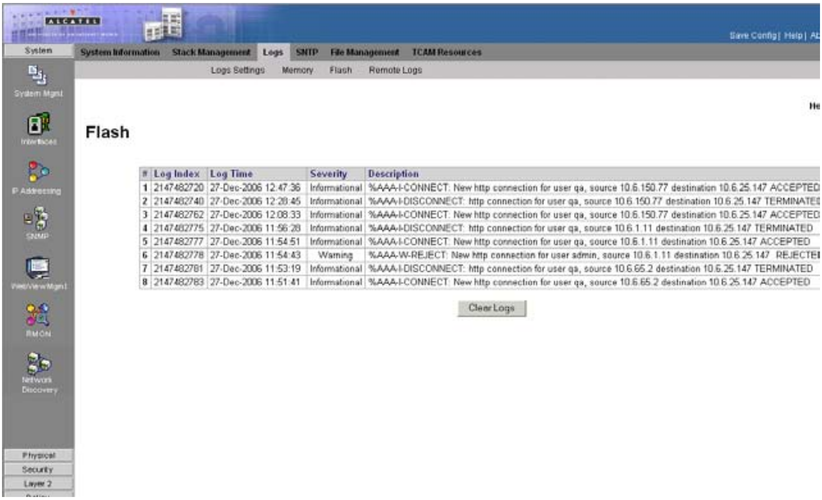
Viewing the Device FLASH Logs

The *FLASH Logs Page* contains all system logs in a chronological order that are saved in FLASH memory.

Command Attributes

- **Log Index** — Displays the log number.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — Displays the log severity.
- **Description** — Displays the log message text.

Web – Click System, System Management, Logs, Flash.



Flash

#	Log Index	Log Time	Severity	Description
1	2147482720	27-Dec-2006 12:47:36	Informational	%AAA-I-CONNECT: New http connection for user qa, source 10.6.150.77 destination 10.6.25.147 ACCEPTED
2	2147482740	27-Dec-2006 12:28:45	Informational	%AAA-I-DISCONNECT: http connection for user qa, source 10.6.150.77 destination 10.6.25.147 TERMINATED
3	2147482762	27-Dec-2006 12:08:33	Informational	%AAA-I-CONNECT: New http connection for user qa, source 10.6.150.77 destination 10.6.25.147 ACCEPTED
4	2147482775	27-Dec-2006 11:56:28	Informational	%AAA-I-DISCONNECT: http connection for user qa, source 10.6.1.11 destination 10.6.25.147 TERMINATED
5	2147482777	27-Dec-2006 11:54:51	Informational	%AAA-I-CONNECT: New http connection for user qa, source 10.6.1.11 destination 10.6.25.147 ACCEPTED
6	2147482778	27-Dec-2006 11:54:43	Warning	%AAA-W-REJECT: New http connection for user admin, source 10.6.1.11 destination 10.6.25.147 REJECTED
7	2147482781	27-Dec-2006 11:53:19	Informational	%AAA-I-DISCONNECT: http connection for user qa, source 10.6.65.2 destination 10.6.25.147 TERMINATED
8	2147482783	27-Dec-2006 11:51:41	Informational	%AAA-I-CONNECT: New http connection for user qa, source 10.6.65.2 destination 10.6.25.147 ACCEPTED

Figure 3-10. FLASH Logs Page

CLI – The following is an example of the CLI commands used to display FLASH logs:

```
Console# show logging file                                         4-601
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 12.1.1.2 Logging: warning. Messages: 14 Dropped.
SysLog server 1.1.1.1 Logging: info. Messages: 0 Dropped.
01-Jan-2000 01:12:01:%COPY-W-TRAP: The copy operation was completed
successfully
01-Jan-2000 01:11:49:%LINK-I-Up: 1/e11
01-Jan-2000 01:11:46:%LINK-I-Up: 1/e12
01-Jan-2000 01:11:42:%LINK-W-Down: 1/e13
```

Remote Log Configuration

The *Remote Log Page* allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the event messages sent to only those messages at or above a specified level.

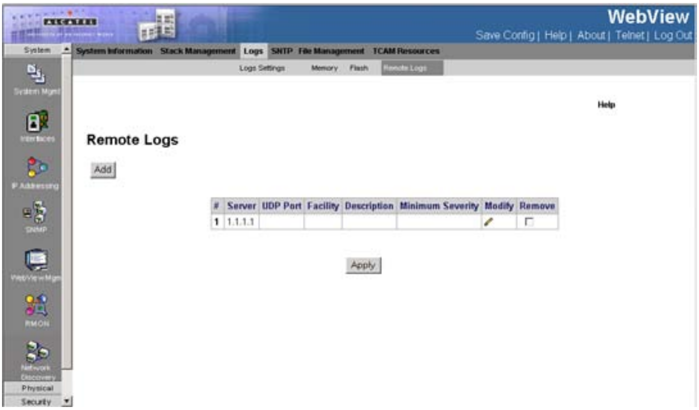
Command Attributes

- **Server** — Specifies the IP address of the server to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 - 65535. The default value is 514.
- **Facility** — Defines an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level

is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is *Local 7*. The possible field values are *Local 0 - Local 7*.

- **Description**— Displays the user-defined server description.
- **Minimum Severity** — Indicates the minimum severity from which logs are sent to the server. For example, if *Notice* is selected, all logs with a severity level of *Notice* and higher are sent to the remote server.
- **Remove** — Deletes the currently selected server from the Servers list. The possible field values are:
  - *Checked* — Removes the selected server from the *Remote Log Page*. Once removed, logs are no longer sent to the removed server.
  - *Unchecked* — Maintains the remote servers.

Web – Click System, System Management, Logs, Remote Logs. Specify Remote Log Status.



Remote Logs

#	Server	UDP Port	Facility	Description	Minimum Severity	Modify	Remove
1	1.1.1.1					✎	□

Figure 3-11. Remote Log Page

CLI – Enable system logging and then specify the level of messages to be logged to remote logs. Use the **show logging** command to display the current settings.

```
Console# show logging file
4-601
Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped
(severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.
File logging: level notifications. File Messages: 0 Dropped (severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).
2 messages were not logged (resources)
Application filtering control

Buffer log:
11-Aug-2004 15:41:43:%LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
11-Aug-2004 15:41:43:%LINK-3-UPDOWN: Interface Ethernet1/0, changed
state to up
11-Aug-2004 15:41:43:%LINK-3-UPDOWN: Interface Ethernet1/1, changed
state to up
11-Aug-2004 15:41:43:%LINK-3-UPDOWN: Interface Ethernet1/2, changed
state to up
11-Aug-2004 15:41:43:%LINK-3-UPDOWN: Interface Ethernet1/3, changed
state to up
11-Aug-2004 15:41:43:%SYS-5-CONFIG_I: Configured from memory by console
11-Aug-2004 15:41:39:%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
11-Aug-2004 15:41:39:%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/0, changed state to down
11-Aug-2004 15:41:39:%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/1, changed state to down
11-Aug-2004 15:41:39:%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/2, changed state to down
11-Aug-2004 15:41:39:%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/3, changed state to down
```

Configuring SNTP

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

Note: The system time is not saved in NVRAM.

The device can poll the following server types for the server time:

- Unicast
- Anycast
- Broadcast

Time sources are established by stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock is. The device receives time from stratum 1 and above.
The following is an example of stratums:

- **Stratum 0** — A real time clock (such as a GPS system) is used as the time source.
- **Stratum 1** — A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **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.

Information received from SNTP servers is evaluated based on the Time level and server type. SNTP time definitions are assessed and determined by the following time levels:

- **T1** — The time at which the original request was sent by the client.
- **T2** — The time at which the original request was received by the server.
- **T3** — The time at which the server sent the client a reply.
- **T4** — The time at which the client received the server's reply.

Polling for Unicast Time Information

Polling for Unicast information is used for polling a server for which the IP address is known. T1 - T4 are used to determine the server time. This is the preferred method for synchronizing device time.

Polling for Anycast Time Information

Polling for Anycast information is used when the server IP address is unknown. The first Anycast server to return a response is used to set the time value. Time levels T3 and T4 are used to determine the server time. Using Anycast time information for synchronizing device time is preferred to using Broadcast time information.

Polling For Broadcast Time Information

Broadcast information is used when the server IP address is unknown. When a broadcast message is sent from an SNTP server, the SNTP client listens for the response. The SNTP client neither sends time information requests nor receives responses from the Broadcast server.

Message Digest 5 (MD5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is 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.

Defining SNTP Global Settings

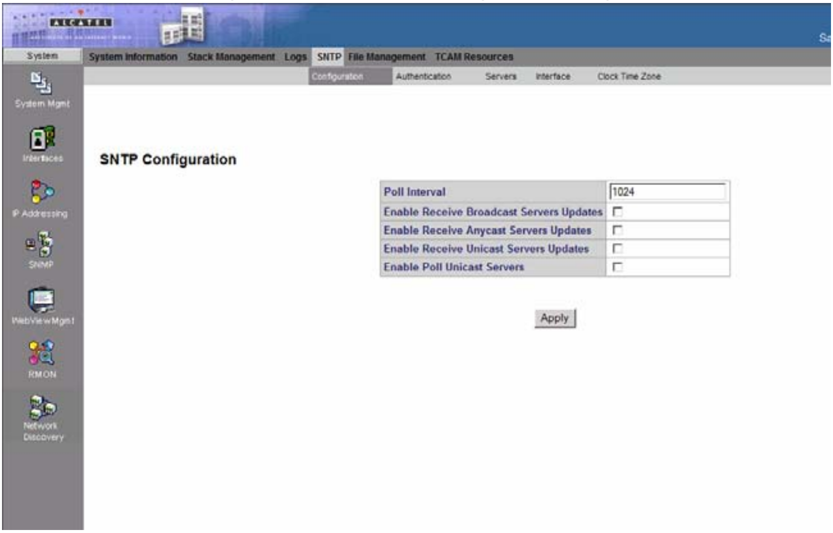
The *SNTP Configuration Page* provides information for defining SNTP parameters globally.

Command Attributes

- **Poll Interval** — Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 1024 seconds.
- **Enable Receive Broadcast Servers Updates** — Defines whether or not the device monitors the SNTP servers for the interface’s Broadcast server time information. The possible values are:
  - *Checked* — Enables the device to receive Broadcast server updates.
  - *Unchecked* — Disables the device from receiving Broadcast server updates.
- **Enable Receive Anycast Servers Updates —** Defines whether or not the device polls the SNTP server for Anycast server time information. If both the *Enable Receive Anycast Servers Update* and the *Enable Receive Broadcast Servers Update* fields are enabled, the system time is set according the Anycast server time information. The possible values are:
  - *Checked* — Enables the device to receive Anycast server updates.
  - *Unchecked* — Disables the device from receiving Anycast server updates.
- **Enable Receive Unicast Servers Updates** — Defines whether or not the device polls the SNTP server for Unicast server time information. If the *Enable Receive Broadcast Servers Updates*, *Enable Receive Anycast Servers Updates*, and *Enable Receive Unicast Servers Updates* fields are all enabled, the system time is set according the Unicast server time information. The possible values are:
  - *Checked* — Enables the device to receive Unicast server updates.
  - *Unchecked* — Disables the device from receiving Unicast server updates.
- **Enable Poll Unicast Servers** — Defines whether or not the device sends SNTP Unicast forwarding information to the SNTP server. The possible values are:
  - *Checked* — Enables the device to receive Poll Unicast server updates.
  - *Unchecked* — Disables the device from receiving Poll Unicast server updates.

Web – Select System, System Management, SNTP, Configuration. Define the fields and click Apply.

Figure 3-12. SNTP Configuration Page



SNTP Configuration

Poll Interval	1024
Enable Receive Broadcast Servers Updates	□
Enable Receive Anycast Servers Updates	□
Enable Receive Unicast Servers Updates	□
Enable Poll Unicast Servers	□

CLI - The following is an example of the SNTP global parameters commands:

```
Console(config)# sntp client poll timer 120
4-355
Console(config)# sntp Broadcast client enable
4-356
Console(config)# sntp unicast client enable
4-358
Console(config)# sntp anycast client enable
4-357
Console(config)# sntp unicast client poll
4-359
```

Defining SNTP Authentication

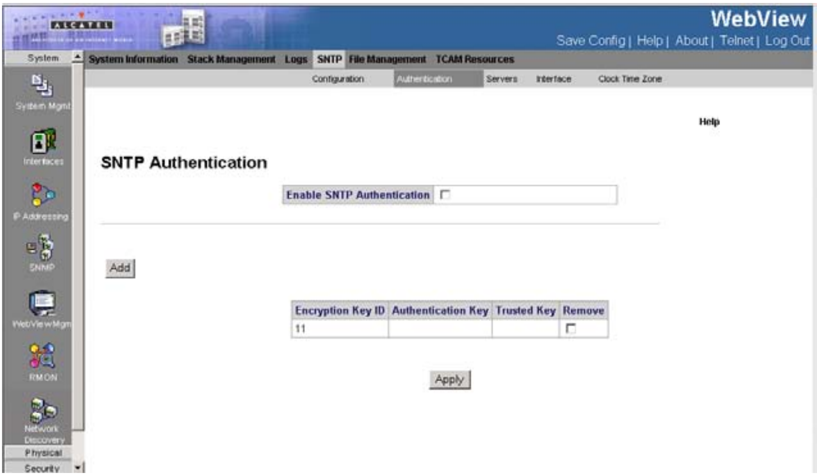
The *SNTP Authentication Page* provides parameters for defining the means by which the SNTP server is authenticated.

Command Attributes

- **Enable SNTP Authentication** — Indicates if authenticating an SNTP session between the device and an SNTP server is enabled on the device. The possible field values are:
  - *Checked* — Authenticates SNTP sessions between the device and SNTP server.
  - *Unchecked* — Disables authenticating SNTP sessions between the device and SNTP server.
- **Encryption Key ID —** Indicates if the encryption key identification is used to authenticate the SNTP server and device. The field value is up to 4294967295.

- **Authentication Key —** Indicates the key used for authentication.
- **Trusted Key —** Indicates the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.
- **Remove** — Removes Encryption Key IDs. The possible field values are:
  - *Checked* **—** Removes the selected Encryption Key ID
  - *Unchecked* **—** Maintains the Encryption Key IDs. This is the default value.

Web – Select System, System Management, SNTP, Authentication. Define the fields and click Apply.



SNTP Authentication

Enable SNTP Authentication ☐

Encryption Key ID	Authentication Key	Trusted Key	Remove
11			☐

Figure 3-13. SNTP Authentication Page

CLI - The following is an example of the SNTP authentication commands:

```
Console(config)# sntp authentication-key 8 md5 ClkKey
4-353
Console(config)# sntp trusted-key 8
4-354
Console(config)# sntp authenticate
4-353
```

Defining SNTP Servers

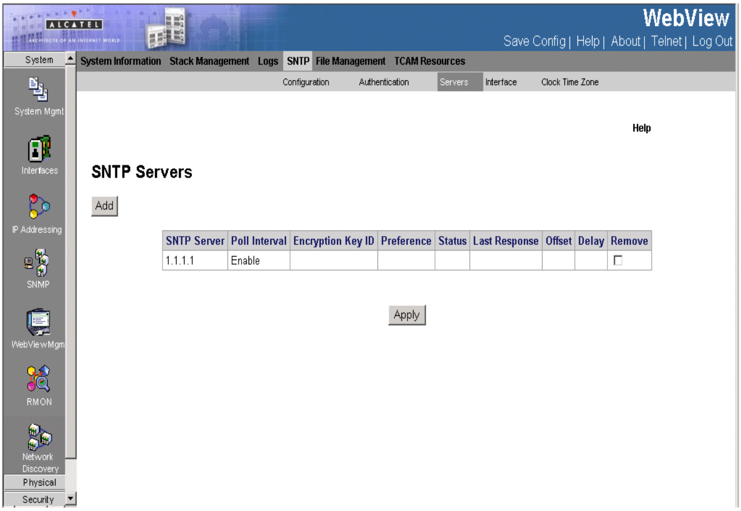
The *SNTP Servers Page* contains information for enabling SNTP servers, as well as adding new SNTP servers. In addition, the *SNTP Servers Page* enables the device to request and accept SNTP traffic from a server.

Command Attributes

- **SNTP Server —** Displays user-defined SNTP server IP addresses. Up to eight SNTP servers can be defined.
- **Poll Interval —** Indicates whether or not the device polls the selected SNTP server for system time information.

- **Encryption Key ID —** Displays the encryption key identification used to communicate between the SNTP server and device. The field range is 1-4294967295.
- **Preference** — Indicates the SNTP server providing SNTP system time information. The possible field values are:
  - *Primary* — Indicates the primary server provides SNTP information.
  - *Secondary* — Indicates the backup server provides SNTP information.
- **Status** — Displays the SNTP server operating status.
- **Last Response** — Displays the last time a response was received from the SNTP server.
- **Offset** — Indicates the time difference between the device local clock and the acquired time from the SNTP server.
- **Delay** — Indicates the amount of time it takes for a device request to reach the SNTP server.
- **Remove** — Removes SNTP servers from the SNTP server list. The possible field values are:
  - *Checked* — Removes the SNTP server.
  - *Unchecked* — Maintains the SNTP server.

Web – Select System, System Management, SNTP, Servers. Define the fields and click Apply.



SNTP Server	Poll Interval	Encryption Key ID	Preference	Status	Last Response	Offset	Delay	Remove
1.1.1.1	Enable							☐

Figure 3-14. SNTP Servers Page

CLI - The following is an example of the SNTP server commands:

```
Console(config)# sntp server 192.1.1.1
4-360
```

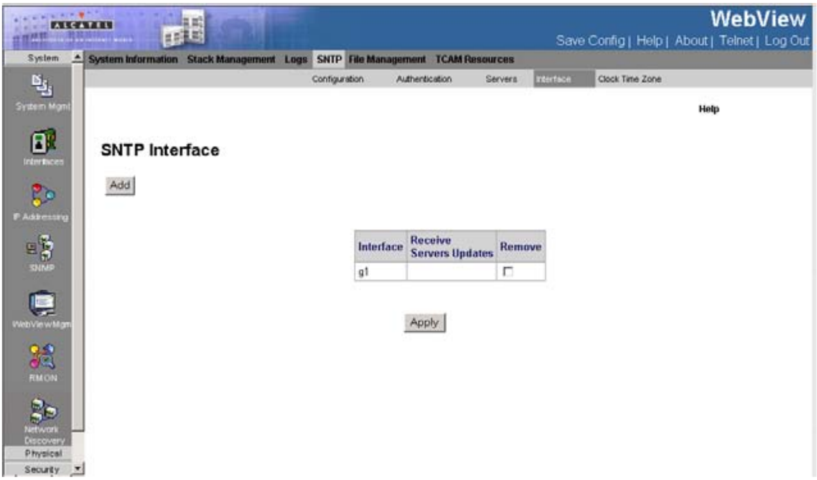
Defining SNTP Interface Settings

The *SNTP Interface Page* contains fields for setting SNTP on different interfaces.

Command Attributes

- **Interface —** Indicates the interface on which SNTP can be enabled. The possible field values are:
  - *Port* — Indicates the specific port number on which SNTP is enabled.
  - *LAG* — Indicates the specific LAG number on which SNTP is enabled.
  - *VLAN* — Indicates the specific VLAN number on which SNTP is enabled.
- **Receive Servers Updates** — Enables the interface to receive or not receive updates.
- **Remove** — Removes SNTP interfaces.
  - *Checked* — Removes the selected SNTP interface.
  - *Unchecked* — Maintains the selected SNTP interfaces.

Web – Select System, System Management, SNTP, Interface. Define the fields and click Apply.



SNTP Interface

Interface	Receive Servers Updates	Remove
g1		□

Figure 3-15. SNTP Interface Page

CLI - The following is an example of the SNTP interface commands:

```
Console(config)# interface ethernet 1/e3                                4-376
Console(config-if)# sntp client enable                                  4-357
```

Configuring System Time

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

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to eight time server IP addresses. The switch attempts to poll each server in the configured sequence. Polling can be enabled per interface.

Configuring Daylight Savings Time

The *Clock Time Zone Page* contains fields for defining system time parameters for both the local hardware clock and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device.

The following is a list of Daylight Savings Time start and end times in specific countries:

- **Albania** — From the last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia** - **Tasmania —** From the beginning of October until the end of March.
- **Armenia** — From the last weekend of March until the last weekend of October.
- **Austria** — From the last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with Daylight Savings Time in the United States.
- **Belarus** — From the last weekend of March until the last weekend of October.
- **Belgium** — From the last weekend of March until the last weekend of October.
- **Brazil** — From the third Sunday in October until the third Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- **Chile** — In Easter Island, from March 9 until October 12. In the rest of the country, from the first Sunday in March or after 9th March.
- **China** — China does not use 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** — From the last weekend of March until the last weekend of October.
- **Denmark** — From the last weekend of March until the last weekend of October.

- **Egypt** — From the last Friday in April until the last Thursday in September.
- **Estonia** — From the last weekend of March until the last weekend of October.
- **Finland** — From the last weekend of March until the last weekend of October.
- **France** — From the last weekend of March until the last weekend of October.
- **Germany** — From the last weekend of March until the last weekend of October.
- **Greece** — From the last weekend of March until the last weekend of October.
- **Hungary** — From the last weekend of March until the last weekend of October.
- **India** — India does not use Daylight Saving Time.
- **Iran** — From Farvardin 1 until Mehr 1.
- **Iraq** — From April 1 until October 1.
- **Ireland** — From the last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.
- **Italy** — From the last weekend of March until the last weekend of October.
- **Japan** — Japan does not use Daylight Saving Time.
- **Jordan** — From the last weekend of March until the last weekend of October.
- **Latvia** — From the last weekend of March until the last weekend of October.
- **Lebanon** — From the last weekend of March until the last weekend of October.
- **Lithuania** — From the last weekend of March until the last weekend of October.
- **Luxembourg** — From the last weekend of March until the last weekend of October.
- **Macedonia** — From the 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** — From the last weekend of March until the last weekend of October.
- **Montenegro** — From the last weekend of March until the last weekend of October.
- **Netherlands** — From the 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 March 15.
- **Norway** — From the last weekend of March until the last weekend of October.
- **Paraguay** — From April 6 until September 7.
- **Poland** — From the last weekend of March until the last weekend of October.
- **Portugal** — From the last weekend of March until the last weekend of October.
- **Romania** — From the last weekend of March until the last weekend of October.
- **Russia** — From the last weekend of March until the last weekend of October.
- **Serbia** — From the last weekend of March until the last weekend of October.
- **Slovak Republic** - From the last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not use Daylight Saving Time.
- **Spain** — From the last weekend of March until the last weekend of October.
- **Sweden** — From the last weekend of March until the last weekend of October.

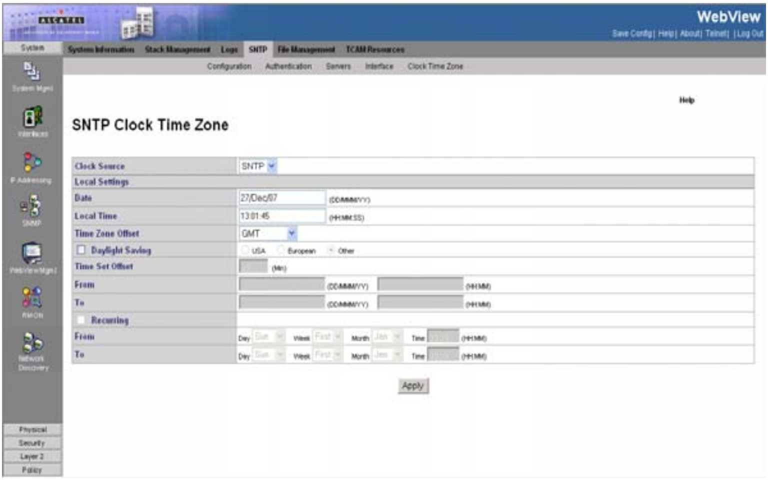
- **Switzerland** — From the last weekend of March until the last weekend of October.
- **Syria** — From March 31 until October 30.
- **Taiwan** — Taiwan does not use Daylight Saving Time.
- **Turkey** — From the last weekend of March until the last weekend of October.
- **United Kingdom** — From the last weekend of March until the last weekend of October.
- **United States of America** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.

Command Attributes

- **Clock Source** — The source used to set the system clock. The possible field values are:
  - *None* — Indicates that a clock source is not used. The clock is set locally.
  - *SNTP* — Indicates that the system time is set via an SNTP server.
- **Date** — The system date. The field format is Day/Month/Year. For example: 04/May/50 (May 4, 2050).
- **Local Time** — The system time. The field format is HH:MM:SS. For example: 21:15:03.
- **Time Zone Offset** — The difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT –5.
- **Daylight Savings** — Enables automatic Daylight Savings Time (DST) on the device based on the device’s location. There are two types of daylight settings, either by a specific date in a particular year or 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. The possible field values are:
  - *USA* — Enables switching to DST at 2:00 a.m. on the first Sunday of April, and reverts to standard time at 2:00 a.m. on the last Sunday of October.
  - *European* — Enables switching 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* — Indicates the DST definitions are user-defined based on the device locality. If Other is selected, the *From* and *To* fields must be defined.
- **Time Set Offset (1-1440) —** Used for non-USA and European countries to set the amount of time for DST (in minutes). The default time is 60 minutes.
- **From** — Indicates the time that DST begins in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST begins on October 25, 2007 at 5:00 am, the two fields should be set to 25/Oct/07 and 05:00. The possible field values are:
  - *Date* — The date on which DST begins. The possible field range is 1-31.
  - *Month* — The month of the year in which DST begins. The possible field range is Jan-Dec.

  - *Year* — The year in which the configured DST begins.
  - *Time* — The time at which DST begins. The field format is HH:MM. For example: 05:30.
- **To** — Indicates the time that DST ends in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST ends on March 23, 2008 at midnight, the two fields should be 23/Mar/08 and 00:00. The possible field values are:
  - *Date* — The date on which DST ends. The possible field range is 1-31.
  - *Month* — The month of the year in which DST ends. The possible field range is Jan-Dec.
  - *Year*— The year in which the configured DST ends.
  - *Time* — The time at which DST starts. The field format is HH:MM. For example: 05:30.
- **Recurring** — Enables user-defined DST for countries in which DST is constant from year to year, other than the USA and Europe.
- **From** — The time that DST begins each year. In the example, DST begins locally every first Sunday in April at midnight. The possible field values are:
  - *Day* — The day of the week from which DST begins every year. The possible field range is Sunday-Saturday.
  - *Week* — The week within the month from which DST begins every year. The possible field range is 1-5.
  - *Month* — The month of the year in which DST begins every year. The possible field range is Jan-Dec.
  - *Time* — The time at which DST begins every year. The field format is Hour:Minute. For example: 02:10.
- **To** — The time that DST ends each year. In the example, DST ends locally every first Sunday in October at midnight. The possible field values are:
  - *Day* — The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.
  - *Week* — The week within the month at which DST ends every year. The possible field range is 1-5.
  - *Month* — The month of the year in which DST ends every year. The possible field range is Jan-Dec.
  - *Time* — The time at which DST ends every year. The field format is HH:MM. For example: 05:30.

Web – Select System, System Management, SNTP, Clock Time Zone. Define the fields and set the offset for your time zone relative to the UTC, and click Apply.



SNTP Clock Time Zone

Clock Source	SNTP
Local Settings	
Date	27/Dec/07 (DD/MMM/YY)
Local Time	13:01:45 (HH:MM:SS)
Time Zone Offset	GMT
□ Daylight Saving	○ USA ○ European ○ Other
Time Set Offset	(Min)
From	(DD/MMM/YY) (HH:MM)
To	(DD/MMM/YY) (HH:MM)
□ Recurring	
From	Day Sun Week First Month Jan Time (HH:MM)
To	Day Sun Week First Month Jan Time (HH:MM)

Figure 3-16. Clock Time Zone Page

CLI - The following is an example of the system clock commands:

```
Console# clock set 13:32:00 7 Mar 2002
4-349
Console# configure                                                    4-655
Console(config)# clock source sntp
4-350
Console(config)# clock timezone -6 zone CST
4-350
Console(config)# clock summer-time recurring first sun apr 2:00 last sun
oct 2:00
4-351
```

Managing System Files

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

The system run-time software and configuration information is kept in files which may be saved, copied, uploaded for host-based storage and manipulation. The system files include:

- **Boot Files** — The system uses two identical copies of the boot image, stored in flash. The first copy is used when the system comes up.
- **Software Image Files** — two images are stored. The device boots from one, and the other is used as a redundant backup.

- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted. The Startup file is created by copying the configuration commands from the Running Configuration file or the Backup Configuration file.
- **Running Configuration File** — Contains all 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 file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Image files** — Software upgrades are used when a new version file is downloaded. The file is checked for the right format, and that it is complete. After a successful download, the new version is marked, and is used after the device is reset.

Downloading System Files

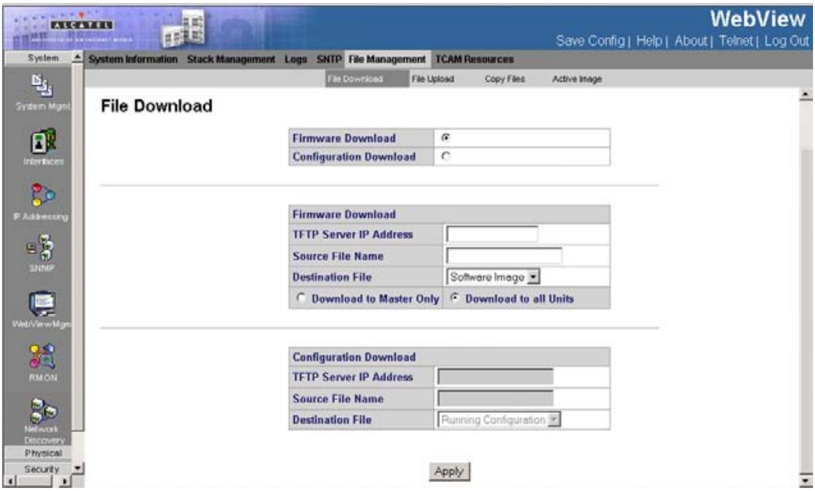
There are two types of files, firmware files and configuration files. The firmware files manage the device, and the configuration files configure the device for transmissions. Only one type of download can be performed at any one time. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”). The *File Download Page* contains parameters for downloading system files.

Command Attributes

- **Firmware Download/Configuration Download** — Indicates whether a firmware file or a configuration is being downloaded. If *Firmware Download* is selected, the Configuration Download fields are grayed out. If *Configuration Download* is selected, the Firmware Download fields are grayed out.
- **TFTP Server IP Address** — Specifies the TFTP Server IP Address from which files are downloaded.
- **Source File Name** — Specifies the file to be downloaded.
- **Destination File** — Specifies the destination file type to which to the file is downloaded. The possible field values are:
  - *Software Image* — Downloads the Image file.
  - *Boot Code* — Downloads the Boot file.
- **Download to Master Only —** Downloads the system file only to the Master.
- **Download to All Units —** Downloads the system file to all units.

- **Configuration Download** — Indicates that the download is for configuration files. If *Configuration Download* is selected, the Firmware Download fields are grayed out.
- **Configuration TFTP Server IP Address** — Specifies the TFTP Server IP Address from which the configuration files are downloaded.
- **Configuration Source File Name** — Specifies the configuration files to be downloaded.
- **Configuration Destination File** — Specifies the destination file to which to the configuration file is downloaded. The possible field values are:
    - *Running Configuration* — Downloads commands into the Running Configuration file.
    - *Startup Configuration* — Downloads the Startup Configuration file, and overwrites the old Startup Configuration file.

Web – Click System, System Management, File Management, File Download. Define the fields. Click Apply.



File Download

Firmware Download	●
Configuration Download	○

Firmware Download	
TFTP Server IP Address	
Source File Name	
Destination File	Software Image
○ Download to Master Only	● Download to all Units

Configuration Download	
TFTP Server IP Address	
Source File Name	
Destination File	Running Configuration

Figure 3-17. File Download Page

CLI – The following is an example of downloading system files using CLI commands:

```
Console# copy tftp://172.16.101.101/file1 image
4-365

Accessing file 'file1' on 172.16.101.101..
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

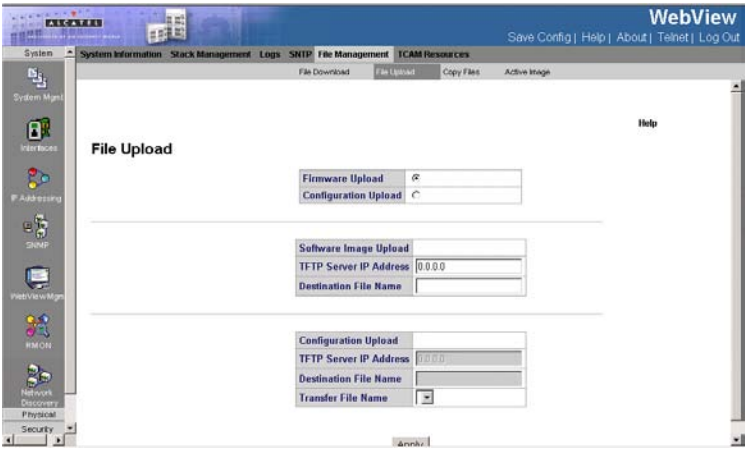
Uploading System Files

The *File Upload Page* contains fields for uploading the software from the device to the TFTP server.

Command Attributes

- **Firmware Upload** — Specifies that the software image file is uploaded. If *Firmware Upload* is selected, the Configuration Upload fields are grayed out.
- **Configuration Upload** — Specifies that the Configuration file is uploaded. If *Configuration Upload* is selected, the Software Image Upload fields are grayed out.
- **Software TFTP Server IP Address** — Specifies the TFTP Server IP Address to which the Software Image is uploaded.
- **Software Destination File Name** — Specifies the software image file path to which the file is uploaded.
- **Configuration TFTP Server IP Address** — Specifies the TFTP Server IP Address to which the Configuration file is uploaded.
- **Configuration Destination File Name**— Specifies the file name to which the Startup Configuration file is uploaded.
- **Configuration Transfer file name** — Specifies the Configuration file name that is uploaded. The possible field values are:
  - *Running Configuration* — Uploads the Running Configuration file.
  - *Startup Configuration* — Uploads the Startup Configuration file.

Web – Click System, System Management, File Management, File Upload. Define the fields. Click Apply.



File Upload

Firmware Upload	●
Configuration Upload	○

Software Image Upload	
TFTP Server IP Address	0.0.0.0
Destination File Name	

Configuration Upload	
TFTP Server IP Address	0.0.0.0
Destination File Name	
Transfer File Name	

Figure 3-18. File Upload Page

CLI – The following is an example of downloading system files using CLI commands:

```
Console# copy tftp://172.16.101.101/file1 image
4-365

Accessing file 'file1' on 172.16.101.101..
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

Copying Files

Files can be copied and deleted from the *Copy Files Page*.

Command Attributes

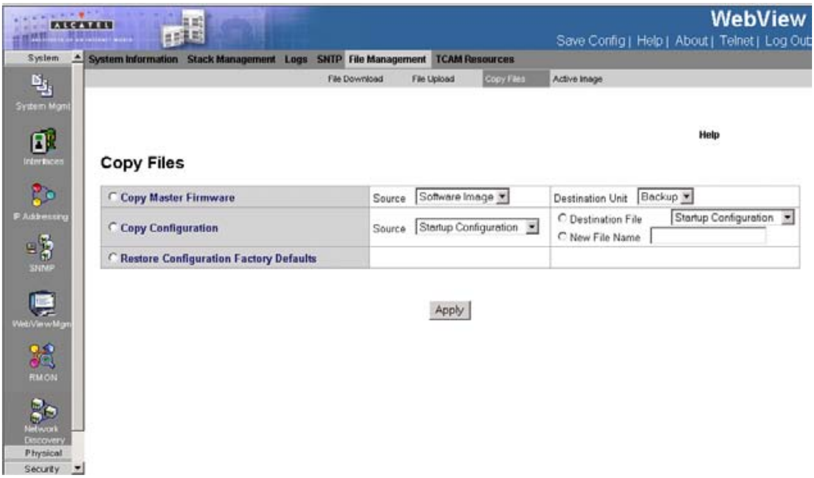
- **Copy Master Firmware** — Copies the Firmware file currently running on the Stacking Master. The possible field values are selected from the following list boxes:
  - *Source* — Select if the Software Image or Bootcode file will be copied.
  - *Destination Unit* — Select the stacking member to which the firmware is copied, the possible field values are All, Backup, and stacking members 1-4.
- **Copy Configuration** — Copies the Running Configuration File. The possible field values are: The possible field values are:
  - *Source* — Select if the Starting Configuration file, the Running Configuration file,

or the Backup file will be copied.

- *Destination* — Specifies the usage for the source file after it is copied. It may be used as a Starting Configuration file, the Running Configuration file, the Backup file, or as a configuration file with a new name.

- **Restore Configuration Factory Defaults** — Resets the Configuration file to the factory defaults. The factory defaults are reset after the device is reset. When unselected, the device maintains the current Configuration file.

Web – System, System Management, File Management, Copy Files. Define the fields. Click Apply.



Copy Files

○ Copy Master Firmware — Source: Software Image — Destination Unit: Backup

○ Copy Configuration — Source: Startup Configuration — ○ Destination File: Startup Configuration; ○ New File Name:

○ Restore Configuration Factory Defaults

Figure 3-19. Copy Files Page

CLI – The following is an example of downloading system files using CLI commands:

```
Console# copy running-config startup-config
4-365
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

Active Image

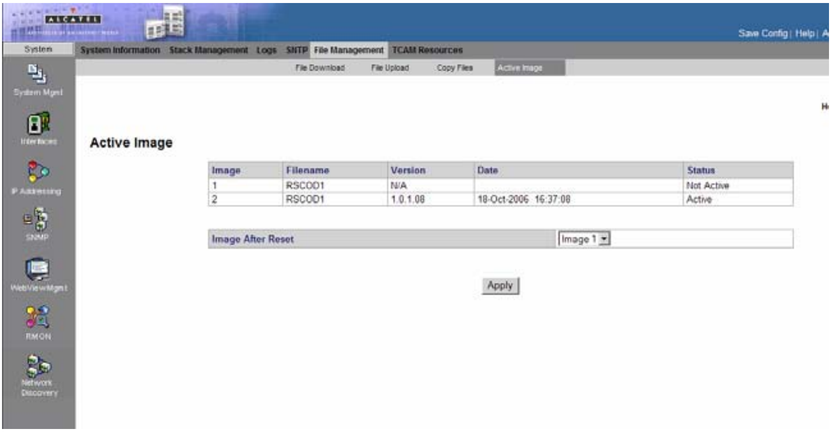
The *Active Image Page* allows network managers to select and reset the Image files. The Active Image file for each unit in a stacking configuration can be individually selected.

Command Attributes

- **Image** – Binary file that contains executable code

- **Filename** – The name of the file
- **Version** – Binary code version
- **Date** – Version's date
- **Status** – Indicates Image status
- **Image After Reset** – The Image file which is active on the unit after the device is reset. The possible field values are:
  - *Image 1* — Activates Image file 1 after the device is reset.
  - *Image 2* — Activates Image file 2 after the device is reset.

Web – System, System Management, File Management, Active Image. Define the fields. Click Apply.



Active Image

Image	Filename	Version	Date	Status
1	RSCOD1	N/A		Not Active
2	RSCOD1	1.0.1.08	18-Oct-2006 16:37:08	Active

Image After Reset: Image 1

Figure 3-20. Active image Page

TCAM Resources

The *TCAM Resources Page* display the availability of TCAM resources (Ternary Content Addressable Memory) across the stack. TCAM is used for high-speed searching throughout the stack, in order to perform security, QoS, and other types of applications. In contrast with binary CAM, TCAM allows a third matching state of "X" or "Don't Care" bits in data searches (the first two bit types are "0" and "1"), adding more flexibility to searches. However, the need to encode three possible states instead of two also adds greater resource costs.

The maximum number of rules that may be allocated by all applications on the device is 1024.

The following table lists all applications that can allocate TCAM rules. Each allocation has its specific allocation policy.

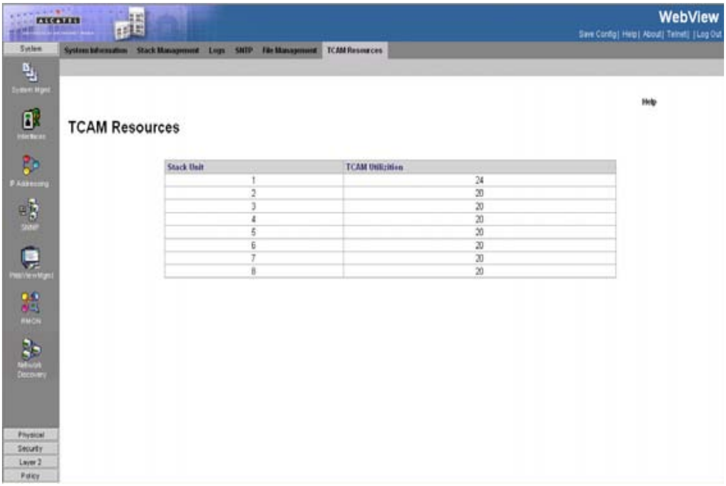
Note: Some applications allocate rules upon their initiation. Additionally, applications that initialize during system boot use some of their rules during the startup process.

Table 3-3. TCAM Allocation

Application	Per Port/ Per Device	Allocation on Activation	Application Upper Limit	TCAM rules per User ACL	Comments
QoS Advanced Mode rules	Port	6/ device	No limit	1 or 2 TCAM entries per each rule.	Feature is activated by default.
Access Control Rules	Port	6/ device	No limit	1 or 2 TCAM entries per each rule.	Feature is activated by default.
PVE	Port	2/port or LAG	---	---	Feature is activated by default. Allocation done only during initialization.
IP Subnet VLAN	Port	0	255	2 or 4	Rules are duplicated for both IP and MAC based VLANs.
Protocol Based VLAN	Port	0	No limit	1 or 2	Rules are duplicated for both IP and MAC based VLANs.
MAC Based VLAN	Port	0	432	1 or 2	Rules are duplicated for both IP and MAC based VLANs.
DHCP Snooping	Device	2/ device	No limit	8 TCAM entries/1 DHCP Snooping rule	
IP Source Guard	Port	0	No limit	1 TCAM entry/1 IP Source Guard entry	
ARP Inspection	Device	2/ device	128	4 TCAM entries/1 ARP Inspection rule	
VLAN Rate Limiting	Both	0	255	1 global rule/1 VLAN Rate Limit. Additional rule is created for each “permit” rule on the interface.	

Command Attributes

- **Stack Unit** – Indicates the stacking member for which TCAM resource usage is displayed.
- **TCAM Utilization** – Percentage of the available TCAM resources which are used. For example, if more ACLs and policy maps are defined, the system will use more TCAM resources.



TCAM Resources

Stack Unit	TCAM Utilization
1	24
2	20
3	20
4	20
5	20
6	20
7	20
8	20

Figure 3-21. TCAM Resources Page

Configuring Interfaces

The Interfaces pages provide detailed information about each interface on the switch, such as administrative status, input/output packets, packet errors and discards.

Configuring Interface Connections

You can use the *Interface Configuration Page* to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control. Interfaces can also be designated as PVE ports. PVE ports bypass the *Forwarding Database* (FDB), and forward all Unicast, Multicast and Broadcast traffic to an uplink. A single uplink can be defined for a protected port.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Interface** — Indicates the stacking member for which the interface configuration information is displayed.
- **Name** — Displays the port number.
- **Port Type** — Displays the port type. The possible field values are:
  - *Copper* — Indicates the port has a copper port connection.
  - *Fiber* — Indicates the port has a fiber optic port connection.

- **Port Status** — Indicates whether the port is currently operational or non-operational. The possible field values are:
  - *Up* — Indicates the port is currently operating.
  - *Down* — Indicates the port is currently not operating.
- **Port Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. Port speeds can only be configured when auto negotiation is disabled. The possible field values are:
  - *10M* — Indicates the port is currently operating at 10 Mbps.
  - *100M* — Indicates the port is currently operating at 100 Mbps.
  - *1000M* — Indicates the port is currently operating at 1000 Mbps.
- **Duplex Mode** — Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
  - *Full* — The interface supports transmission between the device and its link partner in both directions simultaneously.
  - *Half* — The interface supports transmission between the device and the client in only one direction at a time.
- **Auto Negotiation** — Displays the auto negotiation status on the port. Auto negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode, and flow control abilities to its partner.
- **Advertisement** — Defines the auto negotiation setting the port advertises. The possible field values are:
  - *Max Capability* — Indicates that all port speeds and duplex mode settings are accepted.
  - *10 Half* — Indicates that the port advertises for a 10 Mbps speed port and half duplex mode setting.
  - *10 Full* — Indicates that the port advertises for a 10 Mbps speed port and full duplex mode setting.
  - *100 Half* — Indicates that the port advertises for a 100 Mbps speed port and half duplex mode setting.
  - *100 Full* — Indicates that the port advertises for a 100 Mbps speed port and full duplex mode setting.
  - *1000 Full* — Indicates that the port advertises for a 1000 Mbps speed port and full duplex mode setting
- **Back Pressure** — Displays the back pressure mode on the Port. Back pressure mode is used with half duplex mode to disable ports from receiving messages.
- **Flow Control** — Displays the flow control status on the port. Operates when the port is in full duplex mode.
- **MDI/MDIX** — Displays the MDI/MDIX status on the port. Hubs and switches are deliberately wired opposite 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 matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a

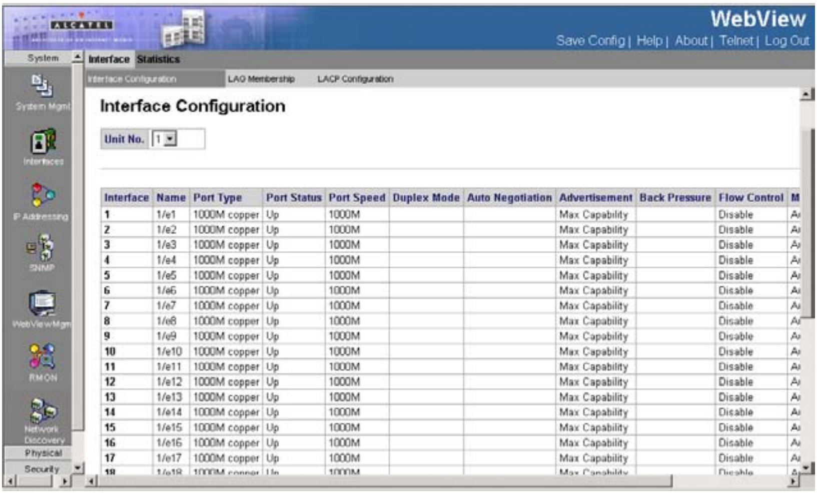
crossover cable is used to ensure that the correct pairs are connected. The possible field values are:

- *Auto* — Use to automatically detect the cable type.
- *MDI (Media Dependent Interface)* — Use for end stations.
- *MDIX (Media Dependent Interface with Crossover)* — Use for hubs and switches.

- **LAG** — Indicates the LAG of which the port is a member.
- **PVE** — Enables a port to be a *Private VLAN Edge* (PVE) port. When a port is defined as PVE, it bypasses the Forwarding Database (FDB), and forwards all Unicast, Multicast and Broadcast traffic to an uplink (except MAC-to-me packets). Uplinks can be a port or GE port. Traffic from the uplink is distributed to all interfaces.

Only one uplink can be defined for a protected port. Private VLANs cannot be configured on ports on which IGMP snooping or Multicast TV VLAN has been configured. An IP address cannot be configured on the VLAN of which a protected port is a member. Only one uplink can be defined for a protected port. Private VLANs cannot be configured on ports on which IGMP snooping or Multicast TV VLAN has been configured. An IP address cannot be configured on the VLAN of which a protected port is a member.

Web – Click System, Interfaces, Interface, Interface Configuration. Modify the required interface settings, and click Apply.



Interface Configuration

Unit No. 1

Interface	Name	Port Type	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Advertisement	Back Pressure	Flow Control	M
1	1/e1	1000M copper	Up	1000M			Max Capability		Disable	A
2	1/e2	1000M copper	Up	1000M			Max Capability		Disable	A
3	1/e3	1000M copper	Up	1000M			Max Capability		Disable	A
4	1/e4	1000M copper	Up	1000M			Max Capability		Disable	A
5	1/e5	1000M copper	Up	1000M			Max Capability		Disable	A
6	1/e6	1000M copper	Up	1000M			Max Capability		Disable	A
7	1/e7	1000M copper	Up	1000M			Max Capability		Disable	A
8	1/e8	1000M copper	Up	1000M			Max Capability		Disable	A
9	1/e9	1000M copper	Up	1000M			Max Capability		Disable	A
10	1/e10	1000M copper	Up	1000M			Max Capability		Disable	A
11	1/e11	1000M copper	Up	1000M			Max Capability		Disable	A
12	1/e12	1000M copper	Up	1000M			Max Capability		Disable	A
13	1/e13	1000M copper	Up	1000M			Max Capability		Disable	A
14	1/e14	1000M copper	Up	1000M			Max Capability		Disable	A
15	1/e15	1000M copper	Up	1000M			Max Capability		Disable	A
16	1/e16	1000M copper	Up	1000M			Max Capability		Disable	A
17	1/e17	1000M copper	Up	1000M			Max Capability		Disable	A
18	1/e18	1000M copper	Up	1000M			Max Capability		Disable	A

Figure 3-22. Interface Configuration Page

CLI – The following is an example of the Port Configuration CLI commands:

```
Console# set interface active ethernet 1/e5                  4-386
Console# configure
Console(config)# interface ethernet 1/e5                     4-376
Console(config-if)# description "RD SW#3"                    4-379
Console(config-if)# speed 100                                4-380
Console(config-if)# duplex full                              4-381
Console(config-if)# negotiation                              4-382
Console(config-if)# flowcontrol on                           4-383
Console(config-if)# mdix auto                                4-383
Console(config-if)# back-pressure                            4-384
```

Creating Trunks (LAGs)

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 up to eight ports per LAG, and eight LAGs per system.

The device supports both static LAGs and Link Aggregation Control Protocol (LACP) LAGs. LACP LAGs negotiate aggregating ports’ links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

- Consider the following when aggregating ports:
- 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 a different 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 eight 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 determine which packets are carried on which aggregated-link member. The hash function statistically load-balances the aggregated link members. The device considers an Aggregated Link as a single logical port.

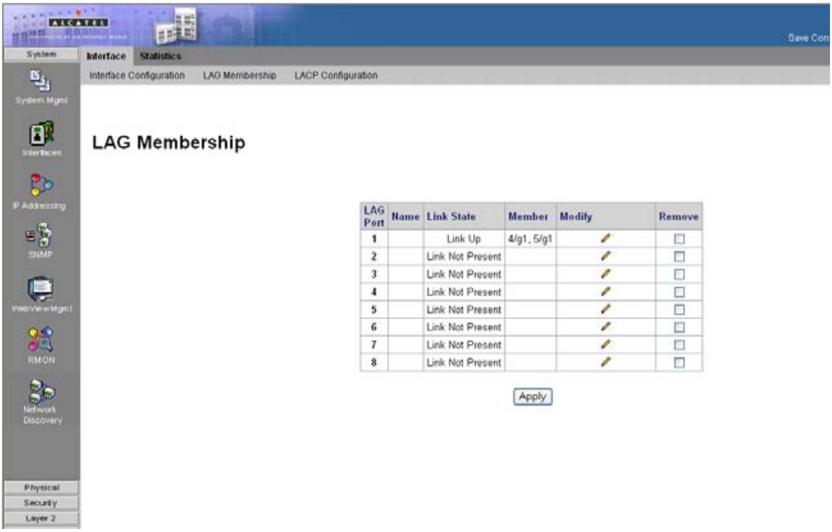
Note: To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

The *LAG Membership Page* contains parameters for defining LAG and LACP ports.

Command Attributes

- **LAG Port** — Displays the LAG number.
- **Name** — Displays the user-defined port name.
- **Link State** — Displays the link operational status.
- **Member** — Displays the ports configured to the LAG.
- **Remove** — Removes the LAG. The possible field values:
  - *Checked* — Removes the selected LAG.
  - *Unchecked* — Maintains the LAGs.

Web – Click System, Interfaces, Interface, LAG Membership. Define the fields and click Apply.



LAG Membership

LAG Port	Name	Link State	Member	Modify	Remove
1		Link Up	4/g1, 5/g1	✎	□
2		Link Not Present		✎	□
3		Link Not Present		✎	□
4		Link Not Present		✎	□
5		Link Not Present		✎	□
6		Link Not Present		✎	□
7		Link Not Present		✎	□
8		Link Not Present		✎	□

Figure 3-23. LAG Membership Page

CLI – The following is an example of the CLI commands for aggregating ports:

```
Console(config-if)# channel-group 1 mode on                          4-456
```

Configuring LACP

Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed, set to full-duplex operations.

LAG ports can contain different media types if the ports are operating at the same speed. Aggregated links can be set up manually or automatically established by enabling Link Aggregation Control Protocol (LACP) on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed.

- Ports assigned to a common port channel must meet the following criteria:
- Ports must have the same LACP System Priority.

Notes: **1.** If the port channel admin key is not set (through the CLI) when a channel group is formed (i.e., it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (lacp admin key).

2. To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.

3. If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.

4. A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.

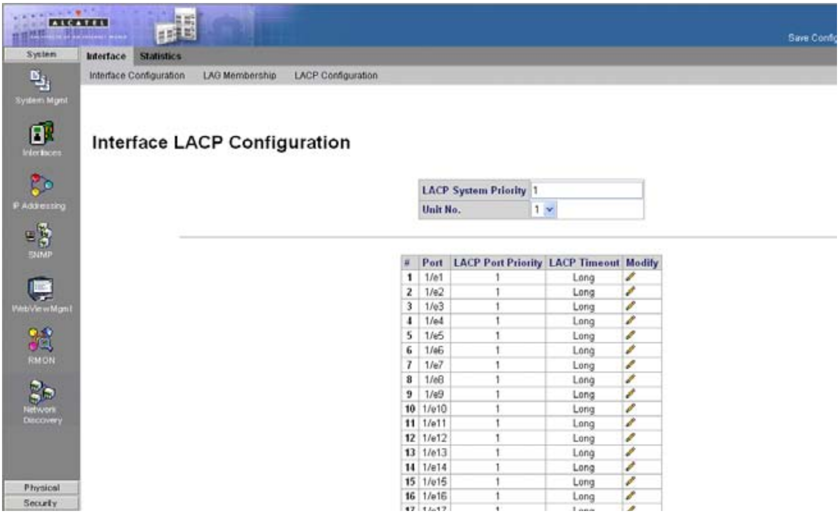
5. All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

The *Interface LACP Configuration Page* contains parameters for defining the LACP ports.

Command Attributes

- **LACP System Priority** — Determines the link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. Ports must be configured with the same system priority to join the same LAG. System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems. The field range is 1 - 65535, and the default is 1.
- **Unit No.** — Displays the stacking member for which the LACP parameters are displayed
- **Port** — Displays the port number to which timeout and priority values are assigned.
- **Port-Priority** — Displays the LACP priority value for the port. The field range is 1-65535.
- **LACP Timeout** — Displays the administrative LACP timeout.

Web – Click System, Interfaces, Interface, LACP Configuration. Define the port LACP parameters and click Apply.



Interface LACP Configuration

LACP System Priority: 1

Unit No.: 1

#	Port	LACP Port Priority	LACP Timeout	Modify
1	1/e1	1	Long	✎
2	1/e2	1	Long	✎
3	1/e3	1	Long	✎
4	1/e4	1	Long	✎
5	1/e5	1	Long	✎
6	1/e6	1	Long	✎
7	1/e7	1	Long	✎
8	1/e8	1	Long	✎
9	1/e9	1	Long	✎
10	1/e10	1	Long	✎
11	1/e11	1	Long	✎
12	1/e12	1	Long	✎
13	1/e13	1	Long	✎
14	1/e14	1	Long	✎
15	1/e15	1	Long	✎
16	1/e16	1	Long	✎
17	1/e17	1	Long	✎

Figure 3-24. Interface LACP Configuration Page

CLI – The following is an example of the LACP interface CLI commands:

```
Console(config)# lacp system-priority 120
4-431
Console(config)# interface ethernet 1/e6
4-376
Console(config-if)# lacp port-priority 247
4-432
Console(config-if)# lacp timeout long
4-432
```

Displaying Port Statistics

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

Interface Statistics

Command Attributes

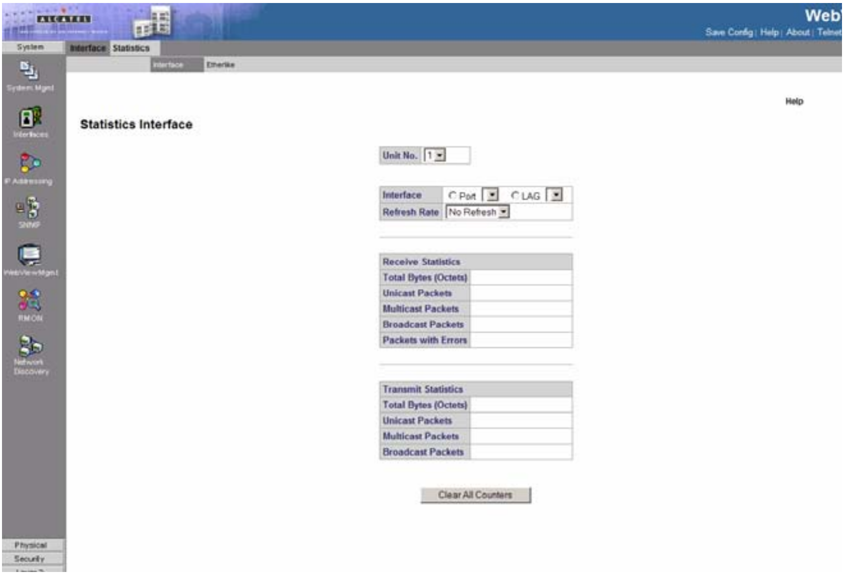
- **Unit No**. — Displays the stacking member for which the Interface Statistics are displayed.
- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
  - *Port* — Defines the specific port for which interface statistics are displayed.
  - *LAG* — Defines the specific LAG for which interface statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - *15 Sec* — Indicates that the Interface statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the Interface statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the Interface statistics are refreshed every 60 seconds.
  - *No Refresh* — Indicates that the Interface statistics are not refreshed.

Receive Statistics

- **Total Bytes (Octets)** — Displays the number of octets received on the selected interface.
- **Unicast Packets** — Displays the number of Unicast packets received on the selected interface.
- **Multicast Packets** — Displays the number of Multicast packets received on the selected interface.
- **Broadcast Packets** — Displays the number of Broadcast packets received on the selected interface.
- **Packets with Errors** — Displays the number of error packets received from the selected interface. Packet with Errors counts all errors without the CRC errors.

Transmit Statistics

- **Total Bytes (Octets)** — Displays the number of octets transmitted from the selected interface.
- **Unicast Packets** — Displays the number of Unicast packets transmitted from the selected interface.
- **Multicast Packets** — Displays the number of Multicast packets transmitted from the selected interface.
- **Broadcast Packets** — Displays the number of Broadcast packets transmitted from the selected interface.



Statistics Interface

Unit No.	1

Interface	○ Port ○ LAG
Refresh Rate	No Refresh

Receive Statistics	
Total Bytes (Octets)	
Unicast Packets	
Multicast Packets	
Broadcast Packets	
Packets with Errors	

Transmit Statistics	
Total Bytes (Octets)	
Unicast Packets	
Multicast Packets	
Broadcast Packets	

Clear All Counters

Figure 3-25. Statistics Interface Page

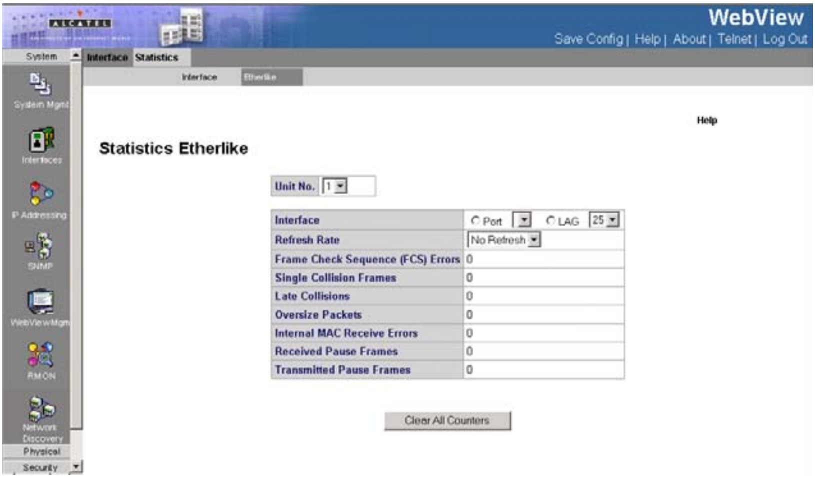
Etherlike Statistics

Command Attributes

- **Unit No**. — Displays the stacking member for which the Etherlike Statistics are displayed.
- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
  - *Port* — Defines the specific port for which Etherlike statistics are displayed.
  - *LAG* — Defines the specific LAG for which Etherlike statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - *15 Sec* — Indicates that the Etherlike statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the Etherlike statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the Etherlike statistics are refreshed every 60 seconds.
  - *No Refresh* — Indicates that the Etherlike statistics are not refreshed.
- **Frame Check Sequence (FCS) Errors** — Displays the number of FCS errors received on the selected interface.
- **Single Collision Frames** — Displays the number of single collision frames received on the selected interface.

- **Late Collisions** — Displays the number of late collision frames received on the selected interface.
- **Oversize Packets** — Displays the number of oversized packet errors on the selected interface.
- **Received Pause Frames** — Displays the number of received paused frames on the selected interface.
- **Transmitted Pause Frames** — Displays the number of paused frames transmitted from the selected interface.

Web – Click System, Interfaces, Statistics, Interface or System, Interfaces, Statistics, Etherlike. Select the required interface, and click Query. Use the Refresh button at the bottom of the page to update the screen.



Statistics Etherlike

Unit No. 1

Interface	○ Port ○ LAG 25
Refresh Rate	No Refresh
Frame Check Sequence (FCS) Errors	0
Single Collision Frames	0
Late Collisions	0
Oversize Packets	0
Internal MAC Receive Errors	0
Received Pause Frames	0
Transmitted Pause Frames	0

Figure 3-26. Statistics Etherlike Page

CLI – The following is an example of the CLI commands displaying Interface statistics:

```
Console> show rmon statistics ethernet 1/e1
4-503

Port: 1/e1

Octets: 878128                Packets: 978

Broadcast: 7                  Multicast: 1

CRC Align Errors: 0           Collisions: 0

Undersize Pkts: 0             Oversize Pkts: 0

Fragments: 0                  Jabbers: 0
```

```
64 Octets: 98                65 to 127 Octets: 0

128 to 255 Octets: 0         256 to 511 Octets: 0

512 to 1023 Octets: 491      1024 to 1518 Octets: 389
```

CLI – The following is an example of the CLI commands displaying Etherlike statistics:

```
Console# show interfaces counters
                                                                    4
                                                                    -
                                                                    3
                                                                    9
                                                                    2



Port     InOctets        InUcastPkts       InMcastPkts      InBcastPkts
----     --------        -----------       -----------      -----------
1/e1     183892          0                 0                0
2/e1     0               0                 0                0
3/e1     123899          0                 0                0

Port     OutOctets       OutUcastPkts      OutMcastPkts     OutBcastPkts
-----    ----------      ------------      ------------     ------------
1/e1     9188            0                 0                0
2/e1     0               0                 0                0
3/e1     8789            0                 0                0

Ch       InOctets        InUcastPkts       InMcastPkts      InBcastPkts
---      --------        ----------        -----------      -----------
1        27889           0                 0                0

Ch       OutOctets       OutUcastPkts      OutMcastPkts     OutBcastPkts
---      ---------       ------------      ------------     ------------
1        23739           0                 0                0
```

Configuring IP Information

This section describes how to configure an initial IP interface for management access over the network. The IP address for this switch is unassigned by default. To manually configure an address, you need to change the switch IP address and netmask to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

You can manually configure a specific IP address, or direct the device to obtain an address from a DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. The system supports up-to 5 IP addresses per device. Anything outside this format will not be accepted by the CLI program.

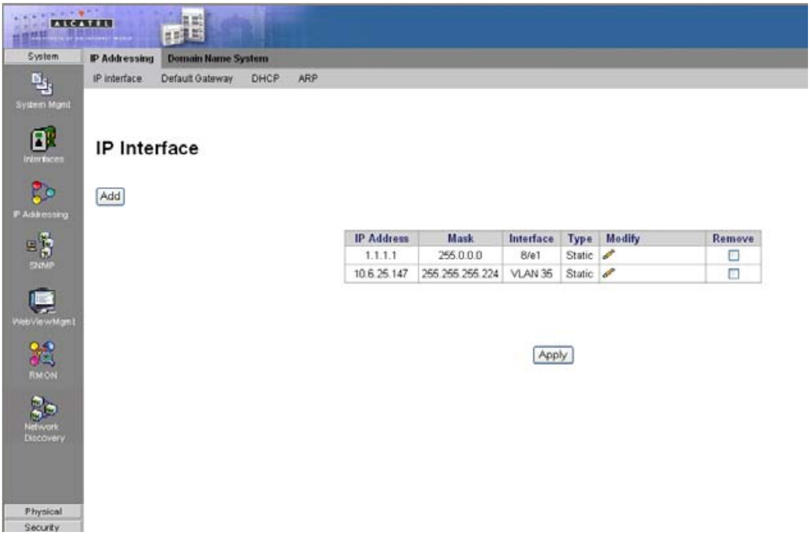
Defining IP Addresses

The *IP Interface Page* contains fields for assigning IP parameters to interfaces, and for assigning gateway devices. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces.

Command Attributes

- **IP Address** — Displays the currently configured IP address.
- **Mask** — Displays the currently configured IP address mask.
- **Interface** — Displays the interface used to manage the device.
- **Remove** — Removes the selected IP address from the interface. The possible field values are:
  - *Checked* — Removes the IP address from the interface.
  - *Unchecked* — Maintains the IP address assigned to the Interface.

Web — Click System, IP Addressing, IP Addressing, IP Interface, define the fields, and specify a Primary interface, click Apply.



IP Interface

IP Address	Mask	Interface	Type	Modify	Remove
1.1.1.1	255.0.0.0	8/e1	Static	✎	□
10.6.25.147	255.255.255.224	VLAN 35	Static	✎	□

Figure 3-27. IP Interface Page

CLI – The following is an example of the CLI commands for defining an IP interface:

```
Console(config)# interface vlan 1
4-664
Console(config-if)# ip address 131.108.1.27 255.255.255.0
4-418
```

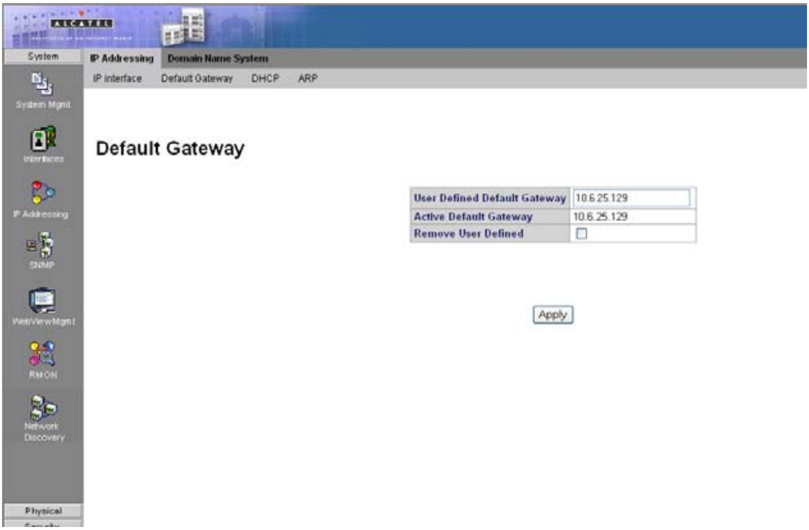
Defining Default Gateways

Packets are forwarded to the default IP when frames are sent to a remote network via the default gateway. The configured IP address must belong to the same subnet as one of the IP interfaces. The *Default Gateway Page* contains parameters for defining default gateways.

Command Attributes

- **User Defined Default Gateway** — Defines the default gateway IP address.
- **Active Default Gateway** — Indicates if the default gateway is active.
- **Remove** — Removes the default gateway. The possible field values are:
  - *Checked* — Removes the selected default gateway.
  - *Unchecked* — Maintains the default gateway.

Web — Click System, IP Addressing, Default Gateway, define the fields, and specify a Primary interface, click Apply.



Default Gateway

User Defined Default Gateway	10.6.25.129
Active Default Gateway	10.6.25.129
Remove User Defined	□

Figure 3-28. Default Gateway Page

CLI – The following is an example of the CLI commands for defining a default gateway:

```
Console(config)# ip default-gateway 192.168.1.1
4-420
```

Configuring DHCP

The *Dynamic Host Configuration Protocol* (DHCP) assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

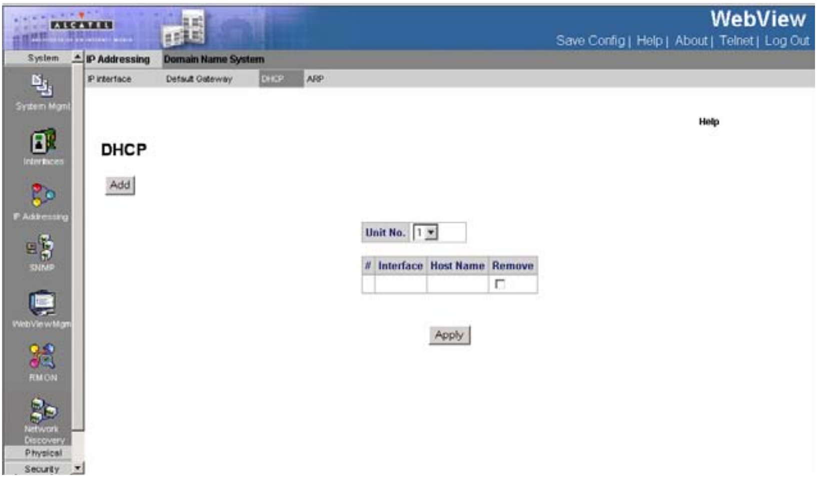
DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. If DHCP is enabled, the IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address.

If your network provides DHCP services, you can configure the switch to be dynamically configured by these services. The *DHCP Page* contains parameters for assigning IP addresses to devices.

Command Attributes

- **Unit No.** — Displays the stacking member for which the DHCP is assigned.
- **Interface** — Displays the DHCP interface address which is connected to the device.
- **Host Name** — Displays the system name.

- **Remove** — Removes DHCP interfaces. The possible field values are:
  - *Checked* — Removes the selected DHCP interface.
  - *Unchecked* — Maintains the DHCP interfaces.
- **Web** — Click System, IP Addressing, DHCP, define the fields, specify a primary interface, and click Apply.



Unit No. 1

#	Interface	Host Name	Remove
			□

Figure 3-29. DHCP Page

CLI – The following is an example of the DHCP CLI commands:

```
Console(config)# interface ethernet 1/e16
4-376
Console(config-if)# ip address dhcp
4-419
```

Configuring ARP

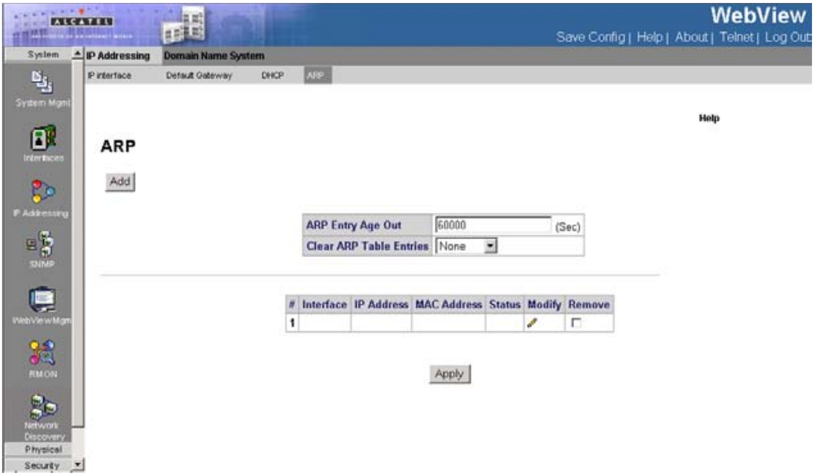
The *Address Resolution Protocol* (ARP) converts IP addresses into physical addresses, and maps the IP address to a MAC address. ARP allows a host to communicate with other hosts only when the IP address of its neighbors is known. The *ARP Page* contains parameters for defining ARP.

Command Attributes

- **ARP Entry Age Out** — Specifies the amount of time (in seconds) that passes between *ARP Table* entry requests. Following the *ARP Entry Age* period, the entry is deleted from the table. The range is *1 - 40000000*. The default value is *60000 seconds*.
- **Clear ARP Table Entries** — Specifies the types of ARP entries that are cleared. The possible values are:
  - *None* — Does not clear ARP entries.

  - *All* — Clears all ARP entries.
  - *Dynamic* — Clears only dynamic ARP entries.
  - *Static* — Clears only static ARP entries.
- **Interface** — Displays the interface type for which ARP parameters are displayed. The possible field values are:
  - *Port* — The port for which ARP parameters are defined.
  - *LAG* — The LAG for which ARP parameters are defined.
  - VLAN — The VLAN for which ARP parameters are defined.
- **IP Address** — Indicates the station IP address, which is associated with the MAC address filled in below.
- **MAC Address** — Displays the station MAC address, which is associated in the ARP table with the IP address.
- **Status** — Displays the ARP table entry type. Possible field values are:
  - *Dynamic* — The ARP entry is learned dynamically.
  - *Static* — The ARP entry is a static entry.
- **Remove** — Removes a specific ARP entry. The possible field values are:
  - *Checked* — Removes the selected ARP entries.
  - *Unchecked* — Maintains the current ARP entries.

Web — Click System, IP Addressing, IP Addressing, ARP, define the fields, and specify a primary interface. Click Apply.



ARP

Add

ARP Entry Age Out	60000 (Sec)
Clear ARP Table Entries	None

#	Interface	IP Address	MAC Address	Status	Modify	Remove
1					✎	□

Apply

Figure 3-30. ARP Page

CLI – The following is an example of the ARP CLI commands:

```
Console(config)# arp 198.133.219.232 00:00:0c:40:0f:bc ethernet 1/e6

4-422
```

Configuring Domain Name Service

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 databases of domain names and their corresponding IP addresses.

When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

When configuring the DNS parameters:

- Enable DNS service on this switch, first configure one or more name servers, and then enable domain lookup status.
- To append domain names to incomplete host names received from a DNS client (i.e., not formatted with dotted notation), you can specify a default domain name or a list of domain names to be tried in sequential order.
- If there is no domain list, the default domain name is used. If there is a domain list, the default domain name is not used.
- When an incomplete host name is received by the DNS server on this switch and a domain name list has been specified, the switch works through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- Note that if all name servers are deleted, DNS will automatically be disabled.

Configuring General DNS Server Parameters

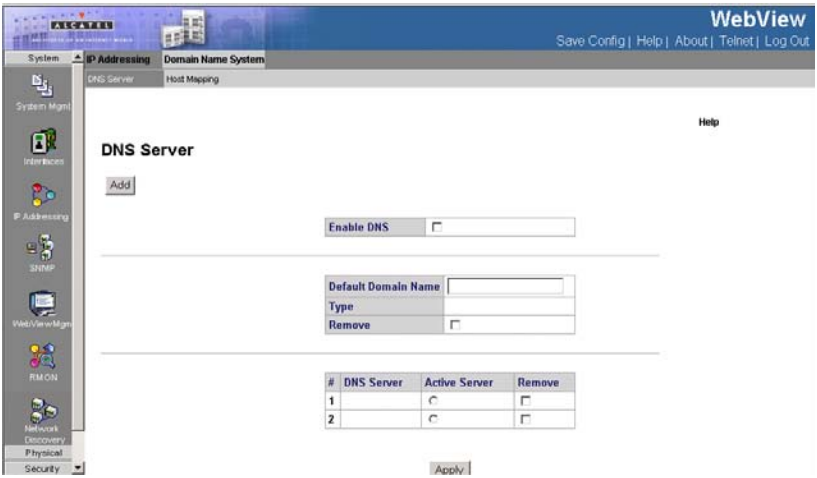
The *DNS Server Page* contains fields for enabling and activating specific DNS servers.

Command Attributes

- **Enable DNS** — Enables translating the DNS names into IP addresses. The possible field values are:
  - *Checked* — Translates the domains into IP addresses.
  - *Unchecked* — Disables translating domains into IP addresses.
- **Default Domain Name** — Specifies the user-defined DNS server name.
- **Type** — Displays the Default Domain Name type. The possible field values are:
  - *Dynamic* — Indicates that the Default Domain Name is dynamically created.
  - *Static* — Indicates that the Default Domain Name is a static IP address.
- **Remove** — Removes DNS servers. The possible field values are:
  - *Checked* — Removes the selected DNS server
  - *Unchecked* — Maintains the current DNS server list.
- **DNS Server** — Displays the DNS server IP address. DNS servers are added in the *Add DNS Server Page*.
- **Active Server**— Specifies the DNS server that is currently active.

Note: All DNS servers can be selected by clicking Select All in DNS Server Table. Do not include the initial dot that separates the host name from the domain name.

Web – Select System, IP Addressing, Domain Name System, DNS Server. Set the default domain name or DNS server list, define the fields and click Apply.



DNS Server

Enable DNS	□

Default Domain Name	
Type	
Remove	□

#	DNS Server	Active Server	Remove
1		○	□
2		○	□

Figure 3-31. DNS Server Page

CLI - The following is an example of the DNS server commands:

```
Console(config)# ip name-server 176.16.1.18                     4-426
```

Configuring Static DNS Host to Address Entries

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

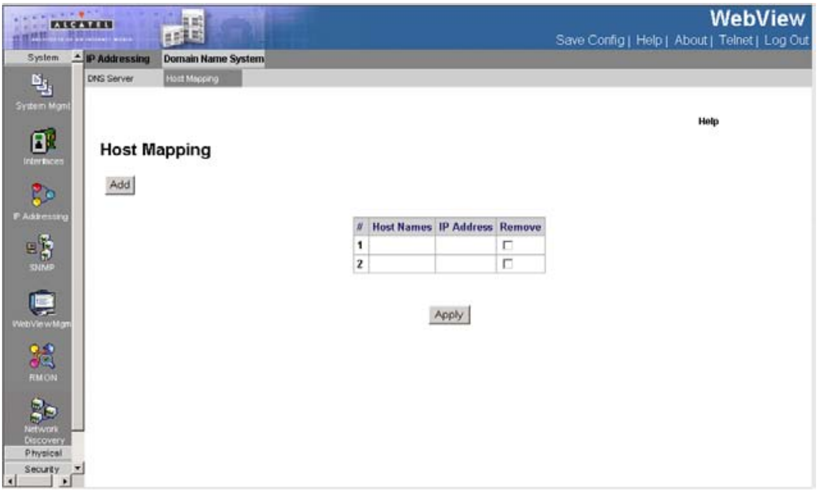
- Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.
- Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name in the static table or via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

The *DNS Host Mapping Page* contains parameters for defining static entries in the DNS table.

Command Attributes

- **Host Names** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- **IP Address** — Displays the DNS host IP address.
- **Remove** — Removes default domain names. The possible field values are:
  - *Checked* — Removes the selected DNS host.
  - *Unchecked* — Maintains the current DNS host mapping list.

Web – Select System, IP Addressing, Domain Name System, Host Mapping. Define the fields and click Apply.



Host Mapping

#	Host Names	IP Address	Remove
1			□
2			□

Figure 3-32. DNS Host Mapping Page

CLI -The following in an example of the DNS Host Mapping Commands:

```
Console(config)# ip host accounting.abc.com 176.10.23.1          4-427
```

Configuring SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as HP OpenView. Access to the onboard agent using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it’s own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to “groups” that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as “views.” The switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

Table 3-4. SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Security
v1	noAuthNoPriv	DefaultROGroup	defaultview	none	Community string only
v1	noAuthNoPriv	DefaultRWGroup	defaultview	defaultview	Community string only
v1	noAuthNoPriv	user defined	user defined	user defined	Community string only
v2c	noAuthNoPriv	DefaultROGroup	defaultview	none	Community string only
v2c	noAuthNoPriv	DefaultRWGroup	defaultview	defaultview	Community string only
v2c	noAuthNoPriv	user defined	user defined	user defined	Community string only
v3	noAuthNoPriv	user defined	user defined	user defined	A user name match only
v3	AuthNoPriv	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

The predefined default groups and view can be deleted from the system.

Enabling SNMP

The *Engine ID Page* permits the enabling of both SNMP and Authentication notifications.

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

A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

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

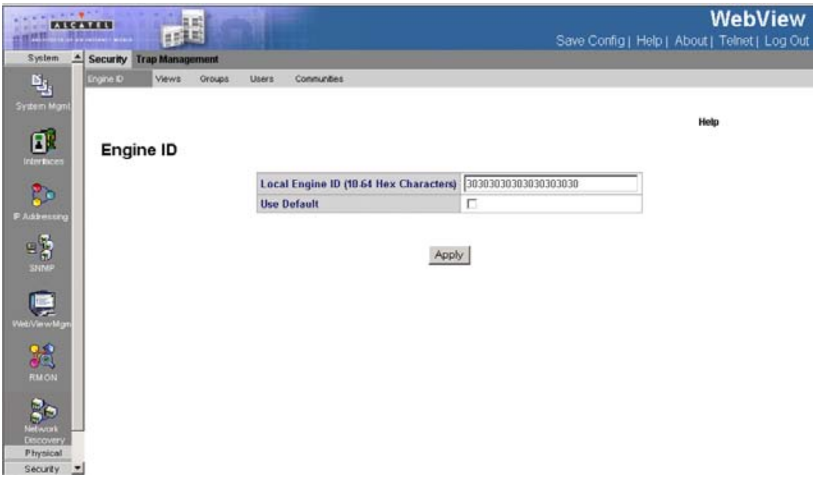
SNMP is enabled by default.

Command Attributes

- **Local Engine ID (10-64 Hex Characters)** — Displays 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. Select a default Engine ID that is comprised of an Enterprise number and the default MAC address.
- **Use Default** — Uses 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.
  - *Fifth octet* — Set to 3 to indicate the MAC address that follows.

- *Last 6 octets* — MAC address of the device.

Web — Click System, SNMP, Security, Engine ID. Define the fields and click Apply.



Engine ID

Local Engine ID (10-64 Hex Characters)	30303030303030303030
Use Default	□

Figure 3-33. Engine ID Page

CLI – The following example enables SNMPv3 on the switch:

```
Console(config)# snmp server engineid local default
4-360
```

Defining SNMP Users

The *SNMP Users Page* enables assigning system users to SNMP groups, as well as defining the user authentication method. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group.

Command Attributes

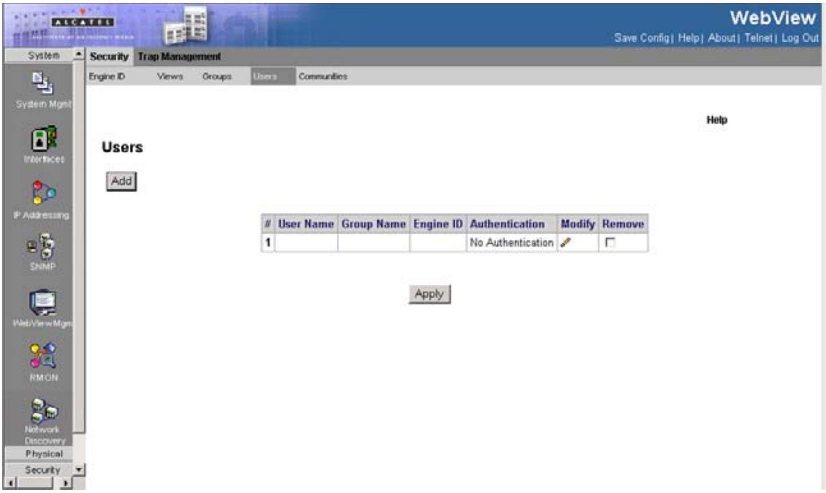
- **User Name** — Contains a list of user-defined user names. The field range is up to 30 alphanumeric characters.
- **Group Name** — Contains a list of user-defined SNMP groups. SNMP groups are defined in the *SNMP Group Profile Page*.
- **Engine ID** — Displays either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 user database.
  - *Local* — Indicates that the user is connected to a local SNMP entity.
  - *Remote* — Indicates that the user is connected to a remote SNMP entity. If the Engine ID is defined, remote devices receive inform messages.

- **Authentication** — Displays the method used to authenticate users. The possible field values are:
  - *MD5 Key* — Users are authenticated using the HMAC-MD5 algorithm.
  - *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.
  - *MD5 Password* — The HMAC-MD5-96 password is used for authentication. The user should enter a password.
  - *SHA Password* — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.
  - *No Authentication* — No user authentication is used.
- **Remove** — Removes users from a specified group. The possible field values are:
  - *Checked* — Removes the selected user.
  - *Unchecked* — Maintains the list of users.
- **Authentication Method** — Defines the SNMP Authentication Method.

***ADD* Command Attributes**

- **Password** — Defines the password for the group member.
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon.
- **Privacy Key** — Defines the privacy key (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

Web – Click System, SNMP, Security, Users. Click Add to configure a user name. In the New User page, define a name and assign it to a group, then click Apply to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete. To change the assigned group of a user, click Change Group in the Actions column of the users table and select the new group.



#	User Name	Group Name	Engine ID	Authentication	Modify	Remove
1				No Authentication	✎	□

Figure 3-34. SNMP Users Page

CLI – The following is an example of the SNMP User CLI commands:

```
Console(config)# snmp-server user John user-group
4-360
```

Defining SNMP Group Profiles

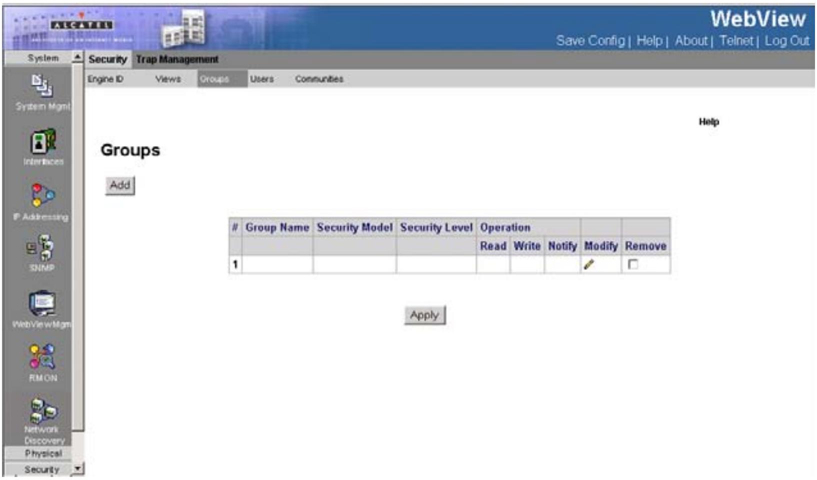
The *SNMP Groups Page* provides information for creating SNMP groups, and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific device features, or feature aspects.

Command Attributes

- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2c* — SNMPv2c is defined for the group.
  - *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:
  - *No Authentication* — Indicates that neither the Authentication nor the Privacy security levels are assigned to the group.
  - *Authentication* — Authenticates SNMP messages, and ensures that the SNMP message’s origin is authenticated.

  - *Privacy* — Encrypts SNMP messages.
- **Operation** — Defines the group access rights. The possible field values are:
  - *Read* — Management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.
  - *Write* — Management access is read-write and changes can be made to the assigned SNMP view.
  - *Notify* — Sends traps for the assigned SNMP view.
- **Remove** — Removes SNMP groups. The possible field values are:
  - *Checked* — Removes the selected SNMP group.
  - *Unchecked* — Maintains the SNMP groups.

Web – Click System, SNMP, Security, Groups. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete. To change the assigned group of a user, click Change Group in the Actions column of the users table and select the new group.



Groups

#	Group Name	Security Model	Security Level	Operation			Modify	Remove
				Read	Write	Notify		
1							✎	□

Figure 3-35. SNMP Groups Page

CLI – The following is an example of the SNMP CLI commands:

```
Console(config)# snmp-server group user-group v3 priv read
user-view
4-360
```

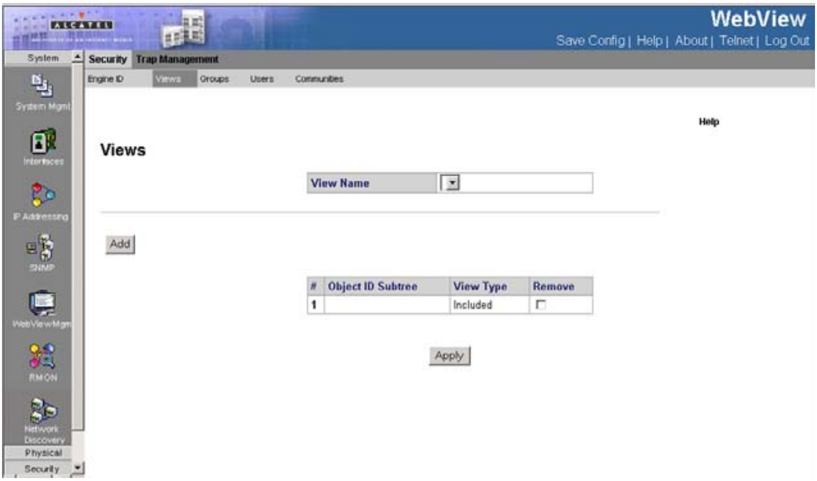
Defining SNMP Views

SNMP views provide or block access to device features or portions of features. For example, a view can be defined which provides that SNMP group A has *Read Only* (R/O) access to Multicast groups, while SNMP group B has *Read-Write* (R/W) access to Multicast groups. Feature access is granted via the MIB name or MIB Object ID. The *SNMP Views Page* contains fields for assigning parameters that provide or block access to device features.

Command Attributes

- **View Name** — Displays the user-defined views. The view name can contain a maximum of 30 alphanumeric characters.
- **Object ID Subtree** — Displays the device feature OID included in or excluded from the selected SNMP view.
- **View Type** — Indicates whether the defined OID branch will be included in or excluded from the selected SNMP view.
- **Remove** — Deletes the currently selected view. The possible field values are:
  - *Checked* — Removes the selected view.
  - *Unchecked* — Maintains the list of views.

Web – Click System, SNMP, Security, Views. Click New to configure a new view. In the New View page, define a name and specify OID subtrees in the switch MIB to be included or excluded in the view. Click Back to save the new view and return to the SNMPv3 Views list. For a specific view, click on View OID Subtrees to display the current configuration, or click on Edit OID Subtrees to make changes to the view settings. To delete a view, check the box next to the view name, then click Delete.



Views

View Name

#	Object ID Subtree	View Type	Remove
1		Included	□

Figure 3-36. SNMP Views Page

CLI – The following in an example of the SNMP View CLI commands:

```
Console(config)# snmp-server filter filter-name system included
Console(config)# snmp-server filter filter-name system.7 excluded
Console(config)# snmp-server filter filter-name ifEntry.*.1 included
4-360
```

Defining SNMP Communities

Access rights are managed by defining communities in the *SNMP Communities Page*. You may configure up to five community strings authorized for management access using SNMP v1 and v2c. For security reasons, you should consider removing the default strings. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c.

Basic Table Command Attributes

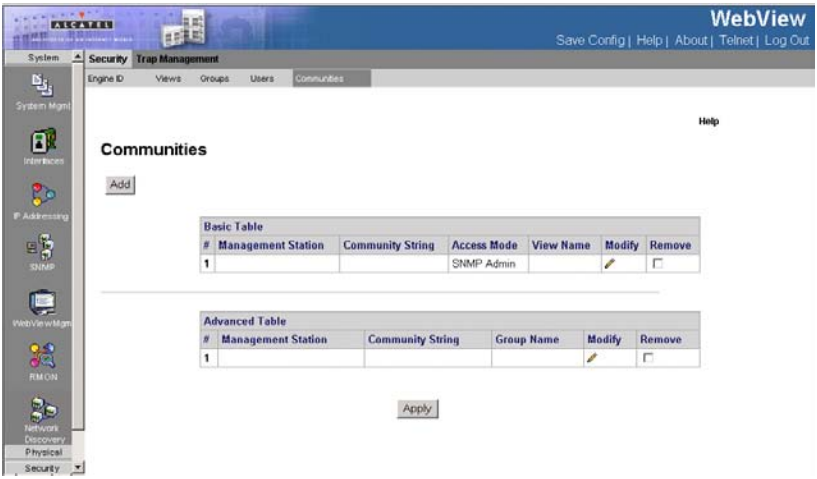
- **Management Station** — Displays the management station IP address for which the basic SNMP community is defined.
- **Community String** — Defines the password used to authenticate the management station to the device.
- **Access Mode** — Defines the access rights of the community. The possible field values 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** — Contains a list of user-defined SNMP views
- **Remove** — Removes a community. The possible field values are:
  - *Checked* — Removes the selected SNMP community.
  - *Unchecked* — Maintains the SNMP communities.

Advanced Table Command Attributes

- **Management Station** — Displays the management station IP address for which the advanced SNMP community is defined.
- **Community String** — Defines the password used to authenticate the management station to the device.
- **Group Name** — Defines advanced SNMP community group names.
- **Remove** — Removes a community. The possible field values are:
  - *Checked* — Removes the selected SNMP communities.
  - *Unchecked* — Maintains the SNMP communities.

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

Add.



Basic Table

#	Management Station	Community String	Access Mode	View Name	Modify	Remove
1			SNMP Admin		✎	□

Advanced Table

#	Management Station	Community String	Group Name	Modify	Remove
1				✎	□

Figure 3-37. SNMP Communities Page

CLI – The following is an example of the SNMP Communities CLI commands:

```
Console(config)# snmp-server community public su 192.168.1.20
4-360
```

Defining SNMP Notification Recipients

The *SNMP Trap Station Management Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

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

Command Attributes

SNMPv1,2 Notification Recipient

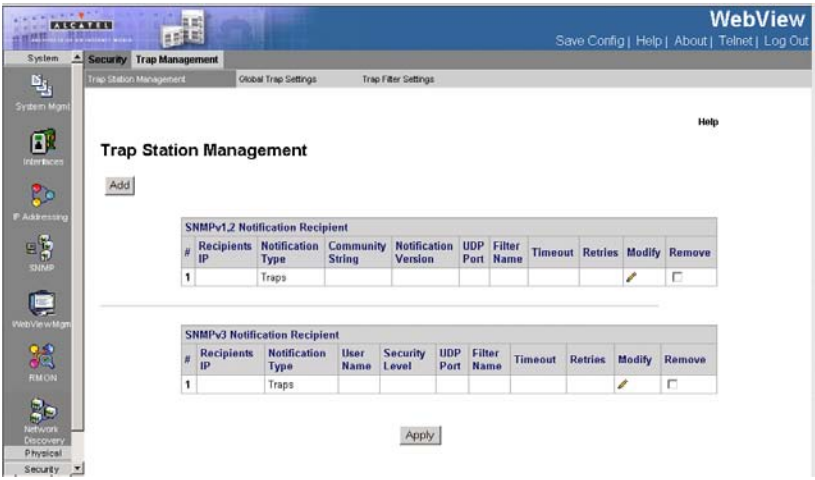
- **Recipients IP** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the notification sent. The possible field values are:
  - *Trap* — Indicates traps are sent.
  - *Inform* — Indicates informs are sent.
- **Community String** — Displays the community string of the trap manager.
- **Notification Version** — Displays the trap type. The possible field values are:
  - *SNMP V1* — Indicates that SNMP Version 1 traps are sent.
  - *SNMP V2c* — Indicates that SNMP Version 2 traps are sent.
- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (in seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.
- **Remove** — Deletes the currently selected recipient. The possible field values are:
  - *Checked* — Removes the selected recipient from the list of recipients.
  - *Unchecked* — Maintains the list of recipients.

SNMPv3 Notification Recipient

- **Recipient IP** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the type of notification sent. The possible field values are:
  - *Trap* — Indicates that traps are sent.
  - *Inform* — Indicates that informs are sent.
- **User Name** — Displays the user to which SNMP notifications are sent.
- **Security Level** — Displays the means by which the packet is authenticated. The possible field values are:
  - *No Authentication* — Indicates that the packet is neither authenticated nor encrypted.
  - *Authentication* — Indicates that the packet is authenticated.
  - *Privacy* — Encrypts SNMP messages.
- **UDP Port** — The UDP port used to send notifications. The field range is 1-65535. The default is 162.
- **Filter Name** — Includes or excludes SNMP filters.
- **Timeout** — The amount of time (seconds) the device waits before resending informs. The field range is 1-300. The default is 10 seconds.
- **Retries** — The amount of times the device resends an inform request. The field range is 1-255. The default is 3.

- **Remove** — Deletes the currently selected recipient. The possible field values are:
  - *Checked* — Removes the selected recipient from the list of recipients.
  - *Unchecked* — Maintains the list of recipients.

Web – Click SNMP, Trap Management, Trap Station Management. Define the fields and click Add.



Trap Station Management

SNMPv1,2 Notification Recipient

#	Recipients IP	Notification Type	Community String	Notification Version	UDP Port	Filter Name	Timeout	Retries	Modify	Remove
1		Traps							✎	□

SNMPv3 Notification Recipient

#	Recipients IP	Notification Type	User Name	Security Level	UDP Port	Filter Name	Timeout	Retries	Modify	Remove
1		Traps							✎	□

Figure 3-38. SNMP Trap Station Management Page

CLI – The following is an example of the SNMP Recipient commands:

```
Console(config)# snmp-server host 10.1.1.1 management 2
```

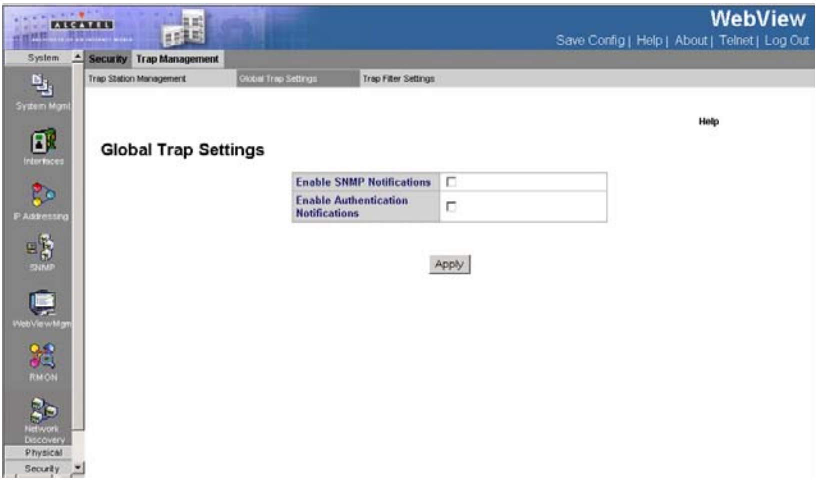
Defining SNMP Notification Global Parameters

The *SNMP Global Trap Settings Page* contains parameters for enables you to define SNMP notification parameters.

Command Attributes

- **Enable SNMP Notifications** — Specifies whether the device can send SNMP notifications. The possible field values are:
  - *Checked* — Enables SNMP notifications.
  - *Unchecked* — Disables SNMP notifications.
- **Enable Authentication Notifications** — Specifies whether SNMP authentication failure notification is enabled on the device. The possible field values are:
  - *Checked* — Enables the device to send authentication failure notifications.
  - *Unchecked* — Disables the device from sending authentication failure notifications.

Web - Click System, SNMP, Trap Management, Global Trap Settings. Define the fields and click Apply.



Global Trap Settings

Enable SNMP Notifications	□
Enable Authentication Notifications	□

Figure 3-39. SNMP Global Trap Settings Page

CLI – The following is an example of the SNMP commands for enabling traps:

```
Console(config)# snmp server enable traps
4-360
```

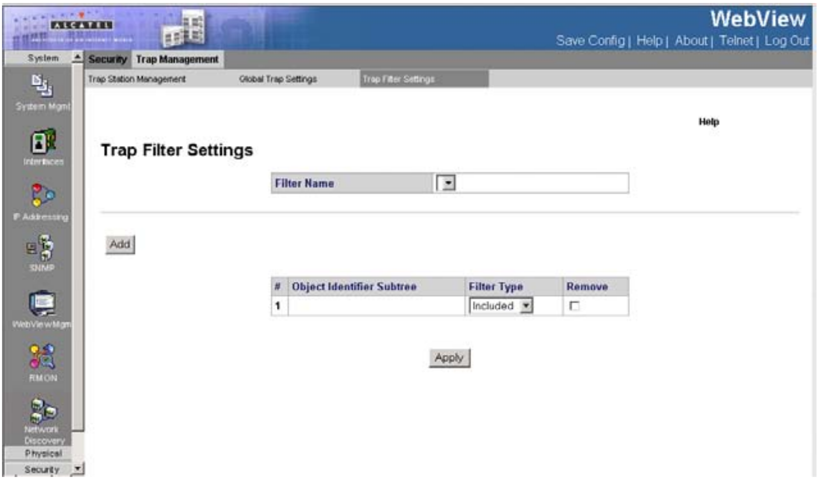
Defining SNMP Notification Filters

The *Trap Filter Settings Page* permits filtering traps based on OIDs. Each OID is linked to a device feature or a portion of a feature. The *Trap Filter Settings Page* also allows network managers to filter notifications.

Command Attributes

- **Filter Name** — Contains a list of user-defined notification filters.
- **Object ID Subtree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. OIDs are selected from either the *Select from* field or the *Object ID* field.
- **Filter Type** — Indicates whether to send traps or informs relating to the selected OID.
  - *Excluded* — Does not send traps or informs.
  - *Included* — Sends traps or informs.
- **Remove** — Deletes filters.
  - *Checked* — Deletes the selected filter.
  - *Unchecked* — Maintains the list of filters.

Web – Click System, SNMP, Trap Management, Trap Filter Settings. Define the fields and click Apply.



Trap Filter Settings

Filter Name

#	Object Identifier Subtree	Filter Type	Remove
1		Included	☐

Figure 3-40. Trap Filter Settings Page

CLI – The following is an example of the Trap Management CLI commands:

```
Console(config)# snmp-server filter filter-name system included
Console(config)# snmp-server filter filter-name system.7 excluded
Console(config)# snmp-server filter filter-name ifEntry.*.1 included
4-360
```

Configuring User Authentication

You can restrict management access to this switch using the following options:

- **Passwords** – Configure the password for the current user.
- **Authentication Settings** – Use remote authentication to configure access rights.
- **HTTPS Settings** – Provide a secure web connection.
- **SSH Settings** – Provide a secure shell (for secure Telnet access).
- **Port Security** – Configure secure addresses for individual ports.
- **802.1x** – Use IEEE 802.1x port authentication to control access to specific ports.
- **IP Filter** – Filters management access to the web, SNMP or Telnet interface.

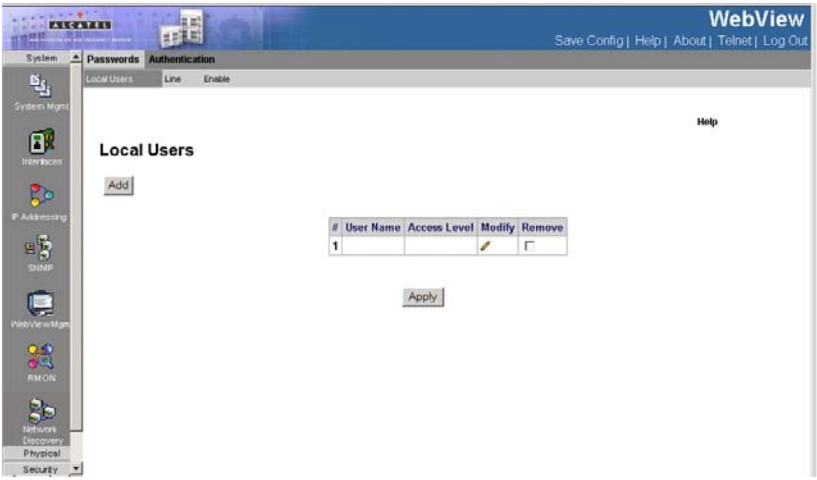
Defining Local Users Passwords

Network administrators can define users, passwords, and access levels for users using the *Local Users Page*.

Command Attributes

- **User Name** — Displays the user name.
- **Access Level** — Displays the user access level. The lowest user access level is 1 and the highest is 15. Users with access level 15 are Privileged Users, and only they can access and use the EWS.
- **Remove** — Removes the user from the *User Name* list. The possible field values are:
  - *Checked* — Removes the selected local user.
  - *Unchecked* — Maintains the local users.
- **Password** — Defines the local user password. Local user passwords can contain up to 159 characters.
- **Confirm Password** — Verifies the password.

Web – Click System, WebViewMgmt, Passwords, Local Users, define the fields, and click Apply.



Local Users

#	User Name	Access Level	Modify	Remove
1			✎	□

Figure 3-41. Local Users Page

CLI – The following is an example of the CLI commands used for configuring Local Users Passwords:

```
Console(config)# username bob password lee level 15
4-297
```

Defining Line Passwords

Network administrators can define line passwords in the *Line Page*. After the line password is defined, a management method is assigned to the password. The device can be accessed using the following methods:

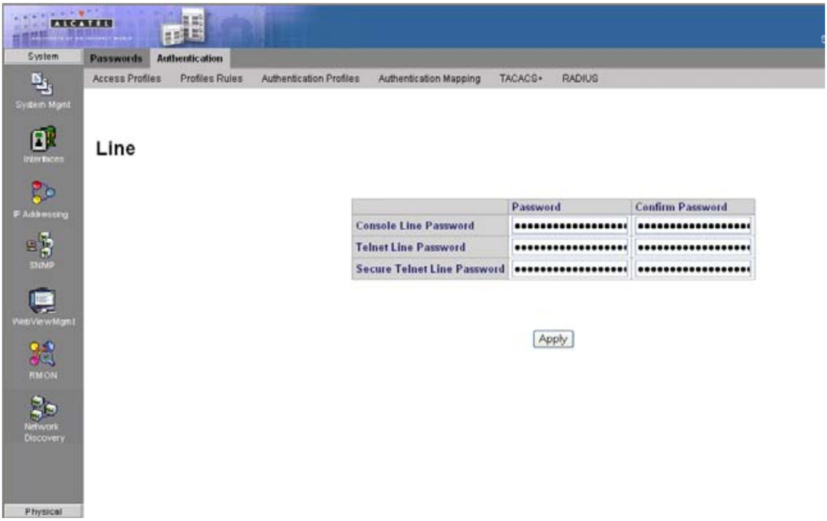
- Console
- Telnet
- Secure Telnet

Command Attributes

To define line passwords:

- **Console Line Password** — Defines the line password for accessing the device via a Console session. Passwords can contain a maximum of 159 characters.
- **Telnet Line Password** — Defines the line password for accessing the device via a Telnet session. Passwords can contain a maximum of 159 characters.
- **Secure Telnet Line Password** — Defines the line password for accessing the device via a secure Telnet session. Passwords can contain a maximum of 159 characters.
- **Confirm Password** — Confirms the new line password. The password appears in the ***** format.

Web – Click System, WebViewMgmt, Passwords, Line, define the fields, and click Apply.



Line

	Password	Confirm Password
Console Line Password	••••••••••••••••••	••••••••••••••••••
Telnet Line Password	••••••••••••••••••	••••••••••••••••••
Secure Telnet Line Password	••••••••••••••••••	••••••••••••••••••

Figure 3-42. Line Page

CLI – The following is an example of the CLI commands used for configuring Line Passwords.

```
Console(config)# line console
4-437
Console(config-line)# password secret
4-296
```

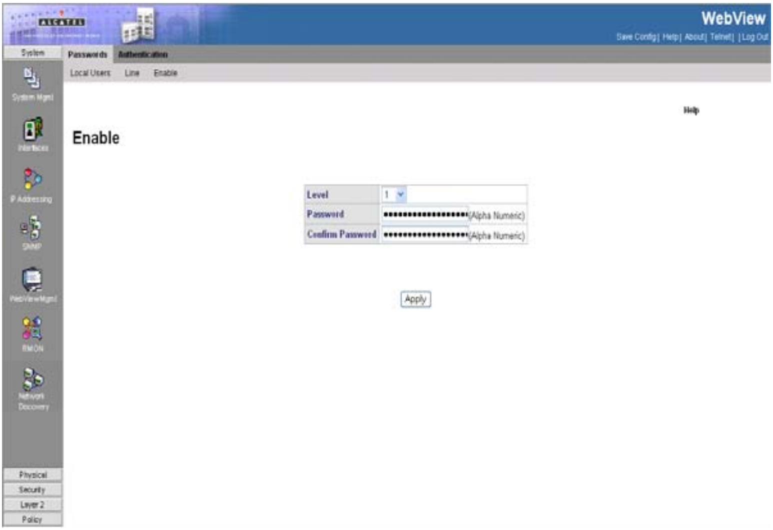
Defining Enable Passwords

The *Enable Page* sets a local password for a particular access level.

Command Attributes

- **Select Enable Access Level** — Defines the access level associated with the enable password. Possible field values are 1-15.
- **Password** — Defines the enable password.
- **Confirm Password** — Confirms the new enable password. The password appears in the `*****` format.

Web – Click System, WebViewMgmt, Passwords, Enable, define the fields, and click Apply.



Level: 1
Password: •••••••••••••••••• (Alpha Numeric)
Confirm Password: •••••••••••••••••• (Alpha Numeric)

Figure 3-43. Enable Page

CLI – The following is an example of the CLI commands used for configuring Enable Passwords:

```
Console(config)# enable password level 15 secret
4-296
```

Configuring Authentication Methods

This section provides information for configuring device authentication methods, and includes the following topics:

- Defining Access Profiles
- Defining Profile Rules
- Defining Authentication Profiles
- Mapping Authentication Methods
- Defining TACACS+ Methods
- Defining RADIUS Settings

Defining Access Profiles

Access profiles are profiles and rules for accessing the device. Access to management functions can be limited to user groups. User groups are defined for interfaces according to IP addresses or IP subnets. Access profiles contain management methods for accessing and managing the device. The device management methods include:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP

Management access to different management methods may differ between user groups. For example, User Group 1 can access the switch module only via an HTTPS session, while User Group 2 can access the switch module via both HTTPS and Telnet sessions. The *Access Profiles Page* contains the currently configured access profiles and their activity status.

Assigning an access profile to an interface denies access via other interfaces. If an access profile is assigned to any interface, the device can be accessed by all interfaces.

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS- aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

For example, if you select (1) RADIUS, (2) TACACS+ and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Ensure the following when configuring Authentication Profiles:

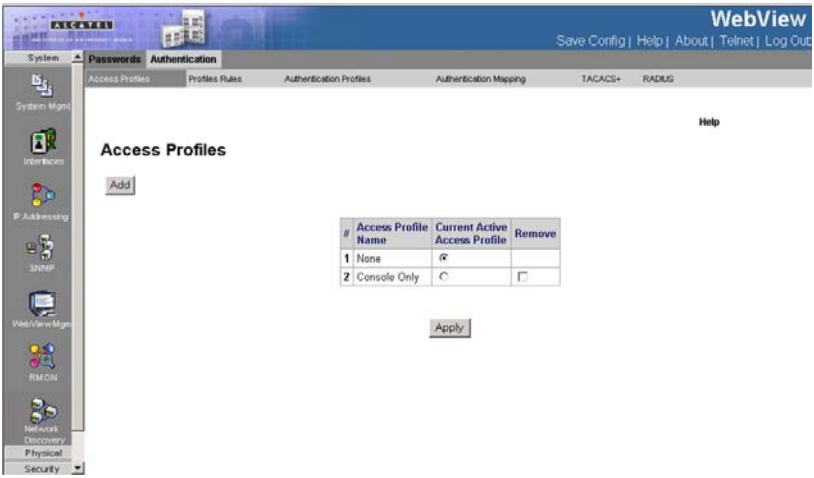
- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.

Command Attributes

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Current Active Access Profile** — Defines the access profile currently active.
- **Remove** — Removes the selected access profile. The possible field values are:
  - *Checked* — Removes the selected access profile.

  - *Unchecked* — Maintains the access profiles.
- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the *Profiles Rules Page*.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
  - *Port* — Specifies the port on which the access profile is defined.
  - *LAG* — Specifies the LAG on which the access profile is defined.
  - *VLAN* — Specifies the VLAN on which the access profile is defined.
- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork.
- **Network Mask** — The IP subnetwork mask.
- **Prefix Length** — The number of bits that comprises the source IP address prefix, or the network mask of the source IP address.
- **Action** —Defines the action attached to the rule. The possible field values are:
  - *Permit* — Permits access to the device.
  - *Deny* — Denies access to the device. This is the default.

Web – Click System, WebViewMgmt, Authentication, Access Profiles, define the fields, and click Apply.



Access Profiles

#	Access Profile Name	Current Active Access Profile	Remove
1	None	●	
2	Console Only	○	□

Figure 3-44. Access Profiles Page

CLI – The following is an example of the CLI commands used for configuring Access Profiles:

```
Console(config)# ip https port 100
4-694
Console(config)# ip http port 100
4-692
```

Defining Profile Rules

Access profiles can contain up to 256 rules that determine which users can manage the switch module, and by which methods. Users can also be blocked from accessing the device. Rules are composed of filters including:

- Rule Priority
- Interface
- Management Method
- IP Address
- Prefix Length
- Forwarding Action

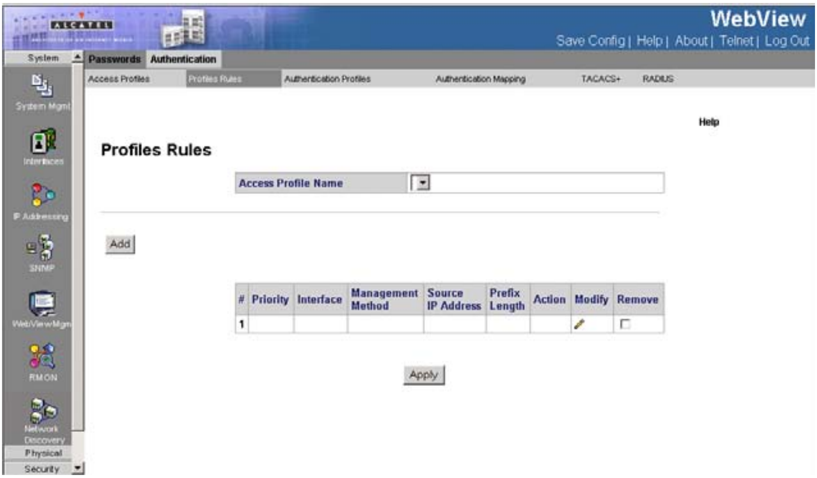
The rule order in the profile rules table is important, since packets are matched to the first rule meeting the rule criteria. The *Profiles Rules Page* contains parameters for defining profile rules.

Command Attributes

- **Access Profile Name** — Displays the access profile to which the rule is attached.

- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Interface** — Indicates the interface type to which the rule applies. The possible field values are:
  - *Port* — Attaches the rule to the selected port.
  - *LAG* — Attaches the rule to the selected LAG.
  - *VLAN* — Attaches the rule to the selected VLAN.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Source IP Address** — Defines the interface source IP address to which the rule applies.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** —Defines the action attached to the rule. The possible field values are:
  - *Permit* — Permits access to the device.
  - *Deny* — Denies access to the device. This is the default.
- **Remove** — Removes rules from the selected access profiles. The possible field values are:
  - *Checked* — Removes the selected rule from the access profile.
  - *Unchecked* — Maintains the rules attached to the access profile.

Web – Click System, WebViewMgmt, Authentication, Profiles Rules, define the fields, and click Apply.



Profiles Rules

Access Profile Name	

#	Priority	Interface	Management Method	Source IP Address	Prefix Length	Action	Modify	Remove
1							✎	□

Figure 3-45. Profiles Rules Page

CLI – The following is an example of the CLI commands used for configuring Profile Rules:

```
Console(config)# ip http server
4-691
Console(config)# ip https server
4-693
```

Defining Authentication Profiles

Authentication profiles allow network administrators to assign authentication methods for user authentication. User authentication can be performed locally or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and the RADIUS server is not available, then the user is authenticated locally.

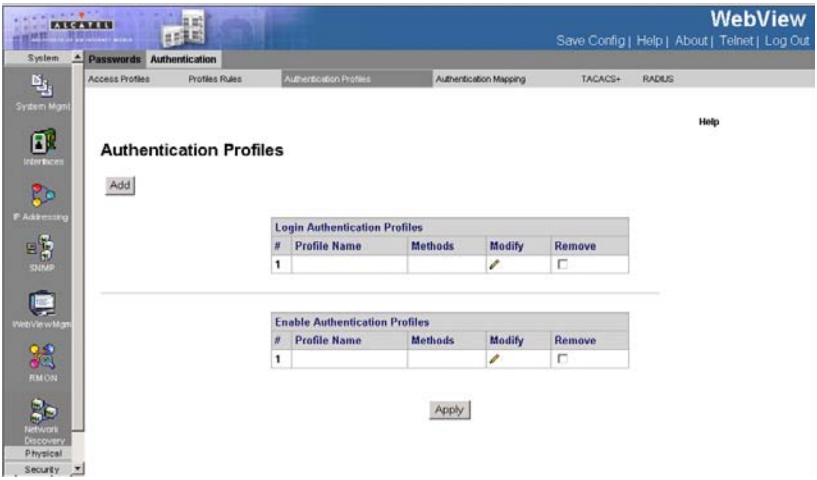
Command Attributes

- **Profile Name** — User-defined authentication profile lists to which user-defined authentication profiles are added.
- **Methods** — Defines the user authentication methods. The possible field values are:
  - *None* — Assigns no authentication method to the authentication profile.
  - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.
  - *RADIUS* — Authenticates the user at the RADIUS server.

- *Line* — Authenticates the user using a line password.
- *Enable* — Authenticates the user using an enable password.
- *TACACS+* — Authenticates the user at the TACACS+ server.

- **Remove** — Removes the selected authentication profile. The possible field values are:
  - *Checked* — Removes the selected authentication profile.
  - *Unchecked* — Maintains the authentication profiles.
- **Profile Method** —
  - *Login* — Specifies the user-defined authentication profile list for login passwords.
  - *Enable* — Specifies the user-define authentication profile list for enable passwords.

Web – Click System, WebViewMgmt, Authentication, Authentication Profiles, define the fields, and click Apply.



Authentication Profiles

Login Authentication Profiles				
#	Profile Name	Methods	Modify	Remove
1			✎	□

Enable Authentication Profiles				
#	Profile Name	Methods	Modify	Remove
1			✎	□

Figure 3-46. Authentication Profiles Page

CLI – The following is an example of the CLI commands used for configuring

Authentication Profiles:

```
Console(config)# aaa authentication login default radius local
enable none
4-288
Console(config)# ip http authentication radius local
4-293
Console(config)# ip https authentication radius local
4-294
Console(config)# line console
4-296
Console(config-line)# login authentication default
4-291
```

Mapping Authentication Methods

After authentication profiles are defined, they can be applied to management access methods. For example, console users can be authenticated by Authentication Profile List 1, while Telnet users are authenticated by Authentication Method List 2. Authentication methods are selected using arrows. The order in which the methods are selected is the order by which the authentication methods are used.

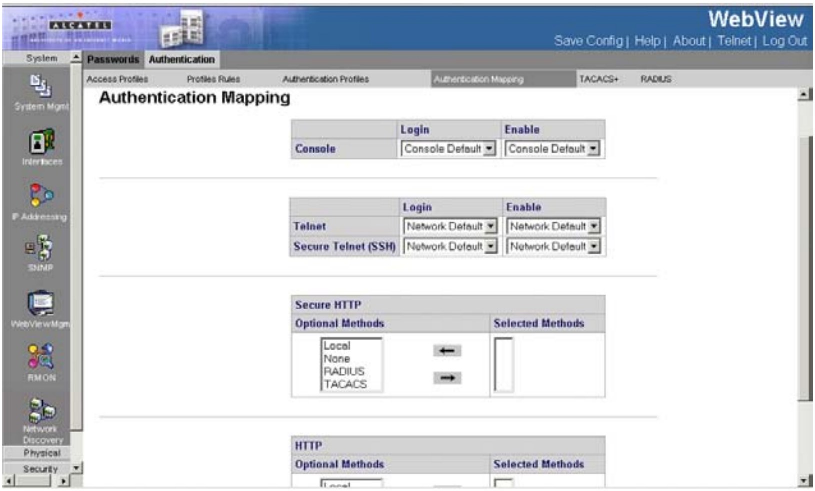
The *Authentication Mapping Page* contains parameters for mapping authentication methods:

Command Attributes

- **Console** — Authentication profiles used to authenticate console users.
- **Telnet** — Authentication profiles used to authenticate Telnet users.
- **Secure Telnet (SSH**) — Authentication profiles used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.
- **Secure HTTP** — Authentication methods used for Secure HTTP access. Possible field values are:
  - *None* — No authentication method is used for access.
  - *Local* — Authentication occurs locally.
  - *RADIUS* — Authentication occurs at the RADIUS server.
  - *TACACS+* — Authentication occurs at the TACACS+ server.
  - *Line* — Authentication using a line password.
  - *Enable* — Authentication using enable.
  - *Local, RADIUS* — Authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is blocked.
  - *RADIUS, Local* — Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.
  - *Local, RADIUS, None* — Authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is permitted.
  - *RADIUS, Local, None* — Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.
- **HTTP** — Authentication methods used for HTTP access. Possible field values are:
  - *None* — No authentication method is used for access.
  - *Local* — Authentication occurs locally.
  - *RADIUS* — Authentication occurs at the RADIUS server.

- *TACACS+* — Authentication occurs at the TACACS+ server.
- *Line* — Authentication using a line password.
- *Enable* — Authentication using enable.
- *Local, RADIUS* — Authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is blocked.
- *RADIUS, Local* — Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.
- *Local, RADIUS, None* — Authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is permitted.
- *RADIUS, Local, None* — Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.

Web – Click System, WebViewMgmt, Authentication, Authentication Mapping, define the fields, and click Apply.



Authentication Mapping

	Login	Enable
Console	Console Default	Console Default

	Login	Enable
Telnet	Network Default	Network Default
Secure Telnet (SSH)	Network Default	Network Default

Secure HTTP	
Optional Methods	Selected Methods
Local None RADIUS TACACS	

HTTP	
Optional Methods	Selected Methods
Local	

Figure 3-47. Authentication Mapping Page

CLI – The following is an example of the CLI commands used for mapping authentication mapping:

```
Console(config)# aaa authentication enable default enable
4-290
```

Defining TACACS+ Methods

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation. Up to 4 TACACS+ servers are supported. TACACS+ provides a centralized user management system, 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. Once the authentication session is completed, an authorization session starts using the authenticated user name.

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

The TACACS+ default parameters are user-assigned defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ new servers. The *TACACS+ Page* contains fields for assigning the Default Parameters for the TACACS+ servers.

Command Attributes

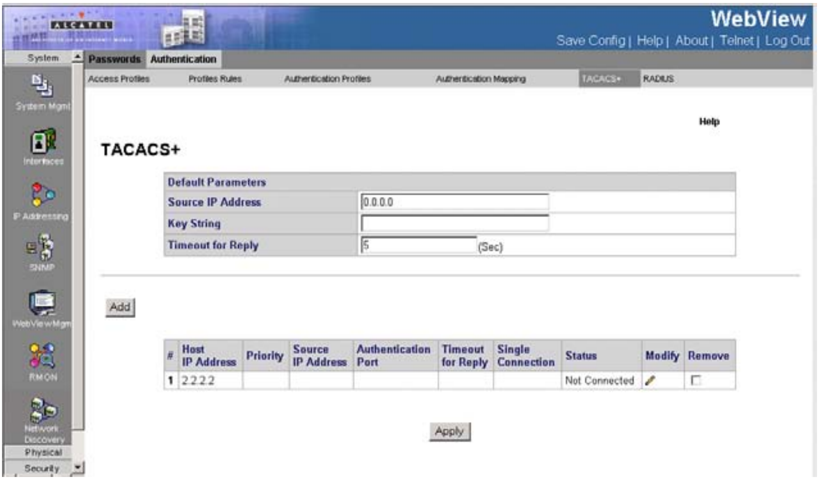
- **Source IP Address** — Defines the default device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** — Defines the default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.
- **Timeout for Reply** — Defines the default time that passes before the connection between the device and the TACACS+ times out. The default is 5.

The following parameters are configured for each TACACS+ server:

- **Host IP Address** — Defines the TACACS+ Server IP address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The field range is 0-65535. The default is 0.
- **Source IP Address** — Defines the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Authentication Port (0-65535)** — Defines the port number via which the TACACS+ session occurs. The default port is port 49.
- **Timeout for Reply**— Defines the amount of time in seconds that passes before the connection between the device and the TACACS+ times out. The field range is 1-1000 seconds.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server. The possible field values are:
  - *Checked* — Enables a single connection.
  - *Unchecked* — Disables a single connection.

- **Status** — Indicates the connection status between the device and the TACACS+ server. The possible field values are:
  - *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
  - *Not Connected* — Indicates there is not currently a connection between the device and the TACACS+ server.
- **Remove** — Removes TACACS+ server. The possible field values are:
  - *Checked* — Removes the selected TACACS+ server.
  - *Unchecked* — Maintains the TACACS+ servers.

Web – Click System, WebViewMgmt, Authentication, TACACS+, define the fields, and click Apply.



TACACS+

Default Parameters	
Source IP Address	0.0.0.0
Key String	
Timeout for Reply	5 (Sec)

#	Host IP Address	Priority	Source IP Address	Authentication Port	Timeout for Reply	Single Connection	Status	Modify	Remove
1	2.2.2.2						Not Connected	✎	□

Figure 3-48. TACACS+ Page

CLI – The following is an example of the TACACS+ CLI Commands:

```
Console(config)# tacacs-server host 172.16.1.1
4-622
Console(config)# tacacs-server key
4-623
Console(config)# tacacs-server timeout 30
4-624
Console(config)# tacacs-server source-ip 172.16.8.1
4-625
```

Defining RADIUS Settings

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access.

Default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers. The *RADIUS Page* contains parameters for defining RADIUS servers.

Command Attributes

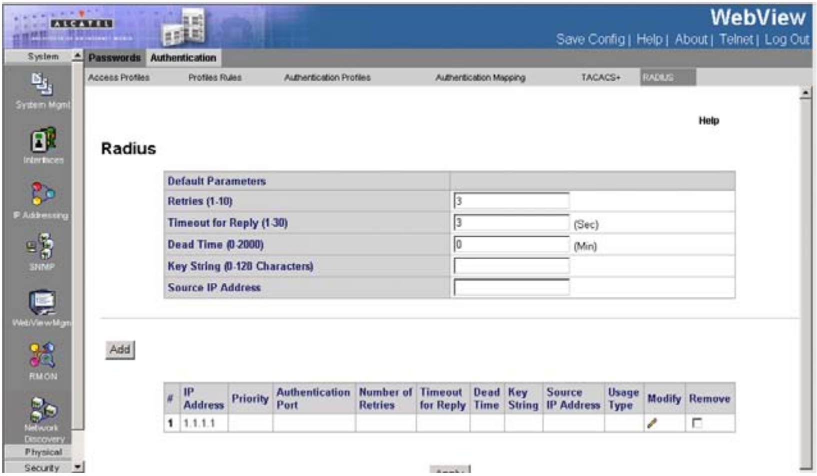
- **Default Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1-10.
- **Default Timeout for Reply** — Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. Possible field values are 1-30.
- **Default Dead Time** — Defines the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000.
- **Default Key String** — Defines the default key string used for authenticating and encrypting all RADIUS-communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Source IP Address** — Displays the source address.

The following parameters are configured for each TACACS+ server:

- **Source IP Address** — Defines the default IP address of a device accessing the RADIUS server.
- **IP Address —** Lists the RADIUS server IP addresses.
- **Priority** — Displays the RADIUS server priority. The possible values are 1-65535, where 1 is the highest value. The RADIUS server priority is used to configure the server query order.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Number of Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. The possible field values are 1-10. Three is the default value.
- **Timeout for Reply** — Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1-30. Three is the default value.
- **Dead Time** — Defines the amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default is 0 minutes.
- **source IP address** — Defines the source IP address that is used for communication with RADIUS servers.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is *All*. The possible field values are:
  - *Log in* — The RADIUS server is used for authenticating user name and passwords.
  - *802.1X* — The RADIUS server is used for 802.1X authentication.
  - *All* — The RADIUS server is used for authenticating user names and passwords, and 802.1X port authentication.

- **Remove**— Removes a RADIUS server. The possible field values are:
  - *Checked* — Removes the selected RADIUS server.
  - *Unchecked* — Maintains the RADIUS servers.

Web – Click System, WebViewMgmt, Authentication, RADIUS, define the fields, and click Apply.



Radius

Default Parameters	
Retries (1-10)	3
Timeout for Reply (1-30)	3 (Sec)
Dead Time (0-2000)	0 (Min)
Key String (0-128 Characters)	
Source IP Address	

#	IP Address	Priority	Authentication Port	Number of Retries	Timeout for Reply	Dead Time	Key String	Source IP Address	Usage Type	Modify	Remove
1	1.1.1.1									✎	□

Figure 3-49. RADIUS Page

CLI – The following is an example of the RADIUS CLI Commands:

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

4-495
Console(config)# radius-server key alcatel-server
4-497
console(config)# radius-server retransmit 5
4-497
console(config)# radius-server source-ip 10.1.1.1
4-498
Console(config)# radius-server timeout 5
4-499
Console(config)# radius-server deadtime 10
4-500
```

Managing RMON Statistics

RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot.

Viewing RMON Statistics

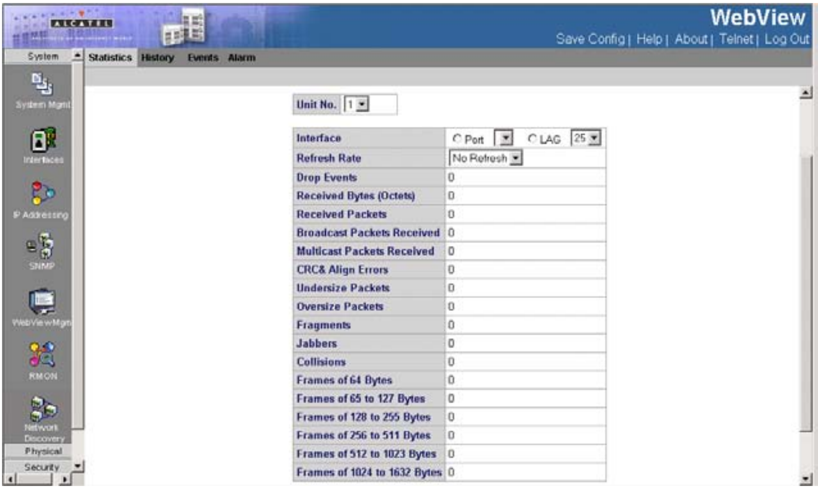
The *RMON Statistics Page* contains fields for viewing information about device utilization and errors that occurred on the device.

Command Attributes

- **Unit No.** — Displays the stacking member for which the Statistics Etherlike is displayed.
- **Interface** — Indicates the interface for which statistics are displayed. The possible field values are:
  - *Port* — Defines the specific port for which RMON statistics are displayed.
  - *LAG* — Defines the specific LAG for which RMON statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - *15 Sec* — Indicates that the RMON statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the RMON statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the RMON statistics are refreshed every 60 seconds.
  - *No Refresh* — Indicates that the RMON statistics are not refreshed automatically.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Broadcast Packets Received** — Displays the 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** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.

- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
- **Frames of xx Bytes** — Number of *xx*-byte frames received on the interface since the device was last refreshed.

Web – Click System, RMON, Statistics. Select an interface.



Unit No. 1

Interface	○ Port ○ LAG 25
Refresh Rate	No Refresh
Drop Events	0
Received Bytes (Octets)	0
Received Packets	0
Broadcast Packets Received	0
Multicast Packets Received	0
CRC& Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	0
Frames of 65 to 127 Bytes	0
Frames of 128 to 255 Bytes	0
Frames of 256 to 511 Bytes	0
Frames of 512 to 1023 Bytes	0
Frames of 1024 to 1632 Bytes	0

Figure 3-50. RMON Statistics Page

CLI – The following is an example of the CLI commands used to view RMON statistics:

```
Console# show rmon statistics ethernet 1/e1
4-503

Port: 1/e1

Octets: 878128                  Packets: 978

Broadcast: 7                    Multicast: 1

CRC Align Errors: 0             Collisions: 0
```

```
Undersize Pkts: 0                Oversize Pkts: 0
Fragments: 0                     Jabbers: 0
64 Octets: 98                    65 to 127 Octets: 0
128 to 255 Octets: 0             256 to 511 Octets: 0
512 to 1023 Octets: 491          1024 to 1518 Octets: 389
```

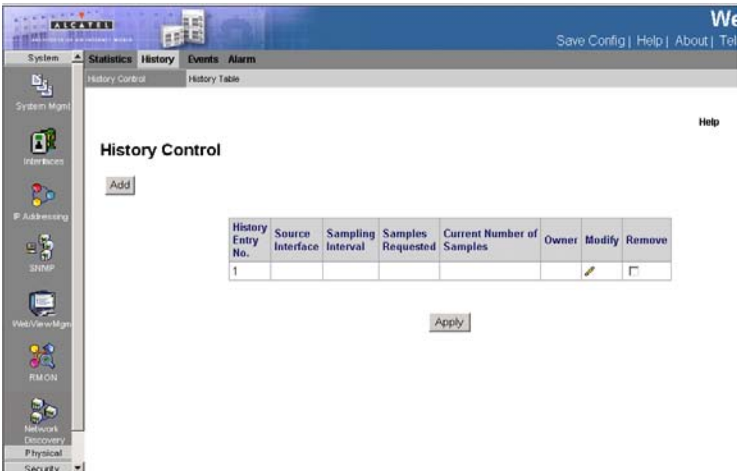
Defining RMON History Control

The *History Control Page* contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

Command Attributes

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Source Interface** — Displays the interface from which the history samples were taken. The possible field values are:
  - *Port* — Specifies the port from which the RMON information was taken.
  - *LAG* — Specifies the port from which the RMON information was taken.
- **Sampling Interval** — Indicates in seconds the time that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).
- **Samples Requested**— Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
- **Current Number of Samples** — Displays the current number of samples taken.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Remove** — Removes History Control entries. The possible field values are:
  - *Checked* — Removes the selected History Control entry.
  - *Unchecked* — Maintains the current History Control entries.

Web – Click System, RMON, History, History Control and select an interface.



History Control

History Entry No.	Source Interface	Sampling Interval	Samples Requested	Current Number of Samples	Owner	Modify	Remove
1						✎	□

Figure 3-51. History Control Page

CLI – The following is an example of the CLI commands used to view RMON History Control statistics:

```
Console(config)# interface ethernet 1/e1
4-376
Console(config-if)# rmon collection history 1 interval 2400
4-506
```

Viewing the RMON History Table

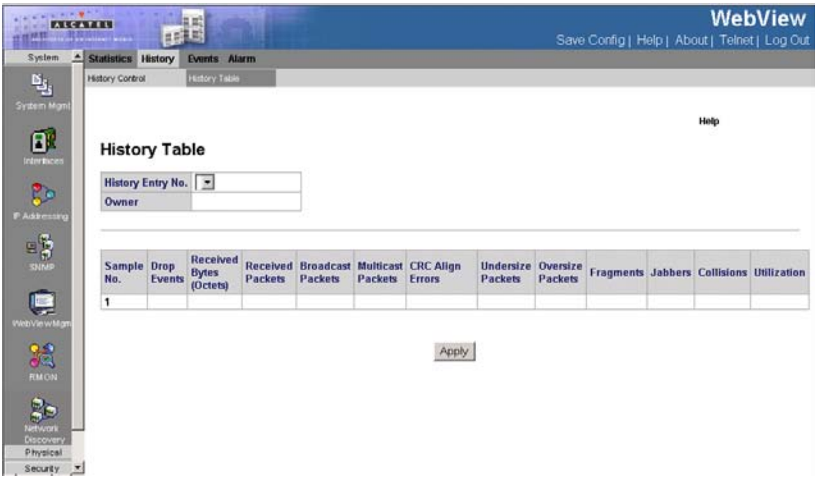
The *History Table Page* contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

Command Attributes

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Sample Number**— Indicates the sample number from which the statistics were taken.
- **Drop Events** — Displays the amount of dropped events on the device.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays the number of packets received on the interface since the device was last refreshed, including bad packets, Multicast and Broadcast packets.

- **Broadcast Packets** — Displays the number of good Broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
- **Utilization** — Displays the percentage of the interface utilized.

Web – Click System, RMON, History, History Table and select an a history entry number.



History Table

History Entry No.	
Owner	

Sample No.	Drop Events	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization
1												

Figure 3-52. History Table Page

CLI – The following is an example of the CLI commands used to view RMON History Table statistics:

```
Console# show rmon history 1 throughput                                         4-507
Sample Set: 1                       Owner: CLI
Interface: 1/e1                     Interval: 1800
Requested samples: 50               Granted samples: 50


Maximum table size: 500


Time                    Octets       Packets      Broadcas     Multicast    Util
                                                  t
-------------------     ---------    -------      --------     ---------    -----
-                                                 -
Jan 18 2002             303595962    357568       3289         7287         19%
21:57:00
Jan 18 2002             287696304    275686       2789         5878         20%
21:57:30


Console# show rmon history 1 errors                                             4-507
Sample Set: 1                       Owner: Me
Interface: 1/e1                     Interval: 1800
Requested samples: 50               Granted samples: 50


Maximum table size: 500 (800 after reset)


Time                    CRC Align    Undersize    Oversize     Fragments    Jabbers
----------              ---------    ---------    --------     ---------    -------
Jan 18 2002             1            1            0            49           0
21:57:00
Jan 18 2002             1            1            0            27           0
21:57:30
```

```
Console# show rmon history 1 other                                     4-507

Sample Set: 1                     Owner: Me

Interface: 1/e1                   Interval: 1800

Requested samples: 50             Granted samples: 50


Maximum table size: 500


Time                              Dropped     Collisio
                                              ns

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

Jan 18 2002 21:57:00              3           0

Jan 18 2002 21:57:30              3           0
```

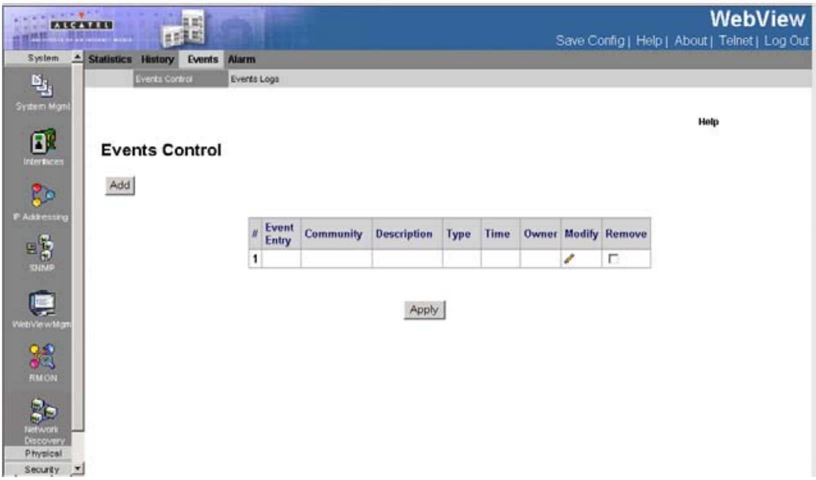
Defining RMON Events Control

The *Events Control Page* contains fields for defining RMON events.

Command Attributes

- **Event Entry** — Displays the event.
- **Community** — Displays the community to which the event belongs.
- **Description** — Displays the user-defined event description.
- **Type** — Describes the event type. Possible values are:
  - *Log* — Indicates that the event is a log entry.
  - *Trap* — Indicates that the event is a trap.
  - *Log and Trap* — Indicates that the event is both a log entry and a trap.
  - *None* — Indicates that no event occurred.
- **Time** — Displays the time that the event occurred.
- **Owner** — Displays the device or user that defined the event.
- **Remove** — Removes a RMON event. The possible field values are:
  - *Checked* — Removes a selected RMON event.
  - *Unchecked* — Maintains RMON events.

Web – Click System, RMON, Events, Events Control and select an interface.



Events Control

#	Event Entry	Community	Description	Type	Time	Owner	Modify	Remove
1							✎	☐

Figure 3-53. Events Control Page

CLI – The following is an example of the CLI commands used to view RMON events Control statistics:

```
Console(config)# rmon event 10 log
4-514
```

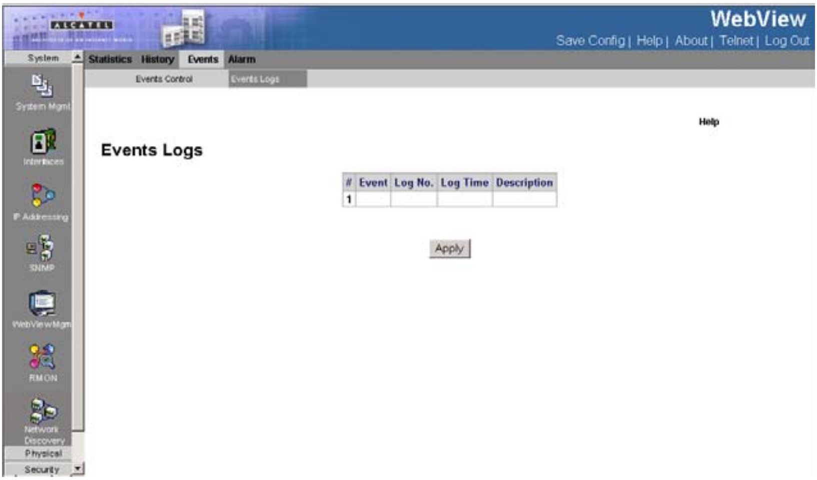
Viewing the RMON Events Logs

The *Events Logs Page* contains a list of RMON events.

Command Attributes

- **Event** — Displays the RMON Events Log entry number.
- **Log No.** — Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Displays the log entry description.

Web – Click System, RMON, Events, Events Logs and select an interface.



Events Logs

#	Event	Log No.	Log Time	Description
1				

Figure 3-54. Events Logs Page

CLI – The following is an example of the CLI commands used to view RMON events Logs:

```
Console> show rmon events
4-514


Index   Description    Type   Community     Owner   Last time sent

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

1       Errors         Log                  CLI     Jan 18 2002 23:58:17

2       High           Log-   device        Manag   Jan 18 2002 23:59:48
        Broadcast      Trap                 er
```

Defining RMON Alarms

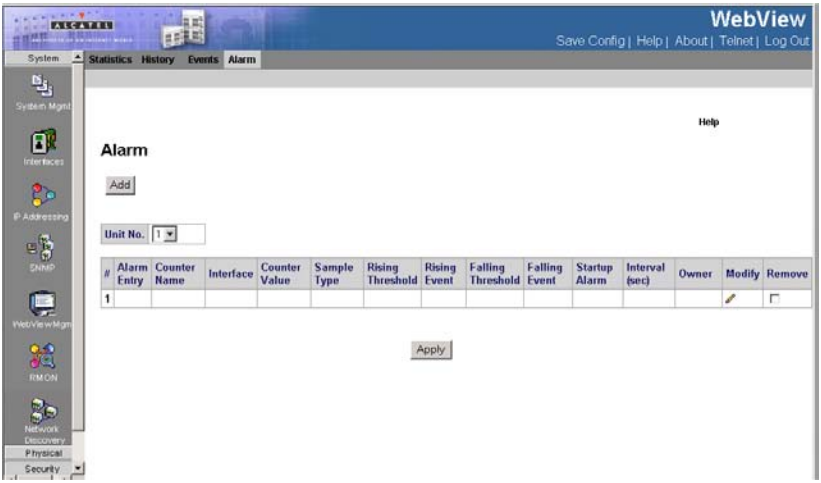
The *Alarm Page* contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.

Command Attributes

- **Unit No.** — Displays the stacking member for which the RMON Alarms are displayed.
- **Alarm Entry** — Indicates a specific alarm.
- **Counter Name** — Displays the selected MIB variable.

- **Interface** — Displays interface for which RMON statistics are displayed. The possible field values are:
  - *Port* — Displays the RMON statistics for the selected port.
  - *LAG* — Displays the RMON statistics for the selected LAG.
- **Counter Value** — Displays the selected MIB variable value.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values 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** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** — Displays the mechanism in which the alarms are reported. The possible field values are:
  - *LOG* — Indicates there is not a saving mechanism for either the device or in the management system. If the device is not reset, the entry remains in the Log Table.
  - *TRAP* — Indicates that an SNMP trap is generated, and sent via the Trap mechanism. The Trap can also be saved using the Trap mechanism.
  - *Both*— Indicates that both the Log and Trap mechanisms are used to report alarms.
- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** — Displays the mechanism in which the alarms are reported.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
  - *Rising Alarm* — The rising counter value that triggers the rising threshold alarm.
  - *Falling Alarm* — The falling counter value that triggers the falling threshold alarm.
  - *Rising and Falling* — The rising and falling counter values that trigger the alarm.
- **Interval** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.
- **Remove** — Removes the RMON Alarms Table entry.

Web – Click System, RMON, Alarm, define the fields, and click Apply.



Alarm

Unit No. 1

#	Alarm Entry	Counter Name	Interface	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Startup Alarm	Interval (sec)	Owner	Modify	Remove
1													✎	□

Figure 3-55. Alarm Page

CLI – The following is an example of the CLI commands used to set RMON alarms:

```
Console(config)# rmon alarm 1000 1.3.6.1.2.1.10.7.2.1.3.51 1000000
1000000 10 20 1
4-510
```

Alcatel Mapping Adjacency Protocol (AMAP)

The AMAP protocol enables a switch to discover the topology of other AMAP-aware devices in the network. The protocol allows each switch to determine if other AMAP-aware switches are adjacent to it. Note that two switches are adjacent if and only if the following two requirements are satisfied:

- There exists a Spanning Tree path between them.
- There exists no other AMAP-aware device between the two switches on that Spanning Tree path.

Configuring AMAP

The AMAP protocol discovers adjacent switches by sending and receiving AMAP Hello packets on active Spanning Tree ports. Each port can be defined as being in one of three logical states of processing the AMAP Hello Packets: discovery, common, or passive.

Note: AMAP packets are registered only on a default VLAN.

Use the *AMAP Settings Page* to enable/disable AMAP and configure timeout parameters.

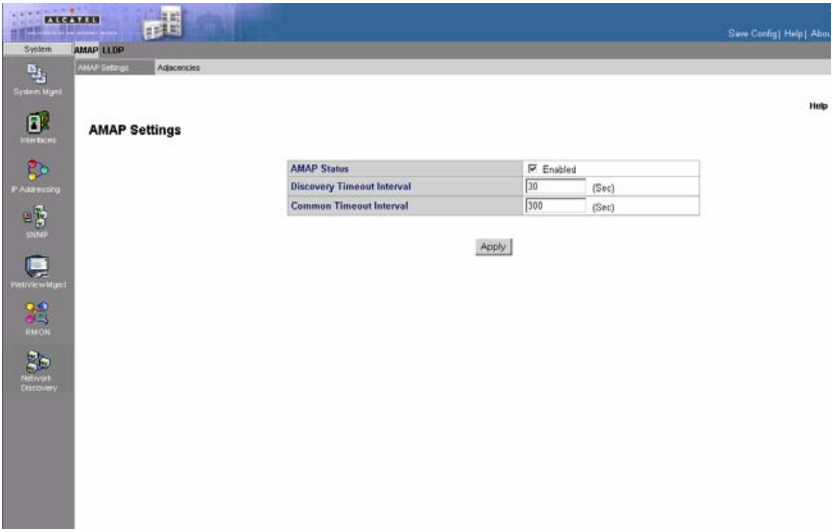
The following parameters describe the three main AMAP port states:

- **Discovery** – The initial state where a port transmits a “Hello” packet to detect an adjacent switch and then waits for a response.
- **Common** – The port has detected an adjacent switch and periodically sends “Hello” packets to determine that it is still present.
- **Passive** – A port enters this state if there is no response to a Discovery “hello” packet. This is a receive-only state and no “Hello” packets are transmitted. If a “Hello” packet is received from an adjacent switch, the port enters the Common state and then transmits a “Hello” packet in reply.

Command Attributes

- **AMAP Status** – Enables or disables AMAP on the switch. (Default: enabled)
- **Discovery Timeout Interval** – Sets the time the switch will wait before sending a “Hello” packet to detect an adjacent switch. (Range:1-65535 seconds)
- **Common Timeout Interval** – After detecting an adjacent switch this sets the time the switch will wait before sending a further “Hello” packet to determine if the adjacent switch is still connected. (Range:1-65535 seconds)

Web – Click System, Network Discovery, AMAP, AMAP Settings. Select whether to enable AMAP, enter the desired timeout intervals and click Apply.



AMAP Settings

AMAP Status	☑ Enabled
Discovery Timeout Interval	30 (Sec)
Common Timeout Interval	300 (Sec)

Figure 3-56. AMAP Settings Page

CLI – The following is an example of the AMAP CLI commands:

```
Console(config)# amap enable                                      4-345
Console(config)# amap discovery time 3000                         4-346
Console(config)# amap common time 5000                            4-346
```

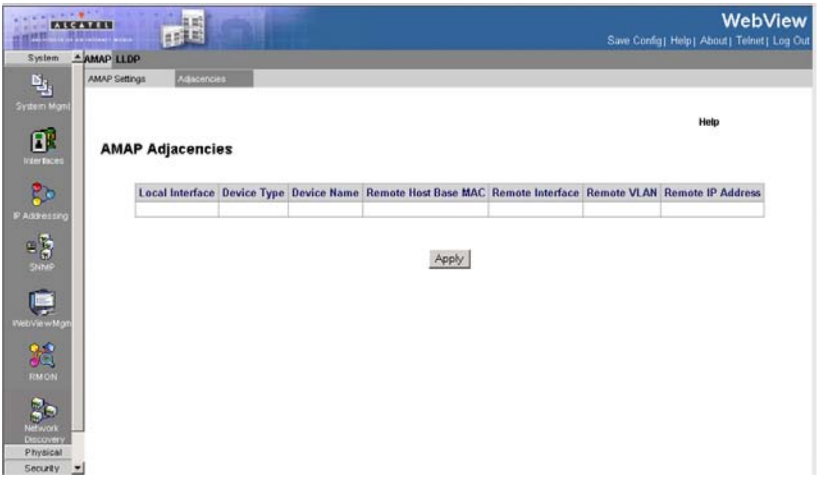
Viewing Adjacent Devices

The *AMAP Adjacencies Page* provides network configuration information about the systems connected to the device. The table displays the IP and MAC addresses of the local port, and the IP and MAC addresses, and VLAN ID of the connected devices.

Command Attributes

- **Local Interface** — Indicates a local interface that has a valid connection to an adjacent device. The connected device's network ID information is displayed in the table’s other columns.
- **Device Type** — Model name for the adjacent switch.
- **Device Name** – Indicates the adjacent switch's hostname.
- **Remote Host Base MAC** – Indicates the adjacent switch's MAC Address.
- **Remote Interface** – Indicate the remote interface port connected to the device.
- **Remote VLAN** – Indicate the remote Vlan connected to the adjacent switch.
- **Remote IP Address** – Indicate the remote switch’s IP address.

Web – Click System, Network Discovery, AMAP, AMAP Adjacencies. Select whether to enable AMAP, enter the desired timeout intervals and click Apply.



AMAP Adjacencies

Local Interface	Device Type	Device Name	Remote Host Base MAC	Remote Interface	Remote VLAN	Remote IP Address

Figure 3-57. AMAP Adjacencies Page

CLI – The following is an example of the AMAP Adjacencies commands:

```
Console# show amap                                                   4-346
Operational Status: active,
Common Phase Timeout Interval (seconds)= 300,
Discovery Phase Timeout Interval (seconds)= 30.
```

Configuring LLDP

The *Link Layer Discovery Protocol* (LLDP) allows 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 system, and to store discovered information. Device discovery information includes:

- Device Identification
- Device Capabilities
- Device Configuration

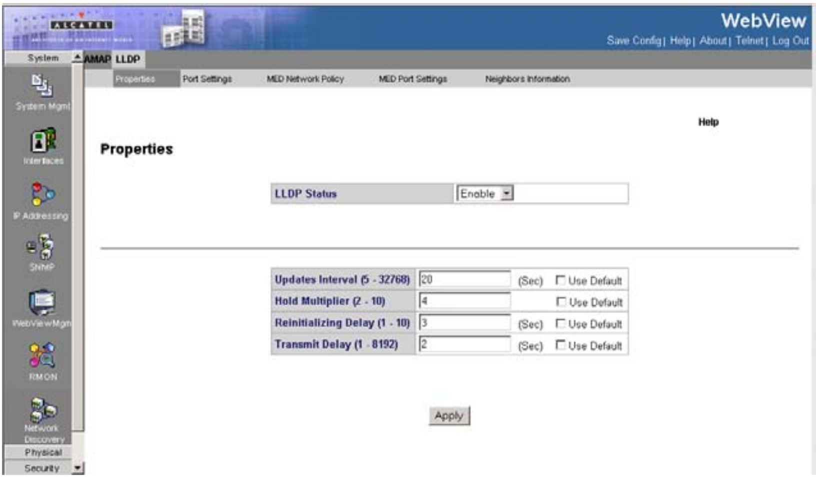
The advertising device transmits multiple advertisement message sets in a single LAN packet. The multiple advertisement sets are sent in the packet *Type Length Value* (TLV) field. LLDP devices must support chassis and port ID advertisement, as well as system name, system ID, system description, and system capability advertisements.

Command Attributes

- **Enable LLDP** — Indicates if LLDP is enabled on the device. The possible field values are:
  - *Enabled* — Indicates that LLDP is enabled on the device.
  - *Disabled* — Indicates that LLDP is disabled on the device. This is the default value.
- **Updates Interval (5-32768) —** Indicates that rate at which LLDP advertisement updates are sent. The possible field range is 5 - 3276 seconds. The default value is 30 seconds.
- **Hold Multiplier** — Indicates the amount of time that LLDP packets are held before the packets are discarded. The value represents a multiple of the Updates Interval. The possible field range is 2 - 10. The field default is 4. For example, if the Update Interval is 30 seconds and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds.
- **Reinitializing Delay (1-10)** — Indicates the amount of time that passes between disabling LLDP and when reinitializing begins. The possible field range is 1 - 10 seconds. The field default is 2 seconds.
- **Transmit Delay** — Indicates the amount of time that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB. The possible field value is 1 – 8192 seconds. The field default is 2 seconds.

Web – Click Network Discovery, LLDP, Properties. Define the fields and click Apply.

opens:



Properties

LLDP Status	Enable

Updates Interval (5 - 32768)	20	(Sec)	□ Use Default
Hold Multiplier (2 - 10)	4		□ Use Default
Reinitializing Delay (1 - 10)	3	(Sec)	□ Use Default
Transmit Delay (1 - 8192)	2	(Sec)	□ Use Default

Figure 3-58. LLDP Properties Page

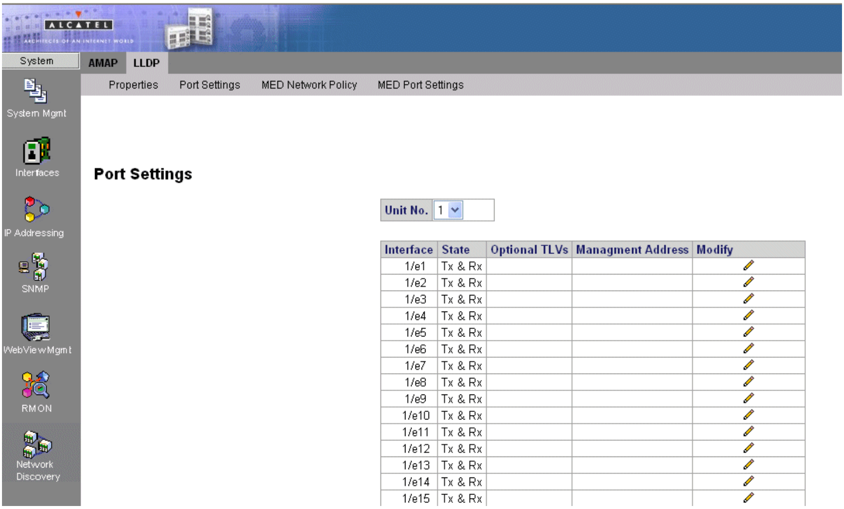
Defining LLDP Port Settings

The *LLDP Port Settings Page* allows network administrators to define LLDP port settings, including the port type, the LLDP port state, and the type of port information advertised. To define LLDP Port Properties:

Command Attributes

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Interface** — Contains a list of ports on which LLDP is enabled.
- **State** — Indicates the port type on which LLDP is enabled. The possible field values are:
  - *Tx Only* — Enables transmitting LLDP packets only.
  - *Rx Only* — Enables receiving LLDP packets only.
  - *Tx & Rx* — Enables transmitting and receiving LLDP packets. This is the default value.
  - *Disable* — Indicates that LLDP is disabled on the port.
- **Optional TLVs** — Contains a list of optional TLVs advertised by the port. For the complete list, see the **Available TLVs** field.
- **Management IP Address** — Indicates the management IP address that is advertised from the interface.
- **Neighbors** — Information received from neighboring device LLDP advertisements.

Web – Click Network Discovery, LLDP, Port settings. Define the fields and click Apply.



Port Settings

Unit No. 1

Interface	State	Optional TLVs	Managment Address	Modify
1/e1	Tx & Rx			✎
1/e2	Tx & Rx			✎
1/e3	Tx & Rx			✎
1/e4	Tx & Rx			✎
1/e5	Tx & Rx			✎
1/e6	Tx & Rx			✎
1/e7	Tx & Rx			✎
1/e8	Tx & Rx			✎
1/e9	Tx & Rx			✎
1/e10	Tx & Rx			✎
1/e11	Tx & Rx			✎
1/e12	Tx & Rx			✎
1/e13	Tx & Rx			✎
1/e14	Tx & Rx			✎
1/e15	Tx & Rx			✎

Figure 3-59. LLDP Port Settings Page

Defining Media Endpoint Discovery Network Policy

LLDP Media Endpoint Discovery (LLDP-MED) increases network flexibility by allowing different IP systems to co-exist on a single network. LLDP provides the following:

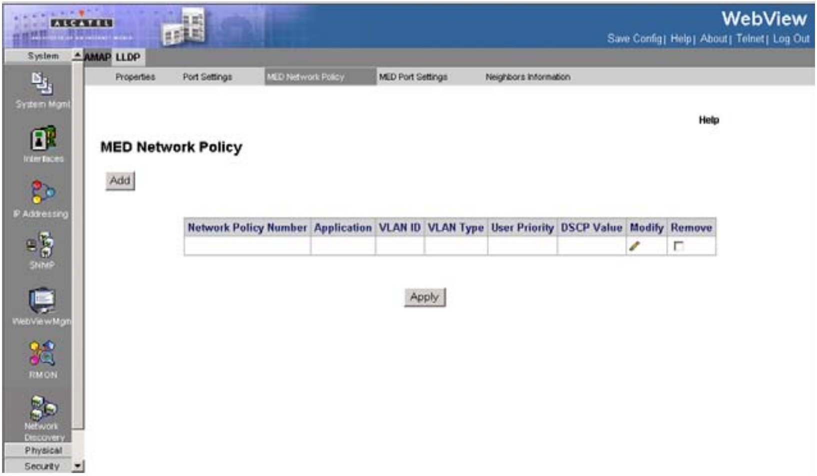
- Detailed network topology information including which device are located on the network, and where these devices are located. For example, what IP phone is connect to what port, what software is running on what switch, and with port is connected to what PC.
- Automatic deployment of policies over networks for:
  - QoS Policies
  - Voice VLANs
- Emergency Call Service (E-911) via IP Phone location information.
- Troubleshooting alerts to network managers for:
  - Port speed and duplex mode conflicts
  - QoS policy misconfigurations

Command Attributes

- **Network Policy Number** — Displays the network policy number.
- **Application** — Displays the application for which the network policy is defined. The possible field values are:
  - *Voice* — Indicates that the network policy is defined for a Voice application.
  - *Voice Signaling* — Indicates that the network policy is defined for a Voice Signaling application.

  - *Guest VLAN* — Indicates that the network policy is defined for a Guest VLAN application.
  - *Guest VLAN Signaling* — Indicates that the network policy is defined for a Guest VLAN Signalling application.
  - *Softphone Voice* — Indicates that the network policy is defined for a Softphone Voice application.
  - *Video Conferencing* — Indicates that the network policy is defined for a Video Conferencing application.
  - *Streaming Video* — Indicates that the network policy is defined for a Streaming Video application.
- **VLAN ID** — Indicates the VLAN ID for which the Network policy is assigned.
- **VLAN Type** — Indicates the VLAN type for which the network policy is defined. The possible field values are:
  - *Tagged* — Indicates the network policy is defined for tagged VLANs.
  - *Untagged* — Indicates the network policy is defined for untagged VLANs.
- **User Priority** — Defines the priority assigned to the network application.
- **DSCP Value** — Defines the DSCP value assigned to the network policy. The possible field value is 1-64.

Web – Click Network Discovery, LLDP, MED Network Policy. Define the fields and click Apply.



MED Network Policy

Network Policy Number	Application	VLAN ID	VLAN Type	User Priority	DSCP Value	Modify	Remove
						✎	□

Figure 3-60. MED Networking Policy Page

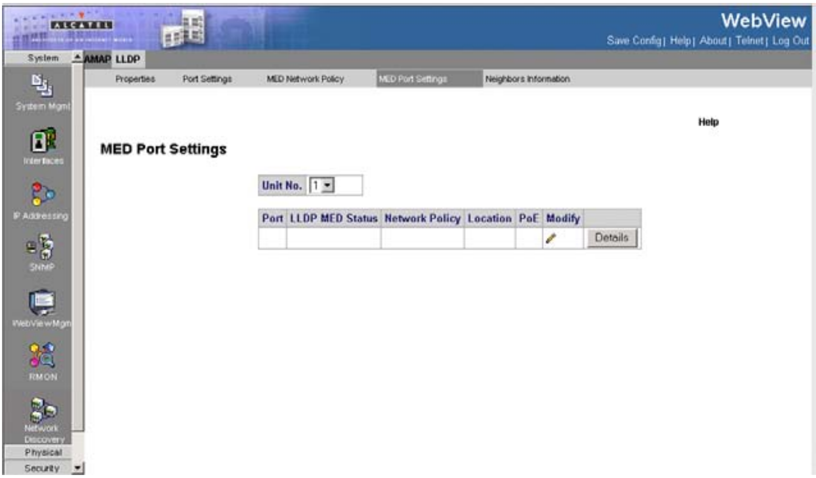
Defining LLDP MED Port Settings

The *MED Port Settings Page* contains parameters for assigning LLDP network policies to specific ports.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Port** — Displays the port to which the network policy is attached.
- **LLDP MED Status** — Indicates if LLDP is enabled on the device. The possible field values are:
  - *Enable* – Enables LLDP MED on the device.
  - *Disable* – Disables LLDP MED on the device. This is the default value
- **Network Policy** — Indicates whether activated or not.
- **Location** — Indicates whether activated or not.
- **PoE** — Indicates whether activated or not.

Web – Click Network Discovery, LLDP, MED Port Settings. Define the fields and click Apply.



MED Port Settings

Unit No. 1

Port	LLDP MED Status	Network Policy	Location	PoE	Modify	
					✎	Details

Figure 3-61. MED Port Settings Page

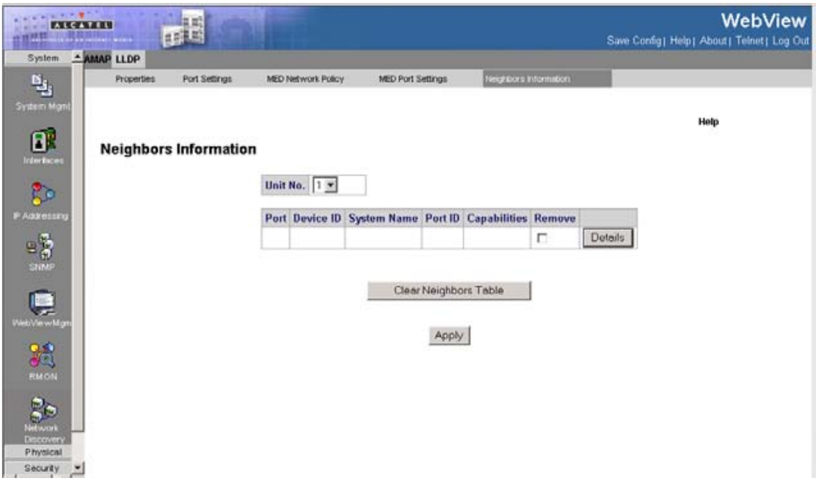
Viewing the LLDP Neighbor Information

The *LLDP Neighbor Information Page* contains information received from neighboring device LLDP advertisements.

Command Attributes

- **Port** — Displays the neighboring port number.
- **Device ID** — Displays the neighboring device ID.
- **System Name** — Displays the neighboring system time.
- **Port ID** — Displays the neighboring port ID.
- **Capabilities** — Displays the neighboring device capabilities.
- **Remove** — Removes the Neighbors Information entry.

Web – Click Network Discovery, LLDP, Neighbors Information. Define the fields and click Apply



Neighbors Information

Unit No. 1

Port	Device ID	System Name	Port ID	Capabilities	Remove	
					□	Details

Figure 3-62. LLDP Neighbor Information Page

Viewing Neighbor Information Details

In the *LLDP Neighbor Information Page*, click the Details button to open the The *Details Neighbor Information Page.*

The *Details Neighbor Information Page* displays the information advertised by neighboring ports when advertising LLDP information.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Port** — Displays the port number from which the advertised information is sent.
- **Auto-Negotiation Status** — Indicates that the Auto Negotiation is supported by the device advertising the LLDP MED information.
- **Advertised Capabilities** — Displays the advertised device capabilities.
- **MAU Type** — Indicates the MAU (Media Attachment Unit) type. The MAU performs physical layer functions including conversion of the digital data from the Ethernet interface, collision detection, and injection of bits onto the network.
- **System Name** — Displays the advertised system name.
- **System Description** — Displays the advertised system description.
- **Device ID** — Displays the advertised device ID.
- **LLDP MED Capabilities** — The capabilities discovered on the neighbor device.
- **LLDP MED Device Type** — Contains a value that indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.

LLDP MED Power over Ethernet

- **Power Type** — Indicates whether the device is a Power Sourcing Entity (PSE) or Power Device (PD)
- **Power Source** — Indicates the power source used by a PSE or PD device. A PSE device advertises its power capability. The possible field values are:
  - *Primary power* – Indicates the power source is the primary power source used by the PSE or the PD
  - *Local power* – Indicates the power source is the local power source used by the PSE or the PD.
- **Power Priority** — Indicates the power source used by a PSE or PD device. A PSE device advertises its power capability. The possible field values are:
  - *Critical* — Defines the power capability as critical
  - *High* — Defines the power capability as high
  - *Low* — Defines the power capability as low
- **Power Value** — Indicates the total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.

LLDP Network Policy

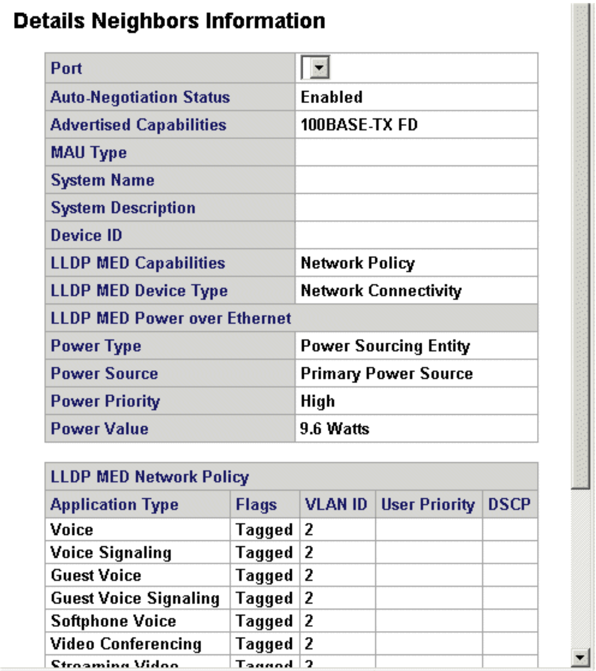
The LLDP Network Policy table displays the application for which the network policy is defined. The possible field values are:

- *Voice* — Indicates that the network policy is defined for a Voice application.
- *Voice Signaling* — Indicates that the network policy is defined for a Voice Signaling application.
- *Guest Voice* — Indicates that the network policy is defined for a Guest Voice application.
- *Guest Voice Signaling* — Indicates that the network policy is defined for a Guest Voice Signalling application.
- *Softphone Voice* — Indicates that the network policy is defined for a Softphone Voice application.
- *Video Conferencing* — Indicates that the network policy is defined for a Video Conferencing application.
- *Streaming Video* — Indicates that the network policy is defined for a Streaming Video application.
- *Video Signaling* — Indicates that the network policy is defined for a Video Signaling application.

LLDP Med Location

- **Location Coordinate** — Displays the device’s location coordinates.
- **Location Civic Address** — Displays the device’s civic or street address location, for example 414 23rd Ave E.
- **Location ECS ELIN** — Displays the device’s ECS ELIN location.

Web – Click Network Discovery, LLDP, Neighbors Information, Details button.



Details Neighbors Information

Port	
Auto-Negotiation Status	Enabled
Advertised Capabilities	100BASE-TX FD
MAU Type	
System Name	
System Description	
Device ID	
LLDP MED Capabilities	Network Policy
LLDP MED Device Type	Network Connectivity
LLDP MED Power over Ethernet	
Power Type	Power Sourcing Entity
Power Source	Primary Power Source
Power Priority	High
Power Value	9.6 Watts

LLDP MED Network Policy

Application Type	Flags	VLAN ID	User Priority	DSCP
Voice	Tagged	2		
Voice Signaling	Tagged	2		
Guest Voice	Tagged	2		
Guest Voice Signaling	Tagged	2		
Softphone Voice	Tagged	2		
Video Conferencing	Tagged	2		
Streaming Video	Tagged	2		

Figure 3-63. Details Neighbor Information Page

Managing Power-over-Ethernet Devices

Power-over-Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power-over-Ethernet removes the necessity of placing network devices next to power sources.

Power-over-Ethernet can be used in the following applications:

- IP Phones
- Wireless Access Points
- IP Gateways
- PDAs
- Audio and video remote monitoring

Powered Devices are devices which receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports.

Guard Band protects the device from exceeding the maximum power level. For example, if 400W is maximum power level, and the Guard Band is 20W, if the total system power consumption exceeds 380W no additional PoE components can be added. The accumulated PoE components power consumption is rounded down for display purposes, therefore remove value after decimal point.

Note: Due do hardware limitations, the power measurement accuracy is 4%.

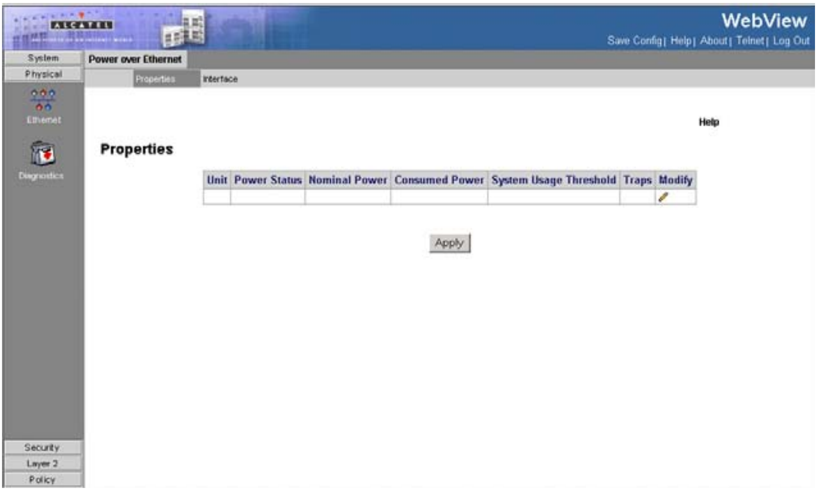
Defining PoE System Information

The *Properties Page* contains system PoE information for enabling PoE on the device, monitoring the current power usage, and enabling PoE traps.

Command Attributes

- **Unit** — Indicates the stacking member for which the PoE information is displayed.
- **Power Status** — Indicates the inline power source status.
  - *On* — Indicates that the power supply unit is functioning.
  - *Off* — Indicates that the power supply unit is not functioning.
  - *Faulty* — Indicates that the power supply unit is functioning, but an error has occurred. For example, a power overload or a short circuit.
- **Nominal Power** — Indicates the actual amount of power the device can supply. The field value is displayed in Watts.
- **Consumed Power** — Indicates the amount of the power used by the device. The field value is displayed in Watts.
- **System Usage Threshold** — Indicates the percentage of power consumed before an alarm is generated. The field value is 1-99 percent. The default is 95 percent.
- **Traps** — Indicate if PoE device traps are enabled. The possible field values are:
  - *Enable* — Enables PoE traps on the device.
  - *Disable* — Disables PoE traps on the device.This is the default value.

Web – Click Physical, Ethernet, Power over Ethernet, Properties page. Define the fields and click Apply.



Properties

Unit	Power Status	Nominal Power	Consumed Power	System Usage Threshold	Traps	Modify
						✎

Figure 3-64. Properties Page

CLI – The following is an example of PoE properties commands:

```
Console(config)# power inline usage threshold 80
4-460
Console(config)# power inline traps enable
4-463
Console(config)# end
Console# show power inline
4-464
Power: On
Nominal Power: 150 Watt
Consumed Power: 120 Watts (80%)
Usage Threshold: 95%
Traps: Enabled
```

Defining PoE Interfaces

The *PoE Interface Page* contains information for configuring PoE interfaces, including the interface PoE operation status and the interface's power consumption.

Command Attributes

- **Port** — Indicates the specific interface for which PoE parameters are defined and assigned to the powered interface connected the to selected port.
- **Admin Status** — Indicates the device PoE mode. The possible field values are:
  - *Auto* — Enables the Device Discovery protocol, and provides power to the device using the PoE module. The Device Discovery Protocol enables the device to discover Powered Devices attached to the device interfaces, and to

learn their classification. This is the default setting.

- *Never* — Disables the Device Discovery protocol, and stops the power supply to the device using the PoE module.

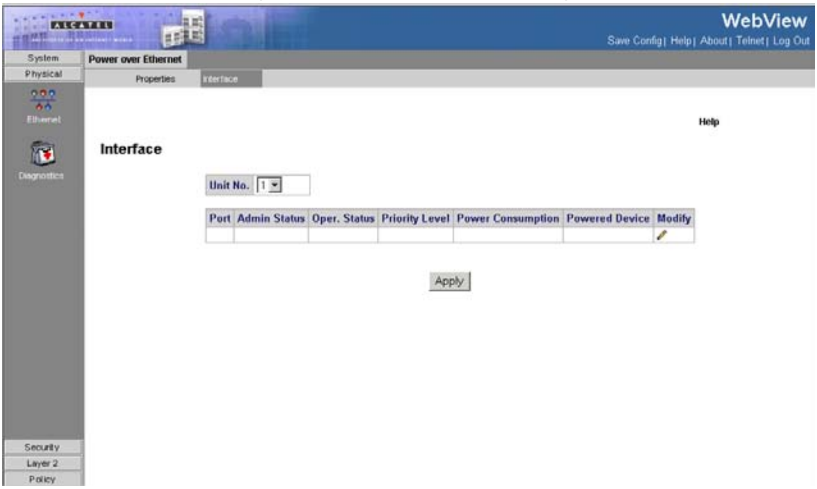
- **Oper. Status** — Indicates if the port is enabled to work on PoE. The possible field values are:
  - *On* — Indicates the device is delivering power to the interface.
  - *Off* — Indicates the device is not delivering power to the interface.
  - *Test Fail* —Indicates the powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.
  - *Testing* — Indicates the powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.
  - *Searching* — Indicates that the device is currently searching for a powered device. Searching is the default PoE operational status.
  - *Fault* — Indicates that the device has detected a fault on the powered device. For example, the powered device memory could not be read.
- **Priority Level** — Determines the port priority if the power supply is low. The port power priority is used if the power supply is low. The field default is low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 is prioritized to receive power, and port 3 may be denied power. The possible field values are:
  - *Low* — Defines the PoE priority level as low.
  - *High* — Defines the PoE priority level as high.
  - *Critical* — Defines the PoE priority level as Critical. This is the highest PoE priority level.
- **Power Consumption** — Indicates the amount of power assigned to the powered device connected to the selected interface. The possible field values are:

Class	Usage	Min. power level at PSE output
0	Default	15.4 watt
1	Optional	4.0 watt
2	Optional	7.0 watt
3	Optional	15.4 watt
4	Reserved	As class 0

- **Powered Device** — Provides a user-defined powered device description. The field can contain up to 24 characters.

Web – Click Physical, Ethernet, Power over Ethernet, Interface page. Define the fields and click Apply.

Figure 3-65. PoE Interface Page



Interface

Unit No. 1

Port	Admin Status	Oper. Status	Priority Level	Power Consumption	Powered Device	Modify
						✎

CLI – The following is an example PoE interface commands:

```
Console(config)# interface ethernet 1/e1
4-376
Console(config)# power inline auto
4-460
Console(config)# power inline powered-device IP phone
4-461
Console(config)# power inline priority high
4-462
```

Device Diagnostic Tests

This section contains information for configuring port mirroring, running cable tests, and viewing device operational information, and includes the following topics:

- Configuring Port Mirroring
- Viewing Integrated Cable Tests
- Viewing Optical Transceivers
- Viewing Device Health

Configuring Port Mirroring

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as a diagnostic tool as well as a debugging feature. Port mirroring also enables switch performance monitoring.

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

When configuring port mirroring, ensure the following:

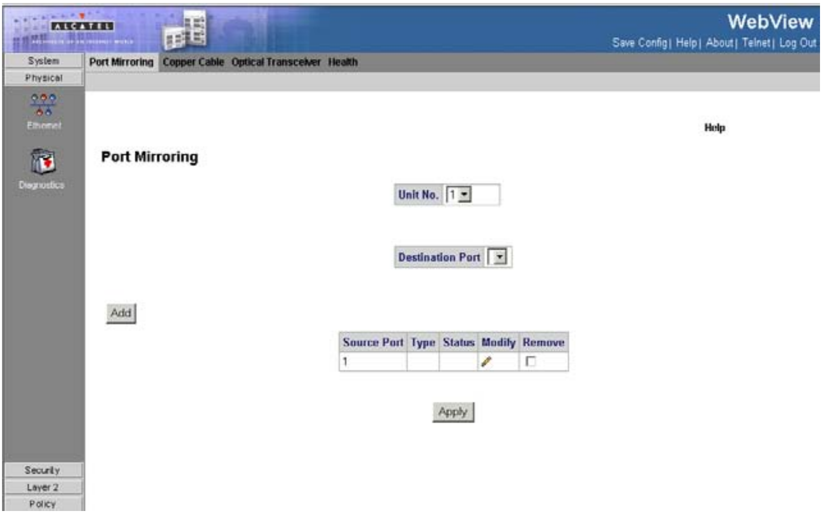
- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

The *Port Mirroring Page* contains parameters for monitoring and mirroring of network traffic.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the port mirroring configuration information is displayed.
- **Destination Port** — Defines the port number to which port traffic is copied.
- **Source Port** — Indicates the port from which the packets are mirrored.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
  - *CopyRXOnly* — Defines the port mirroring on receiving ports.
  - *CopyTXOnly* — Defines the port mirroring on transmitting ports.
  - *CopyBoth* — Defines the port mirroring on both receiving and transmitting ports. This is the default value.
- **Status** — Indicates if the port is currently monitored. The possible field values are:
  - *Active* — Indicates the port is currently monitored.
  - *notReady* — Indicates the port is not currently monitored.
- **Remove** — Removes the port mirroring session. The possible field values are:
  - *Checked* — Removes the selected port mirroring sessions.
  - *Unchecked* — Maintains the port mirroring session.

Web – Click Physical, Diagnostics, Port Mirroring. Specify the source port, the traffic type to be mirrored, and the destination port, then click Add.



Port Mirroring

Unit No. 1

Destination Port

Source Port	Type	Status	Modify	Remove
1			✎	□

Figure 3-66. Port Mirroring Page

CLI – The following is an example of the Port Mirroring CLI commands:

```
Console(config)# interface ethernet 1/e1
4-376
Console(config-if)# port monitor 1/e8
4-458
```

Viewing Integrated Cable Tests

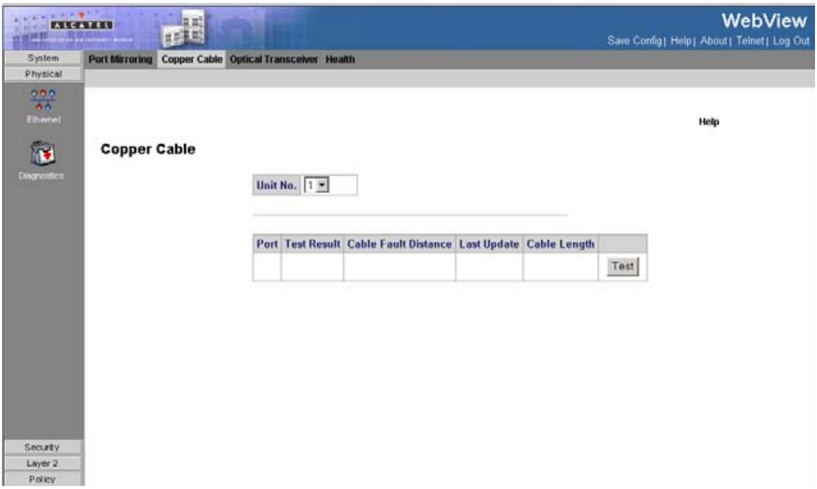
The *Copper Cable Page* contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error, which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test. To test cables:

Command Attributes

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Port** — Specifies the port to which the cable is connected.
- **Test Result** — Displays the cable test results. Possible values are:
  - *No Cable* — Indicates that a cable is not connected to the port.
  - *Open Cable* — Indicates that a cable is connected on only one side.
  - *Short Cable* — Indicates that a short has occurred in the cable.

  - *OK* — Indicates that the cable passed the test.
- **Cable Fault Distance** — Indicates the distance from the port where the cable error occurred.
- **Last Update** — Indicates the last time the port was tested.
- **Cable Length** — Indicates the approximate cable length. This test can only be performed when the port is up.

Web – Click Physical, Diagnostics, Copper Cable, define the fields, and click Test.



Copper Cable

Unit No. 1

Port	Test Result	Cable Fault Distance	Last Update	Cable Length

Figure 3-67. Copper Cable Page

CLI – The following is an example of the CLI commands used to test copper cables:

```
Console# show copper-ports cable-length
4-452


Port      Length [meters]

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

1/e1      < 50

1/e2      Copper not active

1/e3      110-140

1/g1      Fiber
```

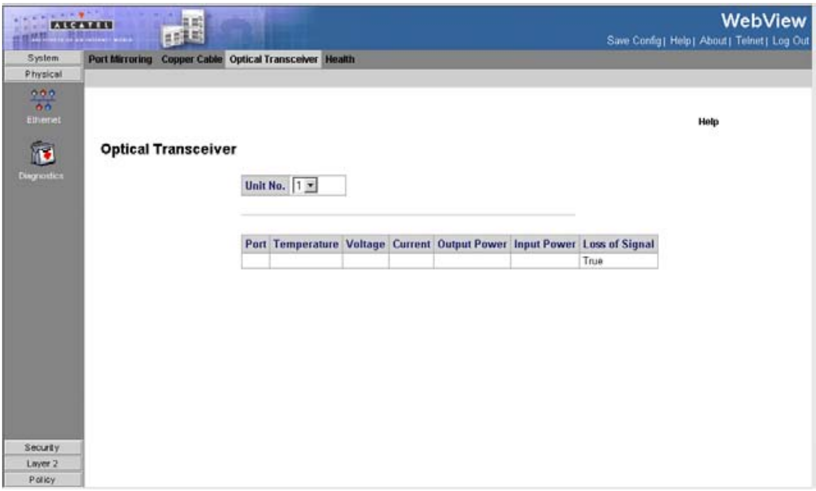
Viewing Optical Transceivers

The *Optical Transceiver Page* allows network managers to perform tests on Fiber Optic cables. Optical transceiver diagnostics can be performed only when the link is present.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Port** — Displays the IP address of the port on which the cable is tested.
- **Temperature** — Displays the temperature (C) at which the cable is operating.
- **Voltage** — Displays the voltage (V) at which the cable is operating.
- **Current** — Displays the current (mA) at which the cable is operating.
- **Output Power** — Indicates the rate (mW) at which the output power is transmitted.
- **Input Power** — Indicates the rate (mW) at which the input power is transmitted.
- **Transmitter Fault** — Indicates if a fault occurred during transmission.
- **Loss of Signal** — Indicates if a signal loss occurred in the cable.
- **Data Ready** — Indicates the transceiver has achieved power up and data is ready.

Web – Click Physical, Diagnostics, Optical Transceivers.



Optical Transceiver

Unit No. 1

Port	Temperature	Voltage	Current	Output Power	Input Power	Loss of Signal
						True

Figure 3-68. Optical Transceiver Page

CLI – The following is an example of the CLI commands used to fiber cables:

```
Console# show fiber-ports optical-transceiver
4-453
```

	Power
Port	Temp Voltage Current Output Input TX Fault LOS

----	----	-------	-------	------	-----	-------	---
1/g1	W	OK	E	OK	OK	OK	OK
1/g2	OK	OK	OK	OK	OK	E	OK
1/g3	Copper						

```
Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power.
Input Power – Measured RX  received power.
Tx Fault – Transmitter fault
LOS – Loss of signal
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

Viewing Device Health

The *Health Page* displays physical device information, including information about the device’s power and ventilation sources.

Command Attributes

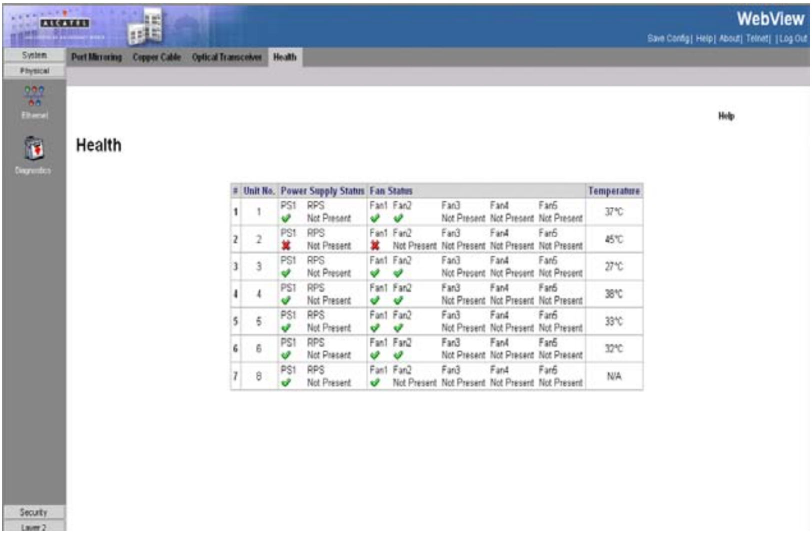
- **Unit No.** — Indicates the stacking member for which the device information is displayed.
- **Power Supply Status** — The power supply status. The device has two power supplies. Power supply 1 is displayed as PS1 in the interface, while the redundant power supply is displayed as RPS. The possible field values are:
  - *Checked* — The power supply is operating normally.
  - *Unchecked* —The power supply is not operating normally.
  - *Not Present* —The power supply is currently not present.
- **Fan Status** — The fan status. The number of fans on the boards is provided based on the device type (number of ports) and PoE chips availability. Each fan is denoted as fan plus the fan number in the interface. The possible field values are:
  - *Checked* — The fan is operating normally.
  - *Unchecked* — The fan is not operating normally.
  - *Not Present* — A fan is currently not present.
- **Temperature** — The temperature at which the device is currently running. The device temperature is displayed in Celsius. The device temperature threshold is 0-40 C (32-104F). The following table displays the temperature in Fahrenheit in increments of 5:

Table 1: Celsius to Fahrenheit Conversion Table

Celsius	Fahrenheit
0	32
5	41

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

Web – Click Physical, Diagnostics, Health.



Health

#	Unit No.	Power Supply Status		Fan Status					Temperature
1	1	PS1 ✓	RPS Not Present	Fan1 ✓	Fan2 ✓	Fan3 Not Present	Fan4 Not Present	Fan5 Not Present	37°C
2	2	PS1 ✗	RPS Not Present	Fan1 ✗	Fan2 Not Present	Fan3 Not Present	Fan4 Not Present	Fan5 Not Present	45°C
3	3	PS1 ✓	RPS Not Present	Fan1 ✓	Fan2 ✓	Fan3 Not Present	Fan4 Not Present	Fan5 Not Present	27°C
4	4	PS1 ✓	RPS Not Present	Fan1 ✓	Fan2 ✓	Fan3 Not Present	Fan4 Not Present	Fan5 Not Present	38°C
5	5	PS1 ✓	RPS Not Present	Fan1 ✓	Fan2 ✓	Fan3 Not Present	Fan4 Not Present	Fan5 Not Present	33°C
6	6	PS1 ✓	RPS Not Present	Fan1 ✓	Fan2 ✓	Fan3 Not Present	Fan4 Not Present	Fan5 Not Present	32°C
7	8	PS1 ✓	RPS Not Present	Fan1 ✓	Fan2 Not Present	Fan3 Not Present	Fan4 Not Present	Fan5 Not Present	N/A

Figure 3-69. Health Page

CLI – The following is an example of the device Health CLI commands:

```
Console# show system
4-618


Unit                 Type

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

1                    Alcatel
```

```
Unit             Main Power Supply         Redundant Power Supply
----             -----------------         ----------------------
1                OPERATIONAL               NOT OPERATIONAL


Unit             Fan1              Fan2     Fan3     Fan4         Fan5
----             ----              ----     ----     ----         ----
1                OK                OK       OK       OK           OK
```

Configuring Traffic Control

This section contains information for managing both port security and storm control, and includes the following topics:

- Enabling Storm Control
- Configuring Port Security

Enabling Storm Control

Storm control limits the amount 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 on all ports.

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

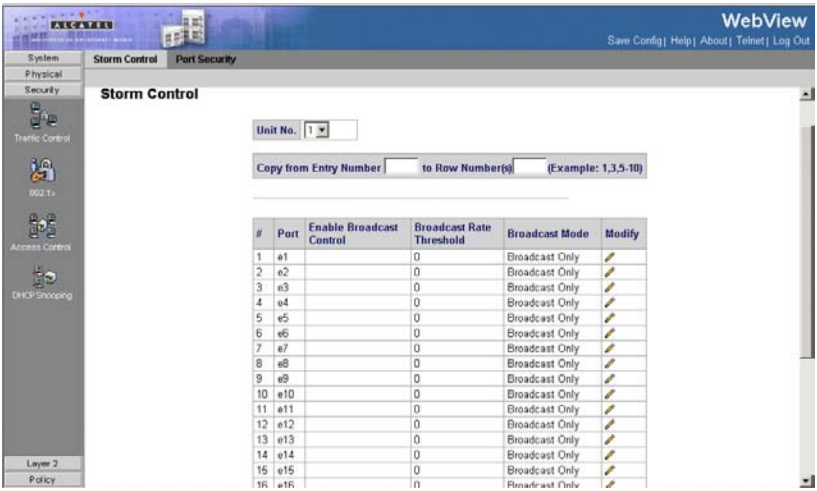
You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped. The *Storm Control Page* provides fields for configuring broadcast storm control.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the Storm Control information is displayed.
- **Copy From Entry Number** — Copies Storm Control information from the selected port.
- **To Row Number(s)** — Copies Storm Control information to the selected ports.
- **Port** — Indicates the port from which storm control is enabled or disabled.
- **Enable Broadcast Control —** Indicates if Broadcast packet types may be forwarded on the interface. The possible values are:
  - *Enabled* — Broadcast Control is enabled on the port.
  - *Disabled* — Broadcast Control is not enabled on the port.

- **Broadcast Rate Threshold** — The maximum rate (kilobits per second) at which unknown packets are forwarded. Rate limitations are as follows:
  - The range for FE ports is 70 - 100000. Default is 3500.
  - The range for GE ports is 3500 - 1000000.
  - The default value is 3500.
- **Broadcast Mode —** Specifies the Broadcast mode currently enabled on the device or stack. The possible field values are:
  - *Broadcast Only* — Counts only Broadcast traffic.
  - *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.

Web – Click Security, Traffic Control, Storm Control, define the fields, and click Apply.



Storm Control

Unit No. 1

Copy from Entry Number ____ to Row Number(s) ____ (Example: 1,3,5-10)

#	Port	Enable Broadcast Control	Broadcast Rate Threshold	Broadcast Mode	Modify
1	e1		0	Broadcast Only	✎
2	e2		0	Broadcast Only	✎
3	e3		0	Broadcast Only	✎
4	e4		0	Broadcast Only	✎
5	e5		0	Broadcast Only	✎
6	e6		0	Broadcast Only	✎
7	e7		0	Broadcast Only	✎
8	e8		0	Broadcast Only	✎
9	e9		0	Broadcast Only	✎
10	e10		0	Broadcast Only	✎
11	e11		0	Broadcast Only	✎
12	e12		0	Broadcast Only	✎
13	e13		0	Broadcast Only	✎
14	e14		0	Broadcast Only	✎
15	e15		0	Broadcast Only	✎
16	e16		0	Broadcast Only	✎

Figure 3-70. Storm Control Page

CLI – The following is an example of the Storm Control CLI commands:

```
Console# configure
Console(config)# port storm-control include-multicast
4-395
Console(config)# interface ethernet 2/e3
4-376
Console(config-if)# port storm-control include-multicast
4-395
Console(config-if)# port storm-control broadcast enable
4-395
Console(config-if)# port storm-control broadcast rate 900
4-396
```

Configuring Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned or statically configured. 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 up to the point when it is locked. When a packet is received on a locked port, and the packet source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving at a locked port are either:

- Forwarded
- Discarded with no trap
- Discarded with a trap
- The port is shut down

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

When port security by MAC address is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security by MAC address, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the source MAC address, VLAN pair for frames received on the port. Note that you can also manually add secure addresses to the port using the Static Address Table. When the port has reached the maximum number of MAC addresses the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch. Disabled ports are activated from the *Port Security Page*.

Ensure the following when configuring port security:

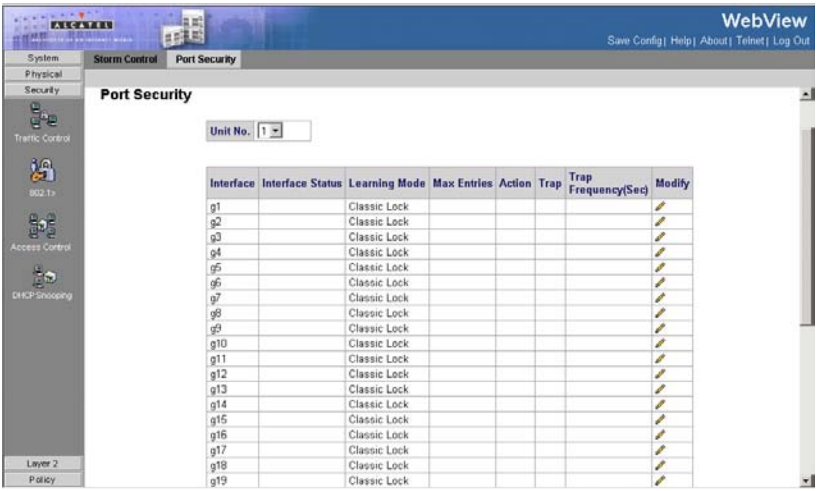
- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.
- Configure a maximum address count for the port to allow access.
- The device supports the range of 1-128 MAC addresses on a locked port.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the port security information is displayed.

- **Interface** — Indicates the port or LAG number.
- **Interface Status** — Indicates if the interface is locked or unlocked.
- **Learning Mode** — Defines the locked interface mode. The Learning Mode field is enabled only if Locked is selected in the Set Port field. The possible field values 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 current 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** — Specifies the number of MAC address that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Set Port field. In addition, the Limited Dynamic Lock mode is selected. The default is 1.
- **Action** — Defines the action to be applied to packets arriving on a locked port. The possible field values are:
  - *Forward* — Forwards packets from an unknown source without learning the MAC address.
  - *Discard* — Discards packets from any unlearned source. This is the default value.
  - *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Trap** — Enables traps when a packet is received on a locked port. The possible field values are:
  - *Checked (True)*— Enables traps.
  - *Unchecked (False)* — Disables traps.
- **Trap Frequency (Sec)** — Defines the amount of time (in seconds) between traps. The default value is 10 seconds.

Web – Click Security, Traffic Control, Port Security. Define the fields and click Apply.



Port Security

Unit No. 1

Interface	Interface Status	Learning Mode	Max Entries	Action	Trap	Trap Frequency(Sec)	Modify
g1		Classic Lock					✎
g2		Classic Lock					✎
g3		Classic Lock					✎
g4		Classic Lock					✎
g5		Classic Lock					✎
g6		Classic Lock					✎
g7		Classic Lock					✎
g8		Classic Lock					✎
g9		Classic Lock					✎
g10		Classic Lock					✎
g11		Classic Lock					✎
g12		Classic Lock					✎
g13		Classic Lock					✎
g14		Classic Lock					✎
g15		Classic Lock					✎
g16		Classic Lock					✎
g17		Classic Lock					✎
g18		Classic Lock					✎
g19		Classic Lock					✎

Figure 3-71. Port Security Page

CLI – The following is an example of the Port Security CLI commands:

```
Console(config)# interface ethernet 1/e1                      4-376
Console(config-if)# port security forward trap 100            4-321
Console(config-if)# port security mode                        4-321
Console(config-if)# port security max 20                      4-322
```

802.1X Port-Based Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1x (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

Port-based authentication authenticates 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-based authentication includes:

- **Authenticators** — Specifies the device port which is authenticated before permitting system access.

- **Supplicants** — Specifies the host connected to the authenticated port requesting to access the system services.
- **Authentication Server** — Specifies the server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server.

The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

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 state.

The device currently supports port-based authentication via RADIUS servers.

Advanced Port-Based Authentication

Advanced port-based authentication enables multiple hosts to be attached to a single port. Advanced port-based authentication requires only one host to be authorized for all hosts to have system access. If the port is unauthorized, all attached hosts are denied access to the network.

Advanced port-based authentication also enables user-based authentication. Specific VLANs in the device are always available, even if specific ports attached to the VLAN are unauthorized. For example, Voice over IP does not require authentication, while data traffic requires authentication. VLANs for which authorization is not required can be defined. Unauthenticated VLANs are available to users, even if the ports attached to the VLAN are defined as authorized.

Advanced port-based authentication is implemented in the following modes:

- **Single Host Mode** — Only the authorized host can access the port.
- **Multiple Host Mode** — Multiple hosts can be attached to a single port. Only one host must be authorized for all hosts 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 Sessions Mode** - Multiple sessions mode enables number of specific hosts that has been authorized to get access to the port. Filtering is based on the source MAC address.
- **Guest VLANs** — Provides limited network access to authorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network

administrator can use Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users.

- **Unauthenticated VLANS** — Are available to users, even if the ports attached to the VLAN are defined as unauthorized.

When configuring port based authentication, ensure the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- Each switch port must be set to dot1x “Auto” mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1x client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

Defining Network Authentication Properties

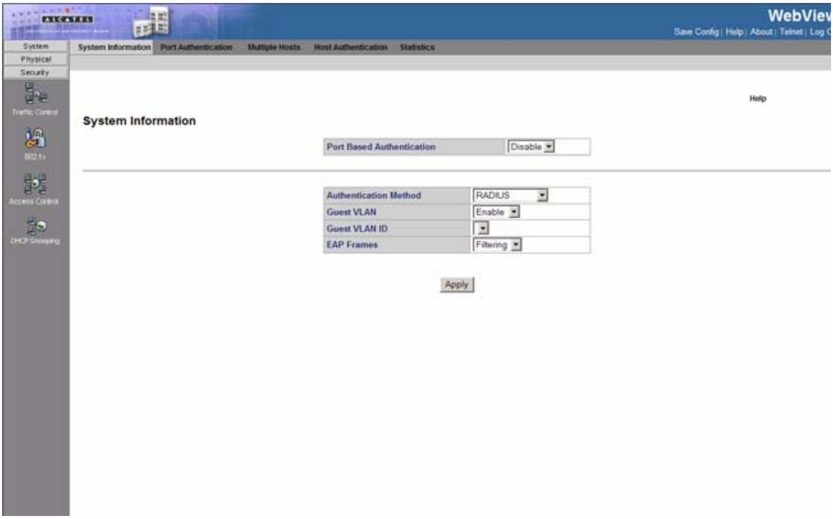
The *System Information Page* allows network managers to configure network authentication parameters. In addition, Guest VLANs are enabled from the *System Information Page*.

Command Attributes

- **Port-based Authentication** — Enables port-based authentication on the device. The possible field values are:
  - *Enable* — Enables port-based authentication on the device.
  - *Disable* — Disables port-based authentication on the device.
- **Authentication Method** — Specifies the authentication method used. The possible field values are:
  - *None* — No authentication method is used to authenticate the port.
  - *RADIUS* — Port authentication is performed via RADIUS server.
  - *RADIUS, None* — Port authentication is performed first via the RADIUS server. If no response is received from RADIUS (for example, if the server is down), then the *None* option is used, and the session is permitted.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  - *Enable* — Enables use of a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
  - *Disable* — Disables use of a Guest VLAN for unauthorized ports. This is the default.
- **Guest VLAN ID** — Contains a list of VLANs. The Guest VLAN is selected from the VLAN list.

- **EAP Frames** — Determines how EAP packets are managed when port based authentication is disabled on the device. EAP packets are used to transmit authentication information. The possible field values are:
  - *Filtering* — Filters EAP packets when port based authentication is disabled globally.
  - *Bridging* — Indicates that if the port based authentication is globally disabled, untagged and tagged EAP packets are flooded, and are subject to ingress and egress VLAN rules.

Web – Click Security, 802.1x, System Information.



System Information

Port Based Authentication	Disable

Authentication Method	RADIUS
Guest VLAN	Enable
Guest VLAN ID	
EAP Frames	Filtering

Figure 3-72. System Information Page

CLI – The following is an example of the device Authentication CLI commands:

```
Console(config)# dot1x system-auth-control
4-265
Console(config)# aaa authentication dot1x default none
4-264
```

Defining Port Authentication

The *Port Authentication Page* allows network managers to configure port-based authentication parameters.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the Port authentication information is displayed.
- **Copy From Entry Number** — Copies port authentication information from the selected port.
- **To Entry Number(s)** — Copies port authentication information to the selected port.
- **Port** — Displays a list of interfaces on which port-based authentication is enabled.
- **User Name** — Displays the supplicant user name.
- **Current Port Control** — Displays the current port authorization state.
  - *Unauthorized* — Indicates that the port control is ForceUnauthorized, 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* — Indicates that the port control is ForceAuthorized, and clients have full port access.
  - *Single-host Lock* — Indicates that the port control is Auto, and a single client has been authenticated via the port.
  - *No Single Host* — Indicates that Multiple Host is enabled.
- **Guest VLAN** — Indicates the VLAN number of the Guest VLAN. If Guest VLAN is not configured, the value is “Disabled”.
- **Authentication Methods** — Defines the user authentication methods. MAC authentication ensures that end-user stations meet security policies criteria, and protects networks from viruses. MAC authentication is active when the **Admin Port Control** option is set to Auto in the Modify Port Authentication page.
  - *802.1X Only* – Enables only 802.1X authentication on the device.
  - *MAC Only* — Enables only MAC authentication on the device.
  - *MAC + 802.1X* – Enables MAC Authentication + 802.1X authentication on the device. In case of MAC+ 802.1x, 802.1x takes precedence.
- **Periodic Reauthentication** — Permits immediate port reauthentication. The possible field values are:
  - *Enable* — Enables immediate port reauthentication. This is the default value.
  - *Disable* — Disables port reauthentication.
- **Reauthentication Period** — Displays the time span (in seconds) in which the selected port is reauthenticated. The field default is 3600 seconds.
- **Reauthenticate Now** — Reauthenticates the selected ports immediately. Click Select All to select all ports for reauthentication.
- **Authenticator State** — Displays the current authenticator state.

- **Quiet Period** — Displays the number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.
- **Resending EAP** — Defines the amount of time (in seconds) that lapses before EAP requests are resent. The field default is 30 seconds.
- **Max EAP Requests** — Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
- **Supplicant Timeout** — Displays the amount of time (in seconds) that lapses before EAP requests are resent to the supplicant. The field default is 30 seconds.
- **Server Timeout** — Displays the amount of time (in seconds) that lapses before the device re-sends a request to the authentication server. The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

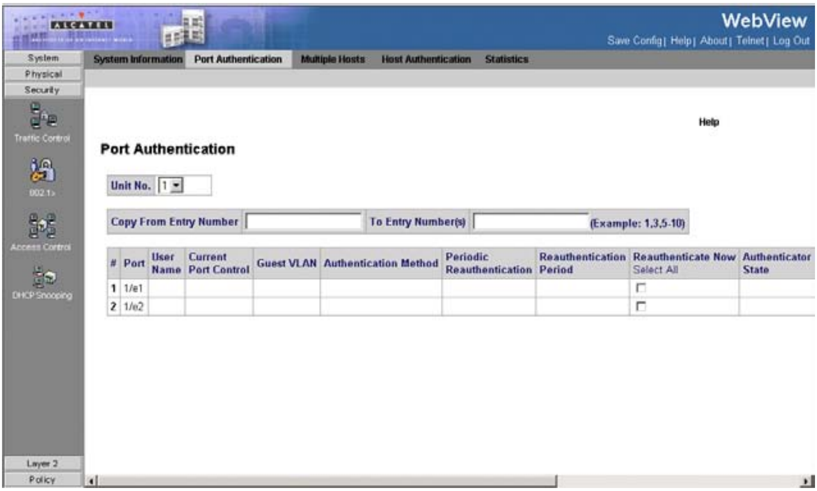
Modify Port Authentication Page

The *Modify Port Authentication Page* contains the following fields:

- **Port** — Displays a list of interfaces on which port-based authentication is enabled.
- **User Name** — Displays the supplicant user name.
- **Admin Port Control** — Displays the current port authorization state. The possible field values are:
  - *Auto* — Enables port-based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  - *ForceAuthorized* — Indicates the interface is in an authorized state without being authenticated. The interface re-sends and receives normal traffic without client port-based authentication.
  - *ForceUnauthorized* — 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 Port Control** — Displays the current port authorization state.
  - *Unauthorized* — Indicates that the port control is ForceUnauthorized, 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* — Indicates that the port control is ForceAuthorized, and clients have full port access.
  - *Single-host Lock* — Indicates that the port control is Auto, and a single client has been authenticated via the port.
- **Enable Guest VLAN** — Enables access to Guest VLAN.
  - *Checked* — Indicates that Guest VLAN is enabled.
  - *Unchecked* — Indicates that Guest VLAN is disabled.
- **Authentication Methods** — Defines the user authentication methods:

  - *802.1X Only* – Enables only 802.1X authentication on the device.
  - *MAC Only* — Enables only MAC authentication on the device.
  - *MAC + 802.1X* – Enables MAC Authentication + 802.1X authentication on the device.
- **Periodic Reauthentication** — Permits immediate port reauthentication. The possible field values are:
  - *Enable* — Enables immediate port reauthentication. This is the default value.
  - *Disable* — Disables port reauthentication.
- **Reauthenticate Now** — Reauthenticates the selected ports immediately. Select All selects all ports for reauthentication.
- **Authenticator State** — Displays the current authenticator state.
- **Quiet Period** — Displays the number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.
- **Resending EAP** — Defines the amount of time (in seconds) that lapses before EAP requests are resent. The field default is 30 seconds.
- **Max EAP Requests** — Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
- **Supplicant Timeout** — Displays the amount of time (in seconds) that lapses before EAP requests are resent to the supplicant. The field default is 30 seconds.
- **Server Timeout** — Displays the amount of time (in seconds) that lapses before the device re-sends a request to the authentication server. The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

Web – Click Security, 802.1x, Port Authentication, define the fields, and click Apply.



Port Authentication

Unit No. 1

Copy From Entry Number | To Entry Number(s) | (Example: 1,3,5-10)

#	Port	User Name	Current Port Control	Guest VLAN	Authentication Method	Periodic Reauthentication	Reauthentication Period	Reauthenticate Now Select All	Authenticator State
1	1/e1							□	
2	1/e2							□	

Figure 3-73. Port Authentication Page

CLI – The following is an example of the Port Authentication CLI commands:

```
Console# dot1x re-authenticate ethernet 1/e16
4-267
Console(config)# interface ethernet 1/e16                          4-376
Console(config-if)# dot1x port-control auto
4-266
Console(config-if)# dot1x re-authentication
4-267
Console(config-if)# dot1x timeout re-authperiod 300
4-268
Console(config-if)# dot1x timeout quiet-period 3600                4-269
Console(config-if)# dot1x timeout tx-period 3600
4-270
Console(config-if)# dot1x max-req 6
4-271
Console(config-if)# dot1x timeout supp-timeout 3600
4-272
Console(config-if)# dot1x timeout server-timeout 3600
4-273
```

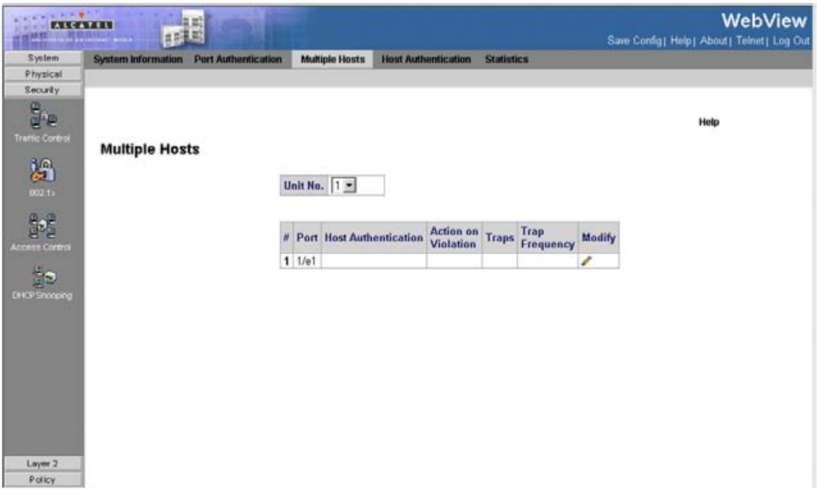
Configuring Multiple Hosts

The *Multiple Hosts Page* allows network managers to configure advanced port-based authentication settings for specific ports and VLANs.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the Multiple Hosts information is displayed.

- **Port** — Displays the port number for which advanced port-based authentication is enabled.
- **Host Authentication**— Indicates the Host Authentication mode. The possible field values are:
  - *Single Host Mode* — Only the authorized host can access the port.
  - *Multiple Host Mode* — Multiple hosts can be attached to a single 802.1x-enabled port. Only one host must be authorized for all hosts 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 Sessions Mode* - “Multiple sessions” mode enables number of specific hosts that has been authorized to get access to the port. Filtering is based on the source MAC address.
- **Action on Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
  - *Forward* — Forwards the packet.
  - *Discard* — Discards the packets. This is the default value.
  - *DiscardDisable* — Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the device is reset.
- **Traps** — Indicates if traps are enabled for Multiple Hosts. The possible field values are:
  - *Enabled* — Indicates that traps are enabled for Multiple hosts.
  - *Disabled* — Indicates that traps are disabled for Multiple hosts.
- **Trap Frequency** — Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.
- **Web** – Click Security, 802.1x, Multiple Hosts, define the fields, and click Apply.



Multiple Hosts

Unit No. 1

#	Port	Host Authentication	Action on Violation	Traps	Trap Frequency	Modify
1	1/e1					✎

Figure 3-74. Multiple Hosts Page

CLI – The following is an example of the Multiple Hosts CLI commands:

```
Console(config-if)# dot1x multiple-hosts
4-282
Console(config-if)# dot1x single-host-violation forward trap 100

4-283
```

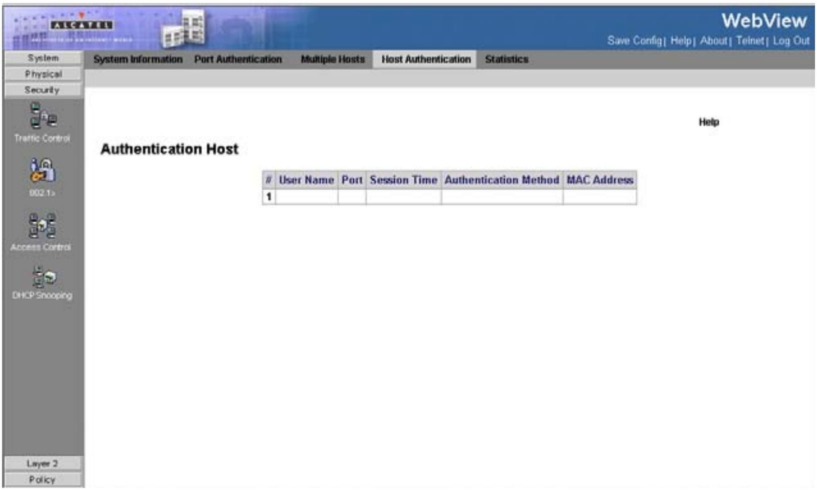
Defining Authentication Hosts

The *Authentication Host Page* contains a list of authenticated users.

Command Attributes

- **User Name** — Lists the supplicants that were authenticated, and are permitted on each port.
- **Port** — Displays the port number.
- **Session Time** — Displays the amount of time (in seconds) the supplicant was logged on the port.
- **Authentication Method** — Displays the method by which the last session was authenticated. The possible field values are:
  - *Remote* — 802.1x authentication is not used on this port (port is forced-authorized).
  - *None* — The supplicant was not authenticated.
  - *RADIUS* — The supplicant was authenticated by a RADIUS server.
- **MAC Address** — Displays the supplicant MAC address.

Web – Click Security, 802.1x, Authentication Host. Define the fields and click Apply.



Authentication Host

#	User Name	Port	Session Time	Authentication Method	MAC Address
1					

Figure 3-75. Authentication Host Page

CLI – The following is an example of the Authentication Host CLI commands:

```
Console# show dot1x
4-274



802.1x is enabled



Port      Admin Mode    Oper Mode      Reauth     Reauth     Username
                                       Control    Period

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

1/e1      Auto          Authorized     Ena        3600       Bob

1/e2      Auto          Authorized     Ena        3600       John

1/e3      Auto          Unauthorized   Ena        3600       Clark

1/e4      Force-auth    Authorized     Dis        3600       n/a

1/e5      Force-auth    Unauthorized   Dis        3600       n/a
                        *



* Port is down or not present.
```

```
Console# show dot1x ethernet 1/e3
4-274


802.1x is enabled.


Port     Admin Mode    Oper Mode      Reauth     Reauth     Username
                                      Control    Period

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

1/e3     Auto          Unauthorized   Ena        3600       Clark


Quiet period: 60 Seconds

Tx period:30 Seconds

Max req: 2

Supplicant timeout: 30 Seconds

Server timeout: 30 Seconds

Session Time (HH:MM:SS): 08:19:17

MAC Address: 00:08:78:32:98:78

Authentication Method: Remote

Termination Cause: Supplicant logoff


Authenticator State Machine

State: HELD


Backend State Machine

State: IDLE

Authentication success: 9

Authentication fails: 1
```

Viewing EAP Statistics

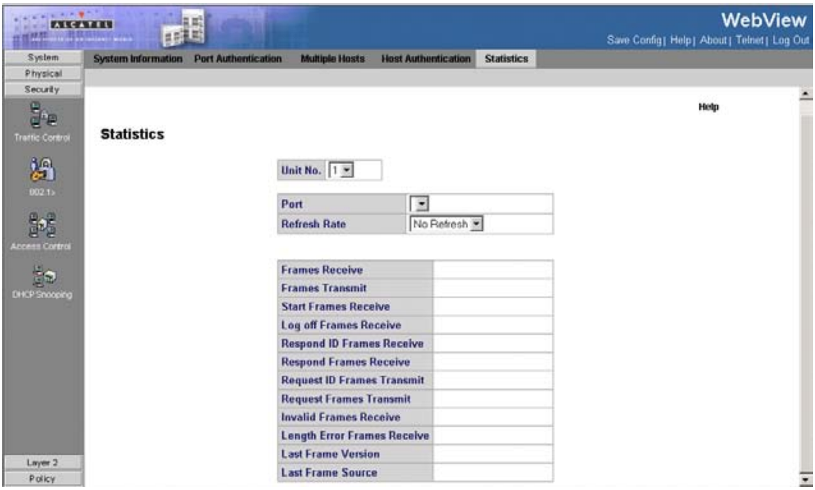
The *Statistics Page* contains information about EAP packets received on a specific port.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the received EAP packets information is displayed.
- **Port** — Indicates the port, which is polled for statistics.

- **Refresh Rate** — Indicates the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
  - *15 Sec* — Indicates that the EAP statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the EAP statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the EAP statistics are refreshed every 60 seconds.
  - *No Refresh* — Indicates that the EAP statistics are not refreshed.
- **Frames Receive** — Indicates the number of valid EAPOL frames received on the port.
- **Frames Transmit** — Indicates the number of EAPOL frames transmitted via the port.
- **Start Frames Receive** — Indicates the number of EAPOL Start frames received on the port.
- **Log off Frames Receive** — Indicates the number of EAPOL Logoff frames that have been received on the port.
- **Respond ID Frames Receive** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Respond Frames Receive** — Indicates the number of valid EAP Response frames received on the port.
- **Request ID Frames Transmit** — Indicates the number of EAP Req/Id frames transmitted via the port.
- **Request Frames Transmit** — Indicates the number of EAP Request frames transmitted via the port.
- **Invalid Frames Receive** — Indicates the number of unrecognized EAPOL frames that have been received by on this port.
- **Length Error Frames Receive** — Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frame Version** — Indicates the protocol version number attached to the most recently received EAPOL frame.
- **Last Frame Source** — Indicates the source MAC address attached to the most recently received EAPOL frame.

Web – Click Security, 802.1x, Statistics and select an interface.



Statistics

Unit No.	1
Port	
Refresh Rate	No Refresh
Frames Receive	
Frames Transmit	
Start Frames Receive	
Log off Frames Receive	
Respond ID Frames Receive	
Respond Frames Receive	
Request ID Frames Transmit	
Request Frames Transmit	
Invalid Frames Receive	
Length Error Frames Receive	
Last Frame Version	
Last Frame Source	

Figure 3-76. Statistics Page

CLI – The following is an example of the 802.1X Statistics CLI commands:

```
Console# show dot1x statistics ethernet 1/e1
4-279



EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 12

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 00:08:78:32:98:78
```

Defining Access Control Lists

Access Control Lists (ACL) provide packet filtering for IP frames and MAC addresses. 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. To filter incoming packets, first create an access list, add the required rules, specify a priority to modify the precedence in which the rules are checked, and then bind the list to a specific port.

For example, an ACL rule is defined that states, 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 made of the filters that determine traffic classifications. The total number of ACEs that can be defined in all ACLs together is 894.

Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted. The following filters can be defined as ACEs:

- **Source Port IP Address and Wildcard Mask** — Filters the packets by the Source port IP address and wildcard mask.
- **Destination Port IP Address and Wildcard Mask** — Filters the packets by the Source port IP address and wildcard mask.
- **ACE Priority** — Filters the packets by the ACE priority.
- **Protocol** — Filters the packets by the IP protocol.
- **DSCP** — Filters the packets by the DiffServ Code Point (DSCP) value.
- **IP Precedence** — Filters the packets by the IP Precedence.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding.

When configuring ACLs, ensure the following:

- Each ACL can have up to 256 Access Control Elements (ACE rules).
- The maximum number of ACLs is 894 per port.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.

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

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

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

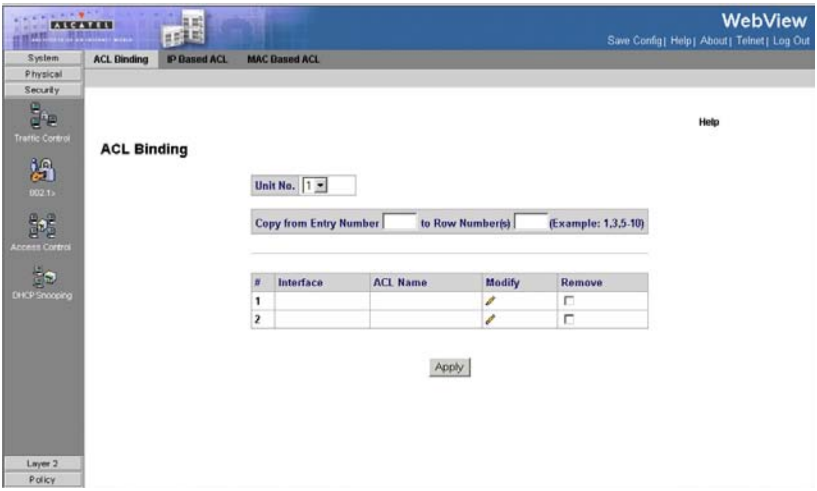
Binding Device Security ACLs

When an ACL is bound to an interface, all the ACE rules that have been defined are applied to the selected interface. Whenever an ACL is assigned on a port or trunk from that ingress interface that do not match the ACL are matched to the default rule, which is Drop unmatched packets. The *ACL Binding Page* binds ACLs to interfaces.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Copy from Entry Number** — Copies the ACL information from the defined interface.
- **To Entry Number(s)** — Copies the ACL information to the defined interface.
- **Interface** — Indicates the interface to which the ACL is bound.
- **ACL Name** — Indicates the ACL which is bound the interface.
- **Remove** — Unbinds the selected ACL from the interface. The possible field values are:
  - *Checked* — Unbinds the ACL and interface.
  - *Unchecked* — Maintains the ACL and interface binding.

Web – Click Security, Access Control, ACL Binding, define the fields, and click Apply.



ACL Binding

Unit No. 1

Copy from Entry Number ___ to Row Number(s) ___ (Example: 1,3,5-10)

#	Interface	ACL Name	Modify	Remove
1			✎	□
2			✎	□

Figure 3-77. ACL Binding Page

CLI – The following is an example of the IP Based ACL CLI commands:

```
Console(config)# ipaccess-list ip-acl1
4-300
Console(config-ip-al)#
```

Defining IP Based Access Control Lists

The *IP Based ACL Page* contains information for defining IP Based ACLs, including defining the ACEs defined for IP Based ACLs.

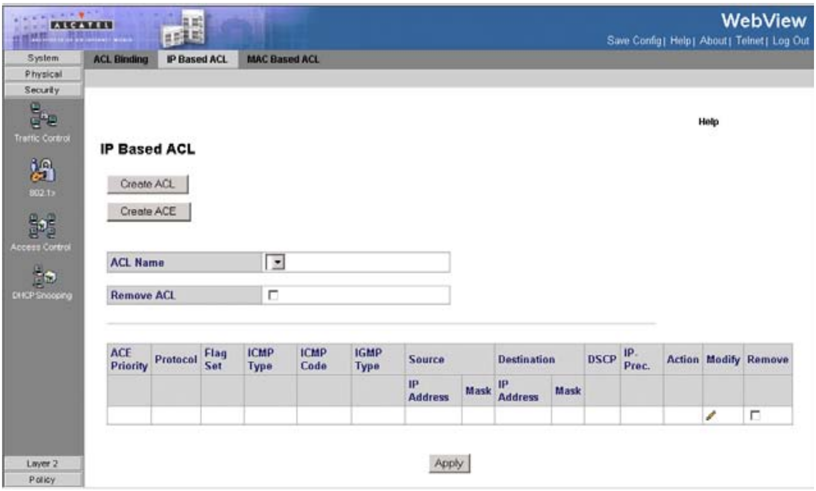
Command Attributes

- **ACL Name** — Displays the user-defined IP based ACLs.
- **Remove ACL** — Removes the IP based ACLs. The possible field values are:
  - *Checked* — Removes the selected IP based ACL.
  - *Unchecked* — Maintains the IP based ACLs.
- **ACE Priority** — Indicates the ACE priority that determines which ACE is matched to a packet based on a first-match basis. The possible field value is 1-2147483647.
- **Protocol** — Creates an ACE based on a specific protocol.
  - *Select from List* — Selects a protocol from a list on which ACE can be based. Some of the possible field values are:
    - **Any** — Matches the protocol to any protocol.
    - **IDRP** — Matches the packet to the *Inter-Domain Routing Protocol* (IDRP).
    - **RSVP** — Matches the packet to the *ReSerVation Protocol* (RSVP).
    - **PIM** — Matches the packet to *Protocol Independent Multicast* (PIM).

        - **L2IP**— Matches the packet to *Layer 2 Internet Protocol* (L2IP).
    - *Protocol ID* — Adds user-defined protocols by which packets are matched to the ACE. Each protocol has a specific protocol number which is unique. The possible field range is 0-255.
- **Flag Set** — Displays the TCP flag that is triggered.
- **ICMP Type** — Specifies an ICMP message type for filtering ICMP packets.
- **ICMP Code** — Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP Type** — Displays the IGMP message type. IGMP packets can be filtered by IGMP message type.
- **Source IP Address** — Matches the source IP address, to which packets are addressed to the ACE.
- **Source Mask** — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card 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. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down menu. The possible field range is 0 - 65535.
    - *Dest. IP Address* — Matches the destination IP address, to which packets are addressed to the ACE.
    - *Mask* — Defines the destination IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card 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. For example, if the destination IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Match DSCP** — Matches the packet DSCP value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-63.
- **Match IP Precedence** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — The ACL forwarding action. Possible values are:
    - *Permit* — Forwards packets which meet the ACL criteria.
    - *Deny* — Drops packets which meet the ACL criteria.
    - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the Interface Configuration Page.
- **Remove** — If checked, remove the ACE.

Web – Click Security, Access Control, IP Based ACL, define the fields and click

Apply.



IP Based ACL

ACL Name

Remove ACL □

ACE Priority	Protocol	Flag Set	ICMP Type	ICMP Code	IGMP Type	Source		Destination		DSCP	IP. Prec.	Action	Modify	Remove
						IP Address	Mask	IP Address	Mask					
													✎	□

Figure 3-78. IP Based ACL Page

CLI – The following is an example of the IP Based ACLs CLI commands:

```
Console(config)# ipaccess-list ip-acl1
4-300
Console(config-ip-al)# permit rsvp 192.1.1.1 0.0.0.0 any dscp 56
4-304
Console(config-ip-al)# deny rsvp 192.1.1.1 0.0.0.255 any
4-304
```

Defining MAC Based Access Control Lists

The *MAC Based ACL Page* allows a MAC- based ACL to be defined. ACEs can be added only if the ACL is not bound to an interface.

Command Attributes

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **Remove ACL** — Removes the MAC based ACLs. The possible field values are:
  - *Checked* — Removes the selected MAC based ACL.
  - *Unchecked* — Maintains the MAC based ACLs.
- **Priority**— Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address** — Defines the source MAC address, to which packets are addressed to the ACE.
- **Source MAC Mask** — Defines the source MAC address wildcard mask. Wild cards are used to mask all or part of a source MAC address. Wild card masks specify

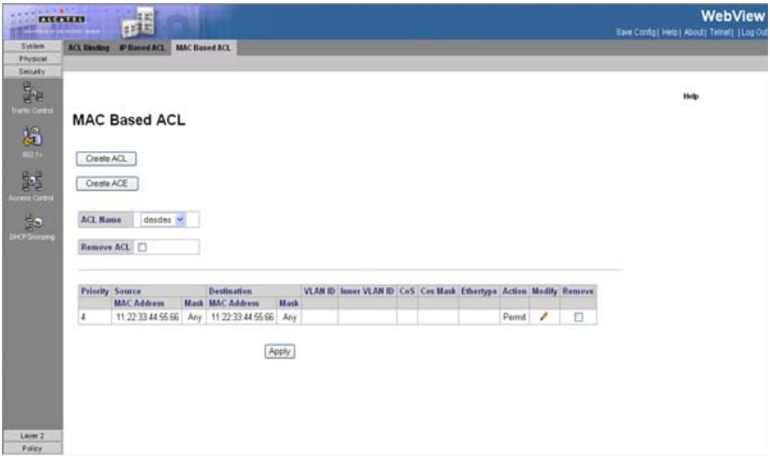
which bits are used and which are ignored. A wild card mask of FF:FF:FF:FF:FF:FF indicates that no bit is important. A wildcard of 00.00.00.00.00.00.00 indicates that all bits are important. For example, if the source MAC address is 00:AB:22:11:33:00 and the wildcard mask is 00:00:00:00:00:FF, the first two bits of the MAC are used, while the last two bits are ignored.

- **Destination MAC Address** — Matches the destination MAC address, to which packets are addressed to the ACE.
- **Destination MAC Mask** — Defines the destination MAC mask. Wild cards are used to mask all or part of a destination MAC address. Wild card masks specify which bits are used and which are ignored. A wild card mask of FF:FF:FF:FF:FF:FF indicates that no bit is important. A wildcard of 00.00.00.00.00.00.00 indicates that all bits are important. For example, if the source MAC address is 00:AB:22:11:33:00 and the wildcard mask is 00:00:00:00:00:FF, the first two bits of the MAC are used, while the last two bits are ignored.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **CoS** — Class of Service of the packet.
- **CoS Mask** — Wildcard bits to be applied to the CoS.
- **Ethertype** — The Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. Possible field values are:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the Interface Configuration Page.
- **Remove** — Removes MAC based ACLs. The possible field values are:
  - *Checked* — Removes the selected ACL.
  - *Unchecked* — Maintains the current MAC based ACLs.

Create ACL and *Create ACE* windows contain the additional following fields:

- **Rule Priority** — Value that specifies the rule priority.
- **Inner VLAN** — The inner VLAN ID of a double tagged packet.

Web – Click Security, Access Control, MAC Based ACL, and click Apply.



MAC Based ACL

ACL Name: desdes

Remove ACL ☐

Priority	Source		Destination		VLAN ID	Inner VLAN ID	CoS	Cos Mask	Ethertype	Action	Modify	Remove
	MAC Address	Mask	MAC Address	Mask								
4	11:22:33:44:55:66	Any	11:22:33:44:55:66	Any						Permit	✎	☐

Figure 3-79. MAC Based ACL Page

CLI – The following is an example of the MAC Based ACL CLI commands:

```
Console(config)# mac access-list macl-acl1
4-306
Console(config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 6

4-307
Console (config-mac-acl)# deny 66:66:66:66:66:66
4-308
```

DHCP Snooping

DHCP Snooping expands network security by providing an extra layer of security between untrusted interfaces and DHCP servers. By enabling DHCP Snooping network administrators can identify between trusted interfaces connected to end-users or DHCP Servers, and untrusted interface located beyond the network firewall.

DHCP Snooping filters untrusted messages. DHCP Snooping creates and maintains a DHCP Snooping Table which contains information received from untrusted packets. Interfaces are untrusted if the packet is received from an interface from outside the network or from a interface beyond the network firewall. Trusted interfaces receive packets only from within the network or the network firewall.

The *DHCP Snooping Table* contains the untrusted interfaces MAC address, IP address, Lease Time, VLAN ID, and interface information.

The DHCP section contains the following topics:

- DHCP Snooping Properties
- Defining DHCP Snooping on VLANs
- Defining Trusted Interfaces
- Binding Addresses to the DHCP Snooping Database
- Configuring Option 82

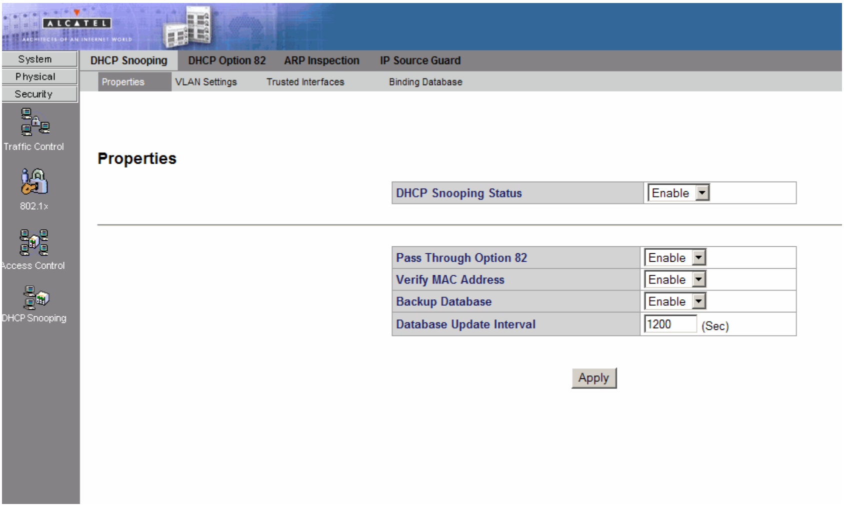
DHCP Snooping Properties

The *DHCP Snooping Properties Page* contains parameters for enabling DHCP Snooping on the device.

Command Attributes

- **DHCP Snooping Status** — Indicates if DHCP Snooping is enabled on the device. The possible field values are:
  - *Enable* — Enables DHCP Snooping on the device.
  - *Disable* — Disables DHCP Snooping on the device, this is the default value.
- **Pass Through Option 82** — Indicates if the device passes or rejects packets that include Option 82 information, while DHCP Snooping is enabled.
  - *Enabled* — Device allows packets containing Option 82 information.
  - *Disabled* — Device rejects packets containing Option 82 information.
- **Verify MAC Address** — Indicates if MAC address are verified. The possible field values are:
  - *Enabled* — Verify (on an untrusted port) that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header (part of the payload).
  - *Disabled* — Disables verifying that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header. This is the default value.
- **Backup Database** — Indicates if the DHCP Snooping Database learning and update is enabled. The possible field values are:
  - *Enabled* — Enables storing the allotted IP address in the DHCP Snooping Database.
  - *Disabled* — Disables storing the allotted IP address in the DHCP Snooping Database. This is the default value.
- **Database Update Interval** — Indicates how often the DHCP Snooping Database is updated. The possible field range is 600 – 86400 seconds. The field default is 1200 seconds.

Web – Click Security, Traffic Control, DHCP Snooping, Properties. Define the fields and click Apply.



Properties

DHCP Snooping Status	Enable

Pass Through Option 82	Enable
Verify MAC Address	Enable
Backup Database	Enable
Database Update Interval	1200 (Sec)

Figure 3-80. DHCP Snooping Properties Page

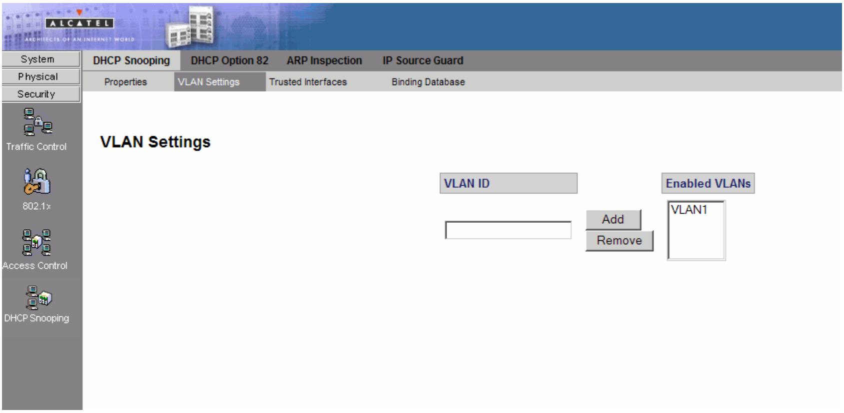
Defining DHCP Snooping on VLANs

The *VLAN Settings Page* allows network managers to enable DHCP snooping on VLANs. To enable DHCP Snooping on a VLAN, ensure DHCP Snooping is enabled on the device.

Command Attributes

- **VLAN ID** — Indicates the VLAN to be added to the Enabled VLAN list.
- **Enabled VLAN** — Contains a list of VLANs for which DHCP Snooping is enabled.

Web – Click Security, Traffic Control, DHCP Snooping, VLAN Settings. Define the fields and click Apply.



VLAN Settings

VLAN ID:

Enabled VLANs: VLAN1

Figure 3-81. VLAN Settings Page

Defining Trusted Interfaces

The *Trusted Interface Page* allows network manager to define Trusted interfaces. Trusted interfaces are connected to DHCP servers, switches, or hosts which do not require DHCP packet filtering. Trusted interfaces receive packets only from within the network or the network firewall, and are allowed to respond to DHCP requests. Packets sent from an interface outside the network, or from beyond the network firewall, are blocked by trusted interfaces.

Conversely, untrusted interfaces can be configured to receive traffic from outside the network or the firewall.

Command Attributes

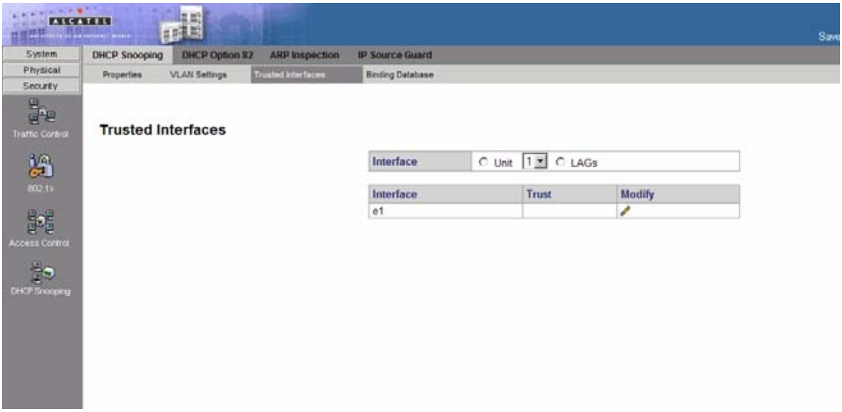
Global-level Parameter

- **Interface** — Displays the interface which can be defined as Trusted. The possible field values are:
  - *Units* — Displays the ports which can be defined as trusted.
  - *LAGs* — Displays the LAGs which can be defined as trusted.

Interface-level Parameters

- **Interface** — Contains a list of existing interfaces.
- **Trust** — Indicates whether the interface is a Trusted interface.
  - *Enable* — Interface is in trusted mode.
  - *Disable* — Interface is in untrusted mode.

Web – Click Security, Traffic Control, DHCP Snooping, Trusted Interface. Define the fields and click Apply.



Trusted Interfaces

Interface ○ Unit 1 ○ LAGs

Interface	Trust	Modify
e1		✎

Figure 3-82. Trusted Interface Page

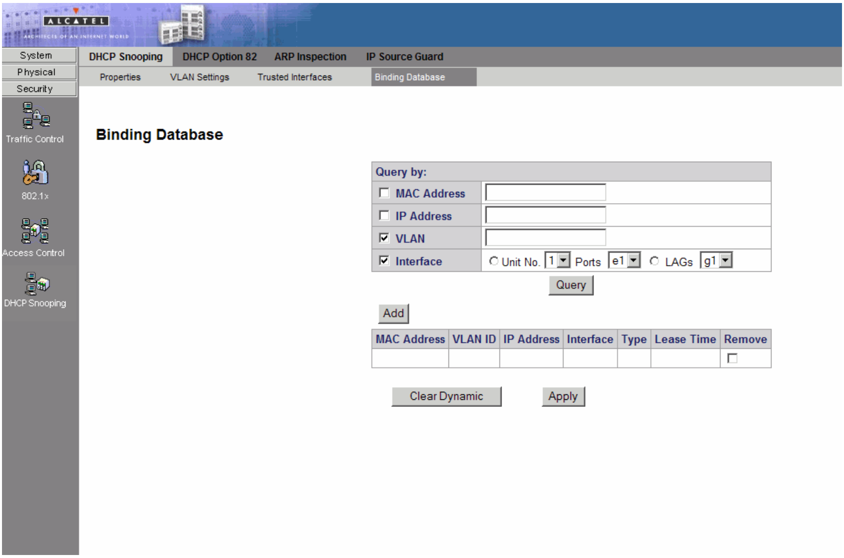
Binding Addresses to the DHCP Snooping Database

The *Binding Database Page* contains parameters for querying and adding IP addresses to the DHCP Snooping Database.

Command Attributes

- **MAC Address** — Indicates the MAC addresses recorded in the DHCP Database. The Database can be queried by MAC address.
- **IP Address** — Indicates the IP addresses recorded in the DHCP Database The Database can be queried by IP address.
- **VLAN** — Indicates the VLANs recorded in the DHCP Database. The Database can be queried by VLAN.
- **Interface** — Contains a list of interface by which the DHCP Database can be queried. The possible field values are:
  - *Port* — Queries the VLAN database by port number.
  - *LAG* — Queries the VLAN database by LAG number.
- **VLAN ID** — Displays the VLAN ID to which the IP address is attached in the DHCP Snooping Database.
- **Type** — Displays the IP address binding type. The possible field values are:
  - *Static* — Indicates the IP address is static.
  - *Dynamic* — Indicates the IP address is dynamically defined by the DHCP server.
- **Lease Time** — Displays the lease time. The Lease Time defines the amount of time the DHCP Database is active. Entries whose lease times are expired are ignored by the switch.

Web – Click Security, DHCP Snooping, DHCP Snooping, Binding Database. Define the fields and click Apply.



Binding Database

Query by:	
☐ MAC Address	
☐ IP Address	
☑ VLAN	
☑ Interface	○ Unit No. 1 Ports e1 ○ LAGs g1

MAC Address	VLAN ID	IP Address	Interface	Type	Lease Time	Remove
						☐

Figure 3-83. Binding Database Page

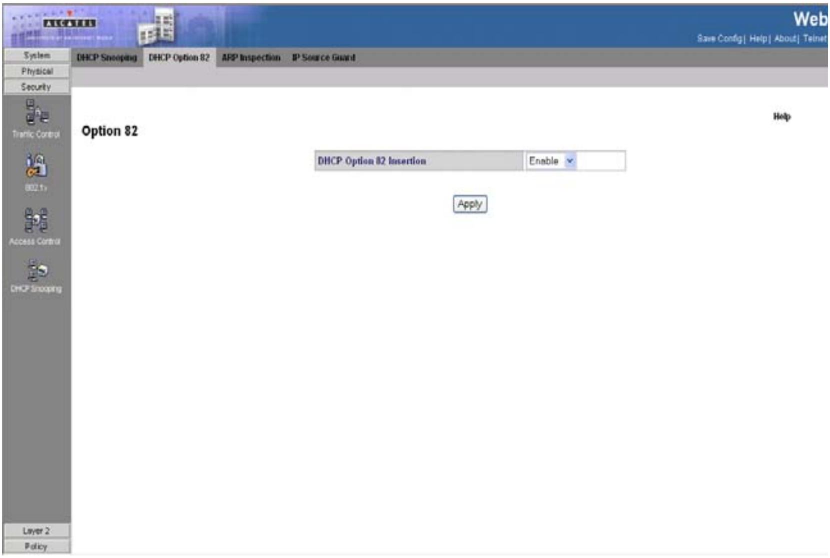
Configuring Option 82

DHCP with Option 82 attaches authentication messages to the packets sent from the host. DHCP passes the configuration information to hosts on a TCP/IP network. This permits network administrators to limit address allocation authorized hosts. DHCP with Option 82 can be enabled only if DHCP snooping is enabled.

Command Attributes

- **DHCP Option 82 Insertion** — Indicates if DHCP Option 82 with data insertion is enabled on the device. The possible field values are:
  - *Enable* — Enables DHCP Option 82 with data insertion on the device. If DHCP Option 82 with data insertion is enabled the DHCP server can insert information into DHCP requests. The DHCP information is used to assign IP addresses to network interfaces or apply Access Control Lists and QoS policies to network users.
  - *Disable* — Disables DHCP Option 82 with data insertion on the device. This is the default value.

Web – Click Security, DHCP Snooping, DHCP Option 82. Define the fields and click Apply.



Option 82

DHCP Option 82 Insertion: Enable

Figure 3-84. DHCP Option 82 Page

Dynamic ARP Inspection

Dynamic Address Resolution Protocol (ARP) is a TCP/IP protocol that translates IP addresses into MAC addresses. Dynamic ARP allows the following:

- Permits two hosts on the same network to communicate and send packets.
- Permits two hosts on different packets to communicate via a gateway.
- Permits routers to send packets via a host to a different router on the same network.
- Permits routers to send packets to a destination host via a local host.

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. Packets with invalid ARP Inspection Bindings are logged and dropped. Packets are classified as:

- **Trusted** — Indicates that the interface IP and MAC address are recognized, and recorded in the ARP Inspection List. Trusted packets are forward without ARP Inspection.
- **Untrusted** — Indicates that the packet arrived from an interface that does not have a recognized IP and MAC addresses. The packet is checked for:
  - *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.

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. If the IP address is found the packet is valid, and is forwarded. ARP inspection is performed only on untrusted interfaces

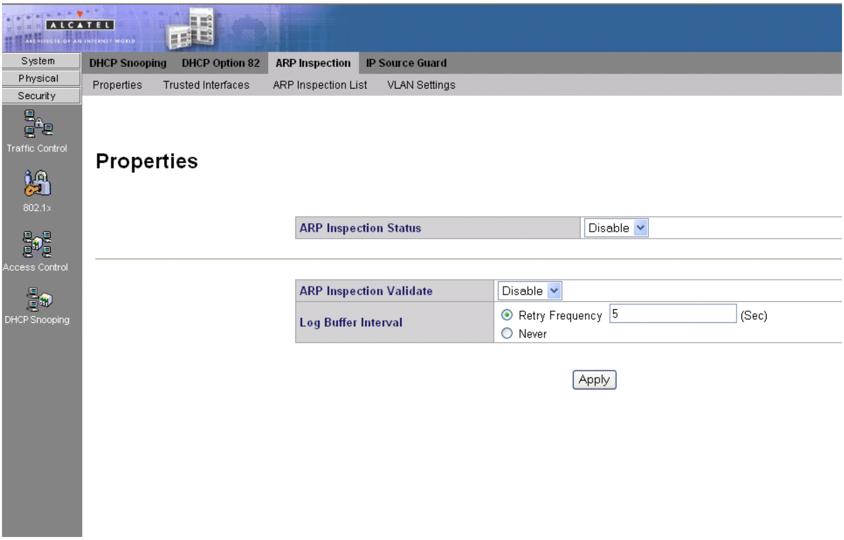
ARP Inspection Properties

The *ARP Inspection Properties Page* provides parameters for enabling and setting global Dynamic ARP Inspection parameters, as well as defining ARP Inspection Log parameters.

Command Attributes

- **ARP Inspection Status** — Indicates if ARP Inspection is enabled on the device. The possible field values are:
  - *Enable* — Enables ARP Inspection on the device.
  - *Disable* — Disables ARP Inspection on the device. This is the default value.
- **ARP Inspection Validate** — Indicates that ARP Inspection Validation is enabled on the device. The possible field values are:
  - *Enabled* — Enables ARP Inspection Validation on the device. If ARP Inspection Validation is enabled, the following parameters are checked in ARP requests and responses:
    - *Source MAC* — Validates the source MAC address against the sender's MAC address in both ARP requests and responses.
    - *Destination MAC* — Validates the destination MAC address against the recipient's MAC in ARP responses.
    - *IP addresses* — Validates invalid and unexpected IP addresses, including 0.0.0.0, 255.255.255.255, and all IP Multicast addresses.
  - *Disable* — Disable ARP Inspection Validation on the device. This is the default value.
- **Log Buffer Interval** — Defines the minimal interval between successive Syslog messages. The possible field values are:
  - *Retry Frequency* — Frequency at which the log is updated.
  - *Never* — Log is never updated.

Web – Click Security, DHCP Snooping, ARP Inspection, Properties. Define the fields and click Apply.



Properties

ARP Inspection Status	Disable

ARP Inspection Validate	Disable
Log Buffer Interval	● Retry Frequency 5 (Sec) ○ Never

Figure 3-85. ARP Inspection Properties Page

ARP Inspection Trusted Interface Settings

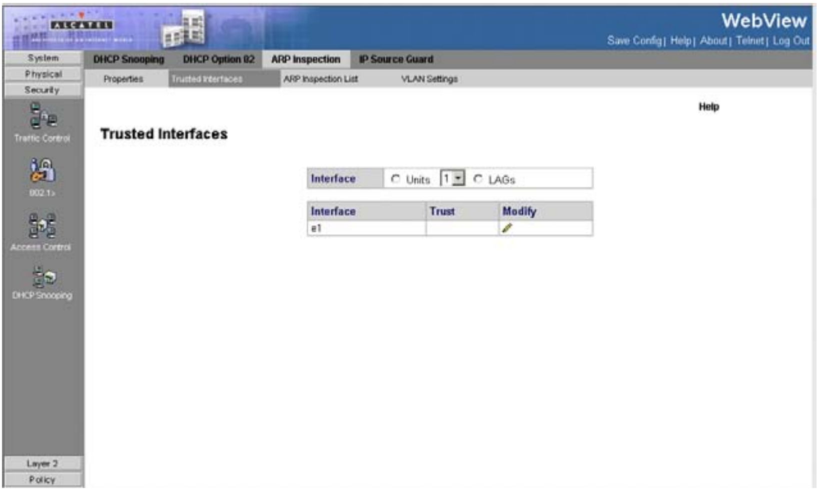
The *ARP Inspection Trusted Interface Page* allows network managers to define trusted and untrusted interfaces (independent of the trusted interface settings defined for DHCP snooping). ARP Inspection can be enabled only on untrusted interfaces.

- **Trusted** — Indicates that the interface IP and MAC address are recognized, and recorded in the ARP Inspec-tion List. Trusted packets are forward without ARP Inspection.
- **Untrusted** — Indicates that the packet arrived from an interface that does not have a recognized IP and MAC addresses. The packet is checked for:
  - *Source MAC* — Compares the packet's source MAC address 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 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. 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. If the IP address is found the packet is valid, and is forwarded.

Command Attributes

- **Interface** — Displays the interfaces on which ARP Inspection Trust mode can be enabled. The possible field values are:
  - *Units* — Indicates the port on which ARP Inspection Trust mode is enabled.
  - *LAGs* — Indicates the LAG on which ARP Inspection Trust mode is enabled.
- **Trust** — Indicates if the selected interface is trusted or untrusted. The possible field values are:
  - *Enable* — Indicates that the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests/replies sent to/from the interface.
  - *Disable* — Indicates the port or LAG is a trusted interface, and ARP inspection is performed on the ARP requests/replies sent to/from the interface. This is the default value if ARP Inspection is enabled.

Web – Click Security, DHCP Snooping, ARP Inspection, Trusted Interface. Define the fields and click Apply.



Trusted Interfaces

Interface	○ Units [1] ○ LAGs

Interface	Trust	Modify
e1		✎

Figure 3-86. ARP Inspection Trusted Interface Page

Defining ARP Inspection List

The *ARP Inspection List Page* provides information for creating static ARP Binding Lists. ARP Binding Lists contains the List Name, IP address and MAC address which are validated against ARP requests.

Command Attributes

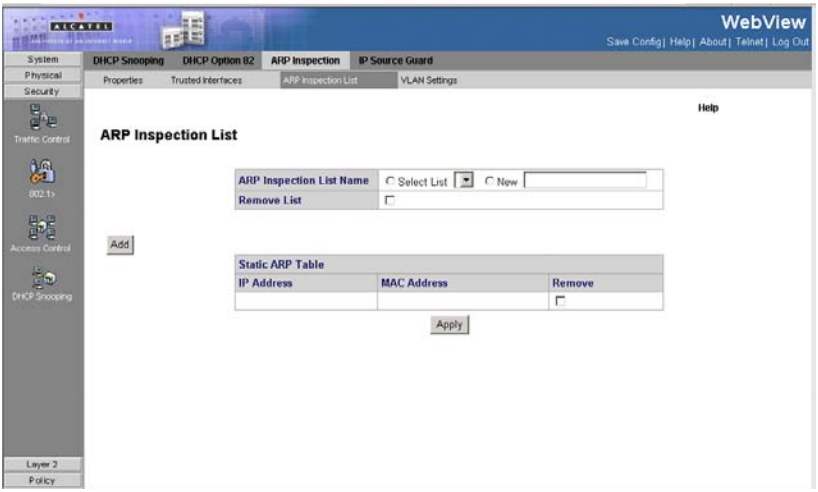
- **ARP Inspection List Name** — Name of the Inspection List, which may be an existing list or a new list.

- **Select List** — Contains a list of user-defined ARP Inspection Lists.
- **New** — Defines a new ARP Inspection List. The list’s name can contain up to 32 characters.

Static ARP Table

- **IP Address** — Specifies IP address included in ARP Binding Lists which is checked against ARP requests.
- **MAC Address** — Specifies MAC address included in ARP Binding Lists which is checked against ARP requests.
- **Remove** — Removes the entry. The possible field values are:
  - *Checked* — Removes the selected entry.
  - *Unchecked* — Maintains the current entry information.

Web – Click Security, DHCP Snooping, ARP Inspection, ARP Inspection List. Define the fields and click Apply.



ARP Inspection List

ARP Inspection List Name	○ Select List ▾ ○ New
Remove List	□

Static ARP Table		
IP Address	MAC Address	Remove
		□

Figure 3-87. ARP Inspection List Page

Assigning ARP Inspection VLAN Settings

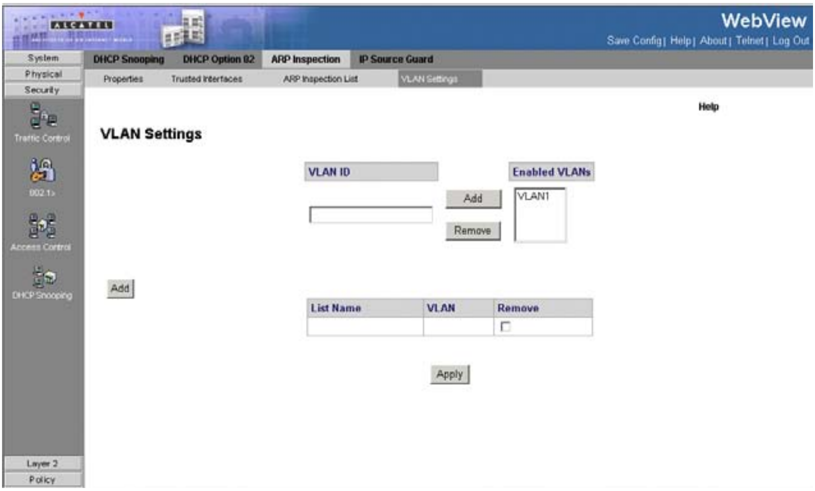
The VLAN Settings Page assigns static ARP Inspection Lists to VLANs.

Command Attributes

- **VLAN ID** — A new VLAN ID that is defined by the user and added to the Enabled VLANs list.
- **Enabled VLANs** — Contains a list of VLANs in which ARP Inspection is enabled.
- **List Name** — Displays names of static ARP Inspection Lists that can be assigned to VLANs. These lists are defined in the *ARP Inspection List Page.*
- **VLAN** — Contains a the VLAN which is bound to the ARP Bindings List.

- **Remove** — Removes the entry. The possible field values are:
  - *Checked* — Removes the selected entry.
  - *Unchecked* — Maintains the current entry information.

Web – Click Security, DHCP Snooping, ARP Inspection, VLAN Settings. Define the fields and click Apply.



VLAN Settings

VLAN ID

Enabled VLANs: VLAN1

List Name	VLAN	Remove
		☐

Figure 3-88. VLAN Settings Page

IP Source Guard

IP Source Guard is a security feature that restricts the client IP traffic to those source IP addresses configured in the binding. IP traffic restrictions are applied according to definitions in both the DHCP Snooping Binding Database and in manually configured IP source bindings. For example, IP Source Guard can help prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

Notes:

1. IP Source Guard must be enabled globally in the *IP Source Guard Properties Page* before it can be enabled on the device interfaces.
2. IP Source Guard uses Ternary Content Addressable Memory (TCAM) resources, requiring use of 1 TCAM rule per 1 IP Source Guard address entry. If the number of IP Source Guard entries exceeds the number of available TCAM rules, new IP source guard addresses remain inactive.
3. IP Source Guard can be enabled only on DHCP Snooping untrusted interfaces.
4. IP Source Guard cannot be configured on routed ports.
5. If IP Source Guard and MAC address filtering is enabled on a port, Port Security cannot be activated on the same port.

Configuring IP Source Guard Properties

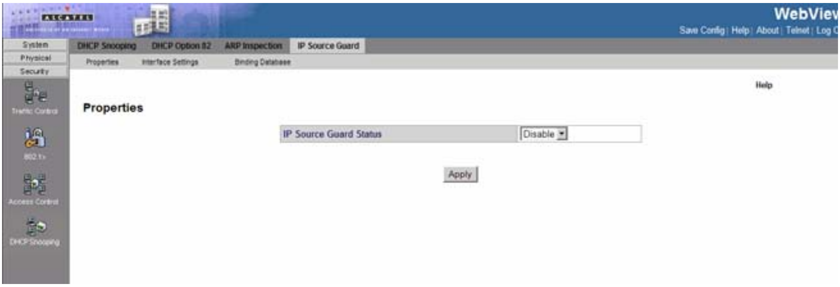
The *IP Source Guard Properties Page* allows network managers to enable the use of IP Source Guard on the device. IP Source Guard must be enabled for the device before it can be enabled on individual ports or LAGs.

Command Attributes

- **IP Source Guard Status** — Allows the use of IP Source Guard status on the device.
  - *Enable* — Indicates that IP Source Guard is enabled for the device.
  - *Disable* — Indicates that IP Source Guard is disabled for the device.

Web – Click Security, DHCP Snooping, IP Source Guard, Properties. Define the fields and click Apply.

I



Properties

IP Source Guard Status: Disable

Figure 3-89. IP Source Guard Properties Page

Defining IP Source Guard Interface Settings

In the IP Source Guard *Interface Settings Page*, IP Source Guard can be enabled on DHCP Snooping untrusted interfaces, permitting the transmission of DHCP packets allowed by DHCP Snooping. If source IP address filtering is enabled, packet transmission is permitted as follows:

- **IPv4 traffic** — Only IPv4 traffic with a source IP address that is associated with the specific port is permitted.
- **Non IPv4 traffic** — All non-IPv4 traffic is permitted.

Notes: **1.** IP Source Guard must be enabled globally in the *IP Source Guard Properties Page* before it can be enabled on the device interfaces.

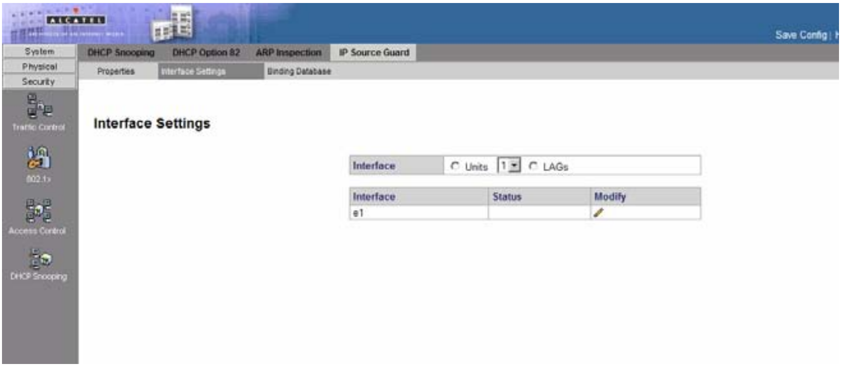
2. If a port is trusted, filtering of static IP addresses can be configured, although IP Source Guard is not active in that condition.

3. When the port’s status changes from untrusted to trusted, the static IP address filtering entries remain but become inactive.

Command Attributes

- **Interface** — Displays the interface on which can be defined as Trusted. The possible field values are:
  - *Ports* — Displays the ports which can be defined as trusted.
  - *LAGs* — Displays the LAGs which can be defined as trusted.
- **Interfaces** — Contains a list of existing interfaces.
- **Status** — Indicates if IP Source Guard is enabled or disabled.
  - *Enable* — Indicates that IP Source Guard is enabled on the interface.
  - *Disable* — Indicates that IP Source Guard is disabled on the interface. This is the default value.

Web – Click Security, DHCP Snooping, IP Source Guard, Interface Settings. Select an interface, click Modify to define the fields and click Apply.



Interface Settings

Interface	○ Units [1 ▾] ○ LAGs

Interface	Status	Modify
e1		✎

Figure 3-90. Interface Settings Page

Adding Interfaces to the IP Source Guard Database

The *IP Source Guard Binding Database Page* contains parameters for querying IP addresses to the IP Source Guard Database.

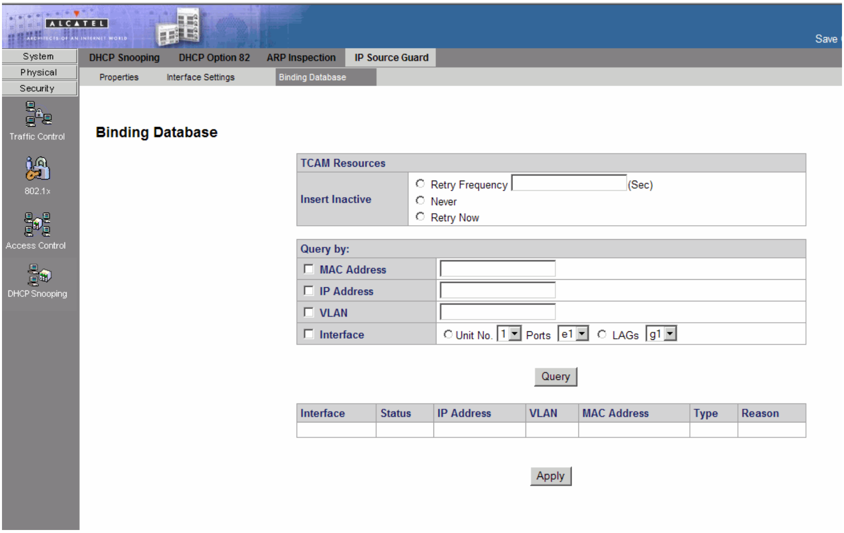
Command Attributes

- **TCAM Resources** — The IP Source Guard Database uses TCAM resources for managing the database. TCAM resources status is checked in diffrent time frequencies.
  - *Retry Frequency* — The frequency in which the TCAM Resources are checked.
  - *Never* — TCAM Resources never checked
  - *Retry Now* — TCAM Resources are checked now
- **MAC Address** — Indicates the MAC addresses recorded in the IP Source Guard Database. The Database can be queried by MAC address.

- **IP Address** — Indicates the IP addresses recorded in the IP Source Guard Database. The Database can be queried by IP address.
- **VLAN** — Indicates the VLANs recorded in the IP Source Guard Database. The Database can be queried by VLAN.
- **Interface** — Contains a list of interface by which the IP Source Guard Database can be queried. The possible field values are:
  - *Port* — Queries the VLAN database by port number.
  - *LAG* — Queries the VLAN database by LAG number.
- **Interface** — Displays the VLAN ID to which the IP address is attached in the IP Source Guard Database.
- **Status** — Displays the Interface status.
- **Type** — Displays the IP address binding type. The possible field values are:
  - *Static* — Indicates the IP address remains static.
  - *Dynamic* — Indicates the IP address was obtained from the DHCP server.
- **Reason** — Indicates a reason if the Status is Inactive. The possible field options are:
  - No Problem
  - VLAN
  - Trusted Port
  - Resource Problem

Web – Click Security, DHCP Snooping, IP Source Guard, Binding Database. Define the fields and click Apply.

•



Binding Database

TCAM Resources	
Insert Inactive	○ Retry Frequency [ ] (Sec) ○ Never ○ Retry Now

Query by:	
□ MAC Address	[ ]
□ IP Address	[ ]
□ VLAN	[ ]
□ Interface	○ Unit No. 1 Ports e1 ○ LAGs g1

Interface	Status	IP Address	VLAN	MAC Address	Type	Reason

Figure 3-91. IP Source Guard Binding Database Page

Defining the Forwarding Database

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

An address becomes associated with a port by learning the frame's source address, but if a frame that is addressed to a destination MAC address is not associated with a port, that frame is flooded to all relevant VLAN ports. To prevent the bridging table from overflowing, a dynamic MAC address, from which no traffic arrives for a set period, is erased.

Packets addressed to destinations stored in either the Static or Dynamic databases are immediately forwarded to the port. The Dynamic MAC Address Table can be sorted by interface, VLAN, or MAC Address, whereas MAC addresses are dynamically learned as packets from sources that arrive at the device. Static addresses are configured manually.

Defining Static Forwarding Database Entries

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

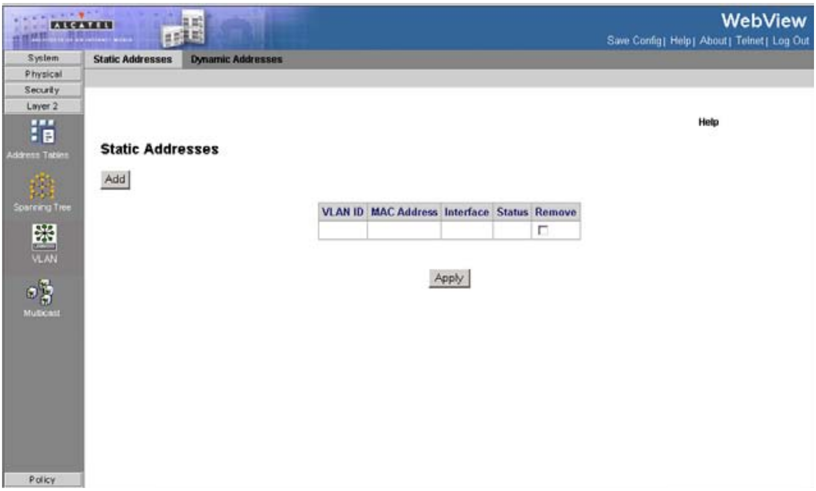
To prevent static MAC addresses from being deleted when the device is reset, ensure that the port attached to the MAC address is locked.

Command Attributes

- **MAC Address** — Displays the MAC address to which the entry refers.
- **VLAN ID** — Displays the VLAN ID number to which the entry refers.
- **Interface** — Displays the interface to which the entry refers:
  - *Port* — The specific port number to which the forwarding database parameters refer.
  - *LAG* — The specific LAG number to which the forwarding database parameters refer.
- **Status** — Displays how the entry was created. The possible field values are:
  - *Secure* — The MAC Address is defined for locked ports.
  - *Permanent* — The MAC address is permanent.
  - *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.
- **Remove** — Removes the entry. The possible field values are:
  - *Checked* — Removes the selected entry.
  - *Unchecked* — Maintains the current static forwarding database.

Web – Click Layer 2, Address Table, Static Addresses. Specify the interface, the

MAC address and VLAN, then click Apply.



Static Addresses

VLAN ID	MAC Address	Interface	Status	Remove
				□

Figure 3-92. Static Addresses Page

CLI – The following is an example of the CLI commands used to define static addresses:

```
Console(config)# interface vlan 2
4-664
Console(config-if)# bridge address 3aa2.64b3.a245 ethernet 1/e16
permanent
4-314
```

Defining Dynamic Forwarding Database Entries

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports. The *Dynamic Addresses Page* contains parameters for querying information in the Dynamic MAC Address Table, including the interface type, MAC addresses, VLAN, and table storing. The Dynamic MAC Address table contains information about the aging time before a dynamic MAC address is erased, and includes parameters for querying and viewing the Dynamic MAC Address table. The Dynamic MAC Address table contains address parameters by which packets are directly forwarded to the ports. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address.

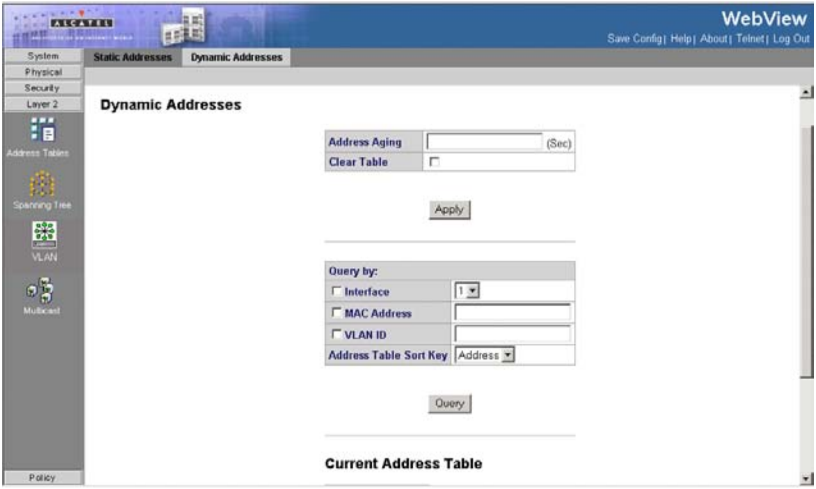
Command Attributes

- **Address Aging** — Specifies the amount of time the MAC address remains in the Dynamic MAC Address table before it is timed out, if no traffic from the source is detected. The default value is 300 seconds.
- **Clear Table** — If checked, clears the MAC address table.

In the Query By table, the following fields are query filter options. In the Current Address Table, the following fields are parameters of the MAC address entries.

- **Interface** — Specifies the interface for which the table is queried. There are two interface types from which to select.
- **MAC Address** — Specifies the MAC address for which the table is queried.
- **VLAN ID** — Specifies the VLAN ID for which the table is queried.
- **Address Table Sort Key** —Specifies the means by which the Dynamic MAC Address Table is sorted. The address table can be sorted by address, VLAN, or interface.

Web – Click Layer 2, Address Table, Dynamic Addresses. Specify the search type, select the sorting method and click Query.



Dynamic Addresses

Address Aging	(Sec)
Clear Table	□

Query by:	
□ Interface	1
□ MAC Address	
□ VLAN ID	
Address Table Sort Key	Address

Current Address Table

Figure 3-93. Dynamic Addresses Page

CLI – The following is an example of the CLI commands used to define dynamic addresses:.

```
Console# clear bridge
4-320
Console# configure
Console(config)# interface vlan 2
4-664
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
4-316
Console(config-if)# bridge multicast forbidden address 0100.5e02.0203 add
ethernet 2/e9
4-317
Console(config-if)# bridge multicast forward-all add ethernet 1/e8

4-318
Console(config-if)# bridge multicast forbidden forward-all add ethernet
1/e1
4-319
```

Configuring Spanning Tree

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

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

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

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

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

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

When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (an extension of RSTP) is designed to support independent spanning trees based on VLAN groups. Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

Defining Spanning Tree

You can display a summary of the current bridge STP information that applies to the entire switch using the STP Information screen.

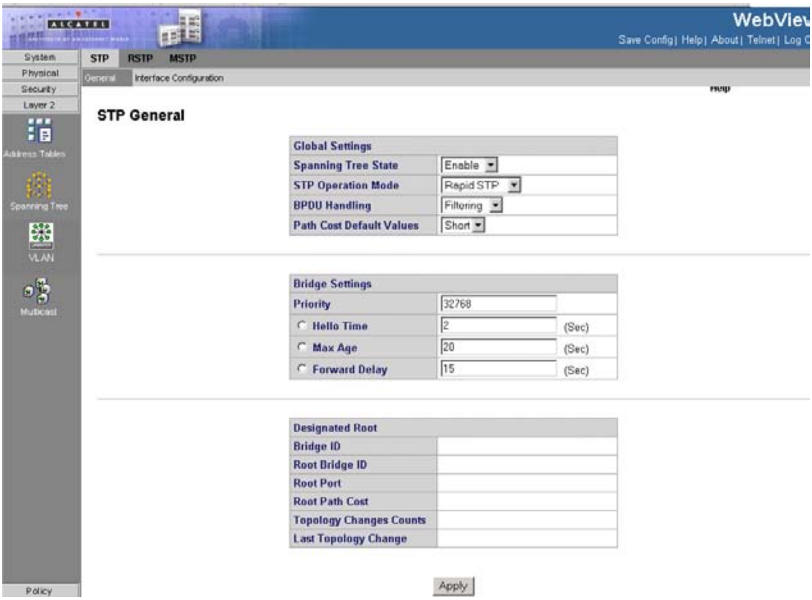
Command Attributes

- **Spanning Tree State** — Indicates whether STP is enabled on the device. The possible field values are:
  - *Enable* — Enables STP on the device.
  - *Disable* — Disables STP on the device.
- **STP Operation Mode** — Specifies the STP mode that is enabled on the device. The possible field values are:
  - *Classic STP* — Enables Classic STP on the device. This is the default value.
  - *Rapid STP* — Enables Rapid STP on the device.
  - *Multiple STP* — Enables Multiple STP on the device.
- **BPDU Handling** — Determines how BPDU packets are managed when STP is disabled on the port or device. BPDUs are used to transmit spanning tree information. The possible field values are:
  - *Filtering* — Filters BPDU packets when spanning tree is disabled on an interface.
  - *Flooding* — Floods BPDU packets when spanning tree is disabled on an interface. This is the default value.
  - *Bridging* — Indicates that if the spanning tree protocol is globally disabled, untagged and tagged BPDU packets are flooded, and are subject to ingress and egress VLAN rules. Bridging BPDU can only be enabled if the spanning tree protocol is enabled on port groups.
- **Path Cost Default Values** — Specifies the method used to assign default path cost to STP ports. The possible field values are:

  - *Short* — Specifies 1 through 65,535 range for port path cost. This is the default value.
  - *Long* — Specifies 1 through 200,000,000 range for port path cost. The default path cost assigned to an interface varies according to the selected method (*Hello Time*, *Max Age*, or *Forward Delay*).
- **Priority** — Specifies 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.
- **Hello Time** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a Root Bridge waits between configuration messages. The default is 2 seconds.
- **Max Age** — Specifies the device Maximum Age Time. The Maximum Age Time is the amount of time in seconds a bridge waits before sending configuration messages. The default Maximum Age Time is 20 seconds.
- **Forward Delay** — Specifies the device Forward Delay Time. The Forward Delay Time is the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is 10 seconds.
- **Bridge ID** — Identifies the Bridge priority and MAC address.
- **Root Bridge ID** — Identifies the Root Bridge priority and MAC address.
- **Root Port** — Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. This field is significant when the bridge is not the Root Bridge. The default is zero.
- **Root Path Cost** — The cost of the path from this bridge to the Root Bridge.
- **Topology Changes Counts** — Specifies the total amount of STP state changes that have occurred.
- **Last Topology Change** — Indicates the amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change that occurred. The time is displayed in a day-hour-minute-second format, such as 2 days 5 hours 10 minutes and 4 seconds.

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

Web – Click Layer 2, Spanning Tree, STP, General.



STP General

Global Settings	
Spanning Tree State	Enable
STP Operation Mode	Rapid STP
BPDU Handling	Filtering
Path Cost Default Values	Short

Bridge Settings		
Priority	32768	
○ Hello Time	2	(Sec)
○ Max Age	20	(Sec)
○ Forward Delay	15	(Sec)

Designated Root	
Bridge ID	
Root Bridge ID	
Root Port	
Root Path Cost	
Topology Changes Counts	
Last Topology Change	

Figure 3-94. STP General Page

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

```
Console(config)# spanning-tree
4-540
console(config)# spanning-tree mode rstp
4-540
Console(config)# spanning-tree bpdu flooding
4-550
Console(config)# spanning-tree pathcost method long
4-549
Console(config)# interface ethernet 1/e15
4-376
Console(config)# spanning-tree priority 12288
4-544
Console(config)# spanning-tree hello-time 5
4-542
Console(config)# spanning-tree max-age 12
4-543
Console(config)# spanning-tree forward-time 25
4-541
```

Defining STP on Interfaces

Network administrators can assign STP settings to specific interfaces using the *Interface Configuration Page*. The Global LAGs section displays the STP information for Link Aggregated Groups. Adhere to the following guidelines when configuring STP on an interface:

- A port on a network segment with no other STP compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STP device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.

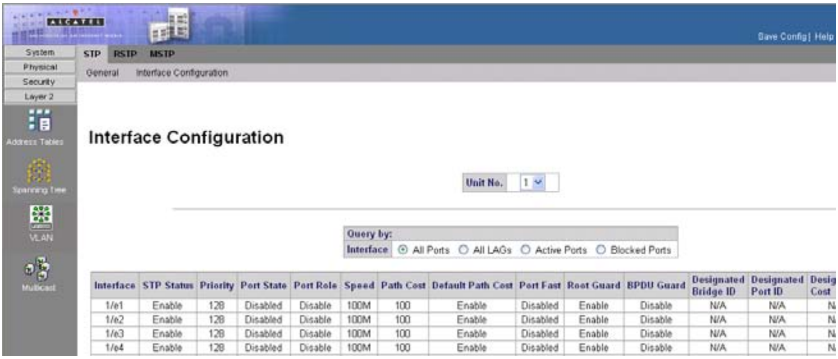
All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the STP settings information is displayed.
- **Query by Interface** — Queries the interface configuration table either by: All ports, All Lags, Active Ports or Blocked Ports.
- **Interface** — The interface for which the information is displayed.
- **STP** — Indicates if STP is enabled on the port. The possible field values are:
  - *Enable* — Indicates that STP is enabled on the port.
  - *Disable* — Indicates that STP is disabled on the port.
- **Priority** — Indicates the priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0-240. The priority value is determined in increments of 16.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
  - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
  - *Forwarding* — Indicates the port is currently in the Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Port Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to the root switch.
  - *Designated* — The port or LAG through which the designated switch is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root switch from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections to a shared segment.
  - *Disabled* — The port is not participating in the Spanning Tree.
- **Speed** — Indicates the speed at which the port is operating.

- **Path Cost** — Indicates 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 is rerouted.
- **Default Path Cost** — Indicates if the default path cost of the port is automatically set by the port speed and the default path cost method.
- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.
  - *Enable* — Port Fast is enabled.
  - *Disable* — Port Fast is disabled.
  - *Auto* — Port Fast mode is enabled a few seconds after the interface becomes active.
- **Root Guard** — Used to prevent an unauthorized device from becoming the root of a spanning tree. It also enables detection and resolution of misconfigurations, while preventing loops or loss of connectivity.
- **BPDU Guard** — BPDU Guard is used as a security mechanism to protect the network from invalid configurations. It is usually used either when fast link ports (ports connected to clients) are enabled or when STP feature is disabled. When BPDU guard is enabled on a port, the port is shut down if a BPDU message is received and an appropriate SNMP trap is generated. The port must then be reactivated by using the **set interface active** command. The **BPDU Guard** indicates if BPDU is enabled for the selected interface. The possible field values are:
  - *Enable* — Enables BPDU guard on the selected port or LAG.
  - *Disable* — Disables BPDU guard on the selected port or LAG. This is the default value.
- **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Indicates the selected port priority and interface.
- **Designated Cost** — Indicates 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** — Indicates the number of times the port has changed from Forwarding state to Blocking state.
- **LAG** — Indicates the LAG to which the port belongs.

Web – Click Layer 2, Spanning Tree, STP, Interface Configuration.



Interface Configuration

Unit No. 1

Query by:
Interface ● All Ports ○ All LAGs ○ Active Ports ○ Blocked Ports

Interface	STP Status	Priority	Port State	Port Role	Speed	Path Cost	Default Path Cost	Port Fast	Root Guard	BPDU Guard	Designated Bridge ID	Designated Port ID	Desig Cost
1/e1	Enable	128	Disabled	Disable	100M	100	Enable	Disabled	Enable	Disable	N/A	N/A	N
1/e2	Enable	128	Disabled	Disable	100M	100	Enable	Disabled	Enable	Disable	N/A	N/A	N
1/e3	Enable	128	Disabled	Disable	100M	100	Enable	Disabled	Enable	Disable	N/A	N/A	N
1/e4	Enable	128	Disabled	Disable	100M	100	Enable	Disabled	Enable	Disable	N/A	N/A	N

Figure 3-95. Interface Configuration Page

CLI –The following is an example of the STP interface commands:

```
Console(config)# interface ethernet 1/e5
4-376
Console(config-if)# spanning-tree disable
4-544
Console(config-if)# spanning-tree cost 35000
4-545
Console(config-if)# spanning-tree port-priority 96
4-553
Console(config-if)# spanning-tree portfast
4-547
```

Defining Rapid Spanning Tree

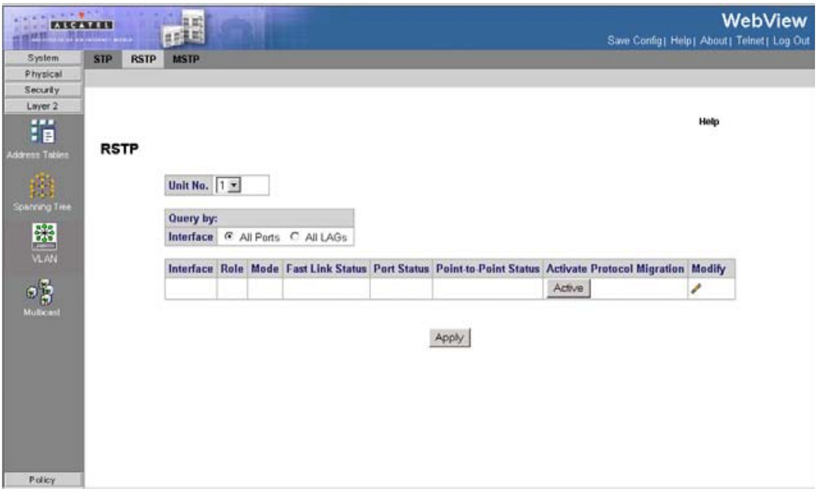
While Classic STP prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops and propagating status topology changes. *Rapid Spanning Tree Protocol* (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops. The Global System LAG information displays the same field information as the ports, but represent the LAG RSTP information. The *RSTP Page* contains parameters for defining RSTP.

Command Attributes

- **Interface** — Displays the interfaces on which RSTP is enabled. The possible field values are:
  - *All Ports* — Enables RSTP on all ports.
  - *All LAGs* — Enables RSTP on all LAGs.
- **Interface** — Displays the port or LAG on which Rapid STP is enabled.
- **Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:

  - *Root* — Provides the lowest cost path to forward packets to the root switch.
  - *Designated* — The port or LAG through which the designated switch is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root switch from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
  - *Disable* — The port is not participating in the Spanning Tree.
- **Mode** — Displays the current STP mode. The STP mode is selected in the *STP General Page*. The possible field values are:
  - *STP* — Classic STP is enabled on the device.
  - *Rapid STP* — Rapid STP is enabled on the device.
  - *Multiple STP* — Multiple STP is enabled on the device.
- **Fast Link Status** — Indicates whether Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- **Port Status** — Displays the RSTP status for the port on which RSTP is enabled. The possible field values are:
  - *Disable* — indicates the port is currently disabled.
  - *Forwarding* — Indicates the port is currently linked and forwarding traffic.
- **Point-to-Point Status** — Indicates whether a point-to-point link is established, or if the device is permitted to establish a point-to-point link. The possible field values are:
  - *Enable* — The device is permitted to establish a point-to-point link, or is configured 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 Protocol* (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.
- **Activate Protocol Migration** — Click the *Activate* button to send Link Control Protocol (LCP) packets.

Web – Click Layer 2, Spanning Tree, RSTP. Define the fields and Click Apply.



RSTP

Unit No. 1

Query by:

Interface ● All Ports ○ All LAGs

Interface	Role	Mode	Fast Link Status	Port Status	Point-to-Point Status	Activate Protocol Migration	Modify
						Active	✎

Figure 3-96. RSTP Page

CLI –The following is an example of the RSTP commands:

```
console# show spanning-tree                                                4-564
```

Defining Multiple Spanning Tree

Multiple Spanning Tree (MSTP) provides differing load balancing scenarios. For example, while port A is blocked in one STP instance, the same port can be placed in the *Forwarding* state in another STP instance. The *MSTP General Page* contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

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

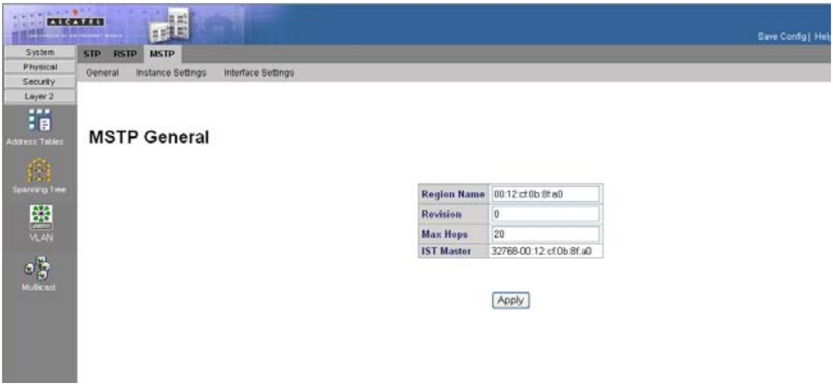
By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 16 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Command Attributes

- **Region Name** — User-defined STP region name.

- **Revision** — An unsigned 16-bit number that identifies the revision of the current MSTP configuration. The revision number is required as part of the MSTP configuration. The possible field range is 0-65535.
- **Max Hops** — Specifies 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. The possible field range is 1-40. The field default is 20 hops.
- **IST Master —** Identifies the Spanning Tree Master instance. The IST Master is the specified instance root.

Web – Click Layer 2, Spanning Tree, MSTP, General. Define the fields and Click Apply.



Region Name	00:12:cf:0b:8f:a0
Revision	0
Max Hops	20
IST Master	32768-00:12:cf:0b:8f:a0

Figure 3-97. MSTP General Page

CLI –The following is an example of the MSTP general properties commands:

```
Console(config)# spanning-tree mst max-hops 10
4-552
```

Defining MSTP Instance Settings

MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

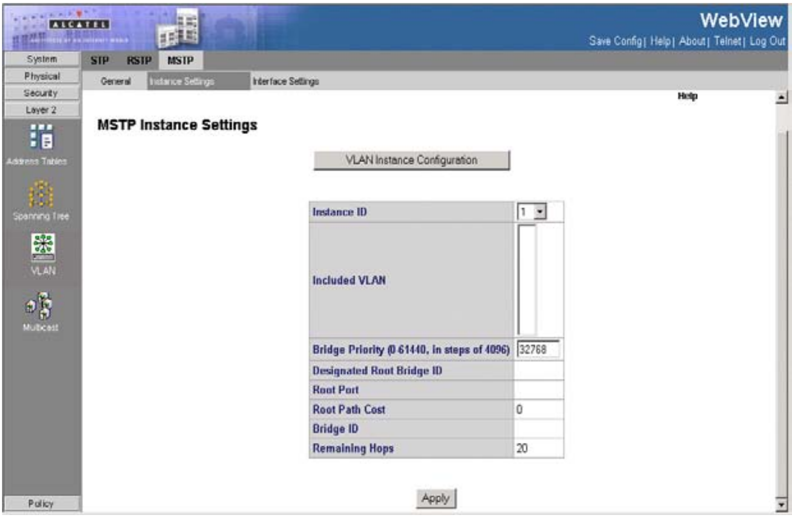
Network administrators can define the MSTP instance settings using the *MSTP Instance Settings Page*.

Note: To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

Command Attributes

- **Instance ID** — Specifies the VLAN group to which the interface is assigned.
- **Included VLAN** — Maps the selected VLANs to the selected instance. Each VLAN belongs to one instance.
- **Bridge Priority** — Specifies the selected spanning tree instance device priority. The field range is 0-61440.
- **Designated Root Bridge ID** — Indicates the ID of the bridge with the lowest path cost to the instance ID.
- **Root Port** — Indicates the selected instance's root port.
- **Root Path Cost** — Indicates the selected instance's path cost.
- **Bridge ID** — Indicates the bridge ID of the selected instance.
- **Remaining Hops** — Indicates the number of hops remaining to the next destination.

Web – Click Layer 2, Spanning Tree, MSTP, Instance Settings. Define the fields and Click Apply.



MSTP Instance Settings

Instance ID	1
Included VLAN	
Bridge Priority (0-61440, in steps of 4096)	32768
Designated Root Bridge ID	
Root Port	
Root Path Cost	0
Bridge ID	
Remaining Hops	20

Figure 3-98. MSTP Instance Settings Page

CLI –The following is an example of the MSTP Instance Settings commands:

```
Console(config)# spanning-tree mst configuration
4-556
Console(config-mst)# instance 1 add vlan 10-20
4-556
```

Defining MSTP Interface Settings

You can configure the STP interface settings for an MSTP Instance using the *MSTP*

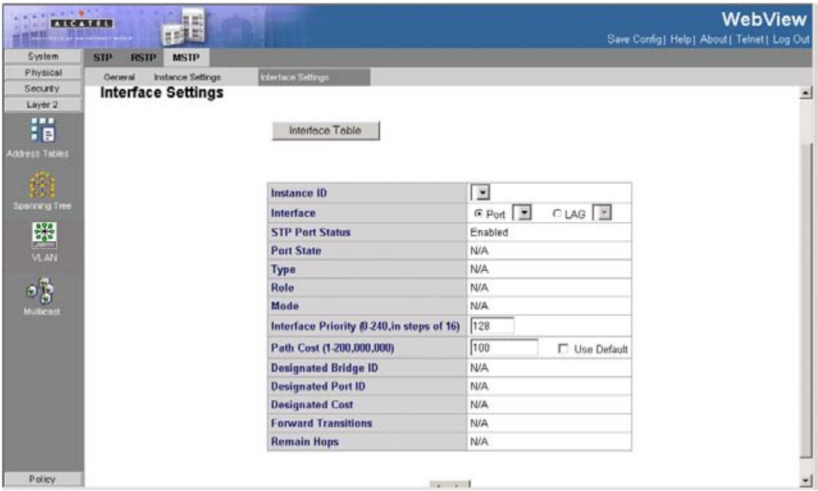
Interface Settings Page.

Command Attributes

- **Instance ID** — Lists the MSTP instances configured on the device. Possible field range is 0-15.
- **Interface** — Displays the interface for which the MSTP settings are displayed. The possible field values are:
  - *Port* — Specifies the port for which the MSTP settings are displayed.
  - *LAG* — Specifies the LAG for which the MSTP settings are displayed.
- **STP Port Status** — Indicates if STP is enabled on the port. The possible field values are:
  - *Enabled* — Indicates that STP is enabled on the port.
  - *Disabled* — Indicates that STP is disabled on the port.
- **Port State** — Indicates whether the port is enabled for the specific instance. The possible field values are:
  - *Enabled* — Enables the port for the specific instance.
  - *Disabled* — Disables the port for the specific instance.
- **Type** — Indicates whether the port is a Boundary or Master port. The possible field values are:
  - *Boundary Port* — Indicates that the port is a Boundary port. A Boundary port attaches MST bridges to LANs in an outlying region. If the port is a Boundary port, this field also indicates whether the device on the other side of the link is working in RSTP or STP mode
  - *Master Port* — Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
- **Role** — Indicates the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to the root device.
  - *Designated* — Indicates the port or LAG through which the designated device is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root device from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link or when a LAN has two or more connections connected to a shared segment.
  - *Disabled* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the STP mode by which STP is enabled on the device. The possible field values are:
  - *Classic STP* — Classic STP is enabled on the device. This is the default value.
  - *Rapid STP* — Rapid STP is enabled on the device.
  - *Multiple STP* — Multiple STP is enabled on the device.
- **Interface Priority** — Defines the interface priority for the specified instance. The default value is 128.

- **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.
- **Designated Bridge ID** — Displays the ID of the bridge that connects the link or shared LAN to the root.
- **Designated Port ID** — Displays the ID of the port on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- **Forward Transitions** — Indicates the number of times the LAG State has changed from a *Forwarding* state to a *Blocking* state.
- **Remain Hops** — Indicates the hops remaining to the next destination.

Web – Click Layer 2, Spanning Tree, MSTP, Interface Settings. Define the fields and Click Apply.



Interface Settings

Instance ID	
Interface	● Port ○ LAG
STP Port Status	Enabled
Port State	N/A
Type	N/A
Role	N/A
Mode	N/A
Interface Priority (0-240,in steps of 16)	128
Path Cost (1-200,000,000)	100 □ Use Default
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A
Remain Hops	N/A

Figure 3-99. MSTP Interface Settings Page

CLI –The following is an example of the MSTP Interface Settings commands.

```
Console (config) # spanning-tree mst 1 priority 4096
4-551
Console(config)# interface ethernet g1
4-376
Console(config-if)# spanning-tree mst 1 port-priority 144
4-546
Console(config-if) # spanning-tree mst 1 cost 4
4-554
```

Configuring VLANs

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

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

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

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

This switch supports the following VLAN features:

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

Assigning Ports to VLANs

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

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

VLAN Classification

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

Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers.

Untagged VLANs

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

Automatic VLAN Registration

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

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

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices. But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

Tagged/Untagged VLANs

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

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

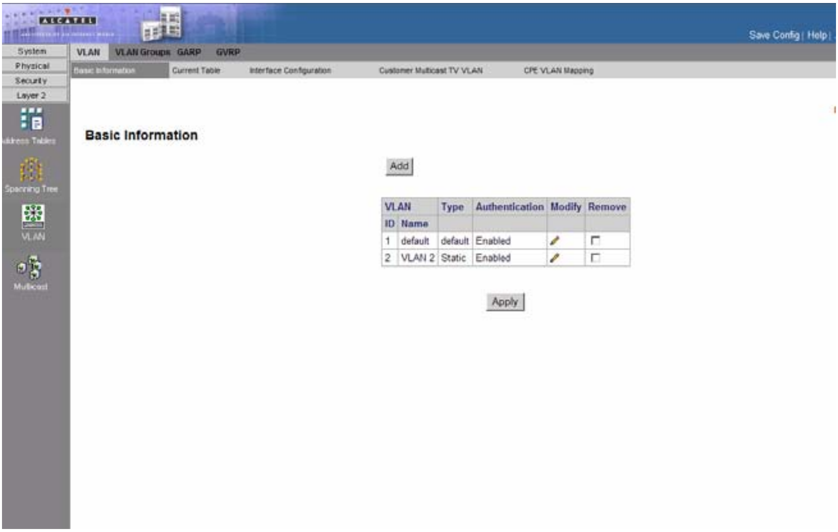
Displaying Basic VLAN Information

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

Command Attributes

- **VLAN ID** — Displays the VLAN ID.
- **Name** — Displays the user-defined VLAN name.
- **Type** — Displays the VLAN type. The possible field values are:
  - *Dynamic* — The VLAN was dynamically created through GARP.
  - *Static* — The VLAN is user-defined.
  - *Default* — The VLAN is the default VLAN.
- **Authentication** — Indicates whether authorization is required in order to access the VLAN. The possible field values are:
  - *Enabled* — Requires authorization in order to access the VLAN.
  - *Guest* — Enables unauthorized users to use the Guest VLAN.
  - *Disabled* — Disables unautherized users from using the Guest VLAN.
- **Remove** — Removes VLANs. The possible field values are:
  - *Checked* — Removes the selected VLAN.
  - *Unchecked* — Maintains VLANs.

Web – Click Layer 2, VLAN, VLAN, Basic Information.



Basic Information

VLAN		Type	Authentication	Modify	Remove
ID	Name				
1	default	default	Enabled	✎	□
2	VLAN 2	Static	Enabled	✎	□

Figure 3-100. VLAN Basic Information Page

CLI – The following is an example of the VLAN Basic Information CLI commands:

```
Console# show vlan
4-682


VLAN      Name           Ports                Type        Authorization

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

1         default        1/e1-e2,2/e1-e4      other       Required

10        VLAN0010       1/e3-e4              dynamic     Required

11        VLAN0011       1/e1-e2              static      Required

20        VLAN0020       1/e3-e4              static      Required

21        VLAN0021                            static      Required

30        VLAN0030                            static      Required

31        VLAN0031                            static      Required

91        VLAN0011       1/e1-e2              static      Not Required

3978      Guest VLAN     1/e17                guest       -
```

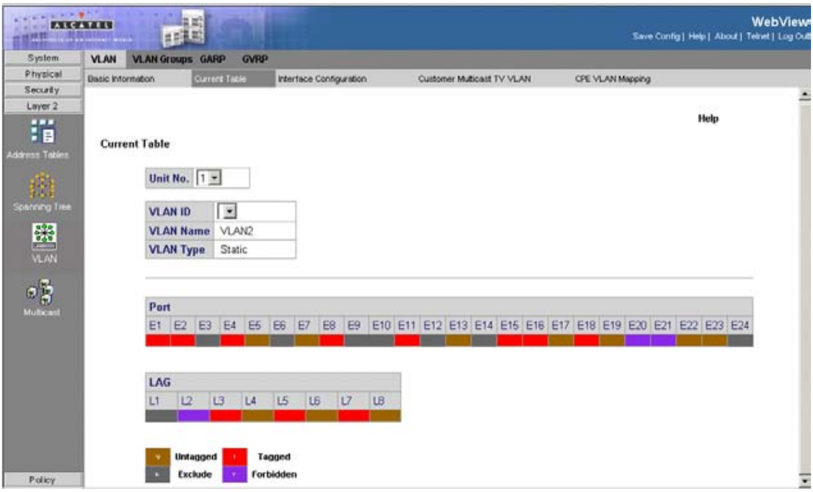
Defining VLAN Membership

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups. The *Current Table Page* contains parameters for defining VLAN groups:

Command Attributes

- **Unit No.** — Indicates the stacking member for which the Current Table information is displayed.
- **VLAN ID** — Displays the user-defined VLAN ID.
- **VLAN Name** — Displays the name of the VLAN.
- **VLAN Type** — Indicates the VLAN type. The possible field values are:
  - *Dynamic* — The VLAN was dynamically created through GARP.
  - *Static* — The VLAN is user-defined.
  - *Default* — The VLAN is the default VLAN.
- **Port/LAG** — Indicates the port or LAG membership status of the VLAN. The possible values are:
  - *Untagged (Brown)* — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
  - *Tagged (Red)* — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
  - *Exclude (Gray)* — Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GARP.
  - *Forbidden (Purple)* — Denies the interface VLAN membership, even if GARP indicates the port is to be added.

Web – Click Layer 2, VLAN, VLAN, Current Table. Define the VLAN ID, VLAN Name, and VLAN type fields. and define the port settings, and click Apply.



Current Table

Unit No.	1

VLAN ID	
VLAN Name	VLAN2
VLAN Type	Static

Port

E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18	E19	E20	E21	E22	E23	E24
🟥	🟥	⬛	🟥	🟫	⬛	🟫	🟥	⬛	⬛	🟥	⬛	🟫	⬛	🟥	🟥	🟫	🟥	🟫	🟪	🟪	🟫	🟫	⬛

LAG

L1	L2	L3	L4	L5	L6	L7	L8
⬛	🟪	🟥	🟫	🟥	🟫	🟥	🟫

🟫 Untagged 🟥 Tagged
⬛ Exclude 🟪 Forbidden

Figure 3-101. Current Table Page

CLI – The following is an example of the CLI commands used to create VLANs:

```
Console(config)# vlan database                                       4-662
Console(config-vlan)# vlan 1972                                      4-663
Console(config-if)# exit                                             4-656
Console(config)# interface vlan 19                                   4-664
Console(config-if)# name Marketing                                   4-666
Console(config-if)# exit                                             4-656
Console(config)# interface ethernet 1/e16                            4-376

Console(config-if)# switchport mode general                          4-668
Console(config-if)# switchport general allowed vlan add 2,5-6 tagged 4-672
Console(config-if)# switchport general pvid 234                      4-673
Console(config-if)# switchport forbidden vlan add 234-256            4-676

console(config-if)# switchport mode general
console(config-if)# switchport g allowed vlan add 2
console(config-if)# switch port g
console(config)# interface ethernet 1/e21
console(config-if)# switchport trunk allowed vlan re 2
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 2
console(config-if)#
```

Defining VLAN Interface Settings

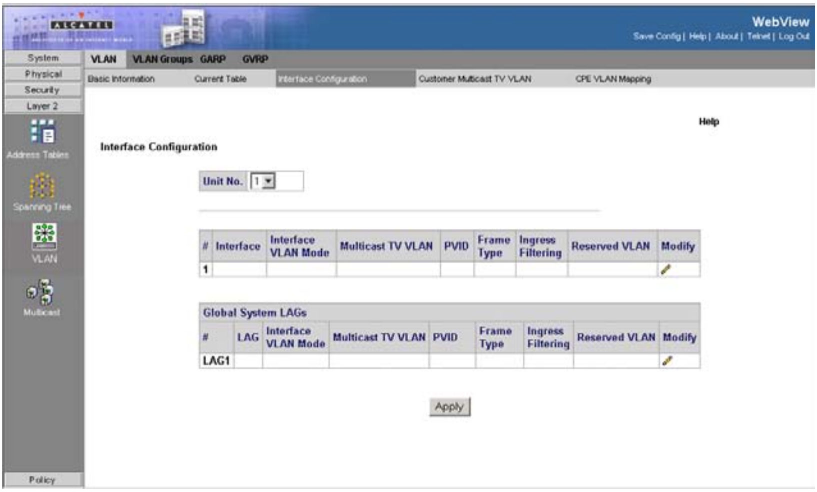
You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP. The *Interface Configuration Page* contains parameters for defining VLAN behavior for specific interfaces.

Note: After reboot the "old" system default VLAN and its associated config is removed from the system config.

Command Attributes

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Interface** — Displays the port number included in the VLAN.
- **Interface VLAN Mode** — Displays the port mode. The possible values are:
  - *General* — Indicates the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full IEEE802.1q mode).
  - *Access* — Indicates a port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port cannot be designated. Ingress filtering cannot be enabled or disabled on an access port.
  - *Trunk* — Indicates the port belongs to VLANs in which all ports are tagged, except for one port that can be untagged.
  - *Customer* — Indicates the port belongs to a customer VLAN in which all ports are double tagged. For more information, see *Configuring Customer VLANs*.
- **Multicast TV VLAN** — Indicates if a Multicast TV VLAN is enabled on the device. Multicast TV VLANs enable VLANs to receive Multicast TV transmissions from ports that are not Access ports.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 1-4094. VLAN 4095 is defined as per standard and industry practice as the Discard VLAN. Packets classified to the Discard VLAN are dropped.
- **Frame Type** — Specifies the packet type accepted on the port. The possible field values are:
  - *Admit Tag Only* — Only tagged packets are accepted on the port.
  - *Admit All* — Both tagged and untagged packets are accepted on the port.
- **Ingress Filtering**— Indicates whether ingress filtering is enabled on the port. The possible field values are:
  - *Enable* — Enables ingress filtering on the device. Ingress filtering discards packets that are defined to VLANs of which the specific port is not a member.
  - *Disable* — Disables ingress filtering on the device.
- **Reserved VLAN** — Indicates the VLAN selected by the user to be the reserved VLAN if not in use by the system.

Web – Click Layer 2, VLAN, VLAN, Interface Configuration. Define the VLAN interface settings and click Apply.



Interface Configuration

Unit No. 1

#	Interface	Interface VLAN Mode	Multicast TV VLAN	PVID	Frame Type	Ingress Filtering	Reserved VLAN	Modify
1								

Global System LAGs

#	LAG	Interface VLAN Mode	Multicast TV VLAN	PVID	Frame Type	Ingress Filtering	Reserved VLAN	Modify
LAG1								

Figure 3-102. Interface Configuration Page

CLI – The following is an example of the VLAN interface configuration :

```
Console(config)# interface ethernet 1/e16
4-376
Console(config-if)# switchport general ingress-filtering disable
4-674
Console(config-if)# switchport general acceptable-frame-type tagged-only

4-675
Console(config)# interface ethernet 1/e19
4-376
Console(config-if)# switchport access multicast-tv vlan 20
4-687
```

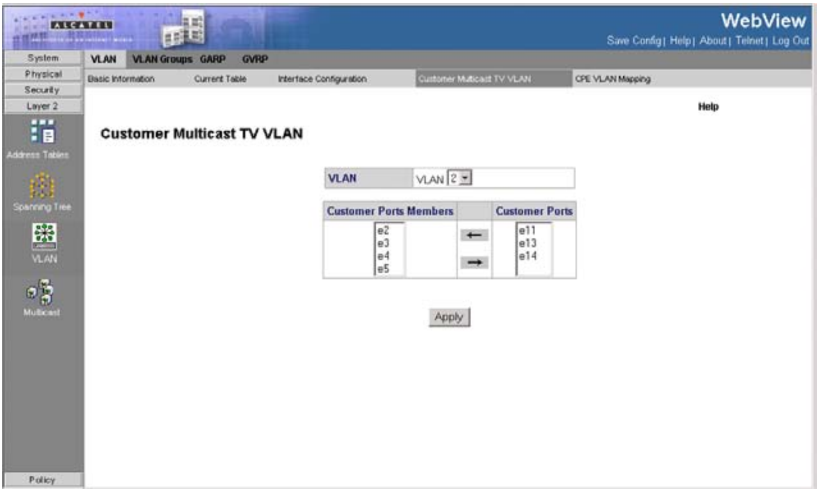
Defining Customer Mapping for Multicast TV

The *Customer Multicast TV VLAN Page* assigns ports to a Multicast TV VLAN. This is required for configuring and implementing the Triple Play functionality.

Command Attributes

- **Interface** — Defines the VLAN to which the ports are assigned.
- **Customer Ports Members** — Defines the ports already as signed to the Multicast TV VLAN.
- **Customer Ports** — Lists the ports available for assigning to the Multicast TV VLAN.

Web – Click Layer 2, VLAN, Customer Multicast TV VLAN, define the fields, and click Apply.



VLAN: VLAN 2

Customer Ports Members: e2, e3, e4, e5

Customer Ports: e11, e13, e14

Figure 3-103. Customer Multicast TV VLAN Page

CLI – The following is an example of the Customer Multicast TV VLAN CLI commands:

```
Console(config-if)# switchport customer multicast-tv vlan add 20
4-627
```

Mapping CPE VLANs

Network managers can map CPE VLANs to Multicast TV VLANs in the *CPE VLANs Mapping Page*. Once the CPE VLAN is mapped to the Multicast VLAN, the VLAN can participate in IGMP snooping.

Note: Configure Triple play only in the following order:

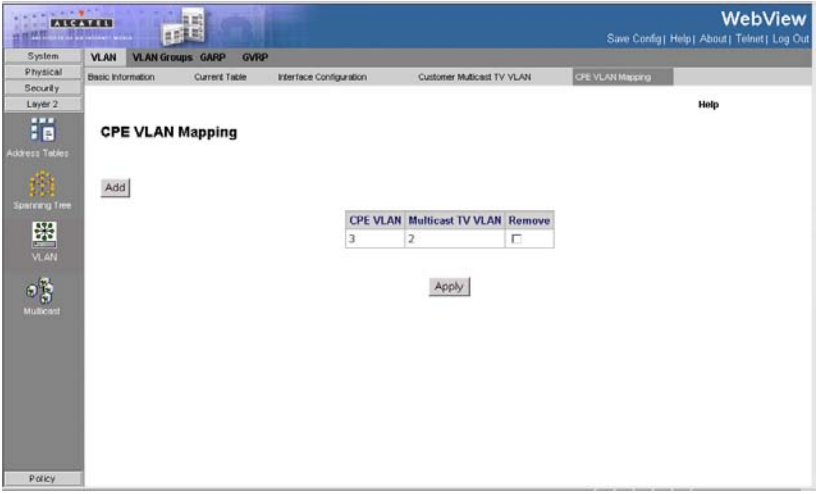
1. Configure the port as QinQ see parameter Interface VLAN Mode on the *Interface Configuration Page*.
2. Add the port to the Multicast TV LAN see *Multicast TV Membership Page*.
3. Configure the port as Triple Play see *Customer Multicast TV VLAN Page*.

Command Attributes

- **CPE VLAN** — Indicates the CPE VLAN which is mapped to the Multicast TV VLAN.
- **Multicast TV VLAN** — Indicates the CPE VLAN which is mapped to the Multicast TV VLAN.
- **Remove** — Removes the CPE VLAN to Multicast TV VLAN mapping the possible field values are:
  - *Checked* — Removes the selected CPE VLAN to Multicast TV VLAN mapping.

- *Unchecked* — Maintains all CPE VLAN to Multicast VLAN mappings.

Web – Click Layer 2, VLAN, CPE VLAN Mapping, click Add, define the fields, and click Apply.



CPE VLAN Mapping

CPE VLAN	Multicast TV VLAN	Remove
3	2	□

Figure 3-104. CPE VLANs Mapping Page

CLI – The following is an example of the Mapping CPE VLANs CLI commands:

```
Console(config)# ip igmp snooping map cpe vlan 3 multicast-tv vlan 20
4-628
```

Defining VLAN Groups

VLAN groups increase network flexibility and portability. For example, network users grouped by MAC address can log on to the network from multiple locations without moving between VLANs.

VLANs can be grouped by MAC address, Subnets, and Protocols. Once a user logs on, the system attempts to classify the user by MAC address. If the user cannot be classified by MAC address, the system attempts to classify the user by Subnet. If the subnet classification is unsuccessful, the system attempts to classify the user by protocol. If the protocol classification is unsuccessful, the user is classified by PVID.

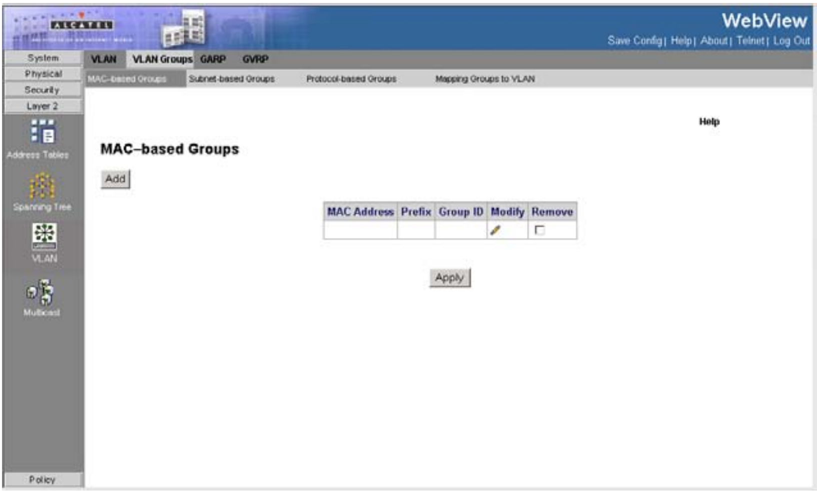
Configuring MAC Based VLAN Groups

The *MAC-Based Groups Page* contains information for defining MAC Based VLAN groups.

Command Attributes

- **MAC Address** – Defines the MAC address assigned to the VLAN group.
- **Prefix** – Defines the MAC address’s prefix. The possible field range is 0-32.
- **Group ID** – Defines the MAC based VLAN ID. The possible field range is 1 - 2147483647.
- **Remove** — If checked, deletes the MAC-Based VLAN Group.

Web – Click Layer 2, VLAN, VLAN Groups, MAC-based VLAN Groups. Define the fields and click Apply.



MAC–based Groups

MAC Address	Prefix	Group ID	Modify	Remove
			✎	□

Figure 3-105. MAC-Based Groups Page

CLI – The following is an example of the CLI commands used to create MAC Based VLAN groups:

```
console(config)# vlan database                                      4-662
console(config-vlan)# map mac 00:08:78:32:98:78 9 macs-group 1 interface
ethernet e17                                                        4-376
```

Configuring Subnet Based VLAN Groups

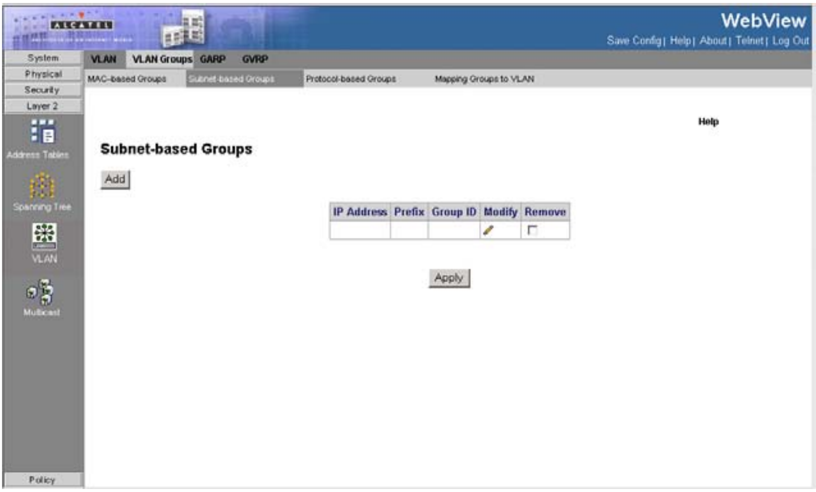
The *Subnet-Based Groups Page* contains information for defining Subnet Based VLAN groups.

Command Attributes

- **IP Address** – Defines the IP address assigned to the VLAN group.
- **Prefix** – Defines the IP address’s prefix. The possible field range is 1-32.
- **Group ID** – Defines the IP based VLAN ID. The possible field range is 1 - 2147483647.

- **Remove** — If checked, deletes the Subnet-Based VLAN Group.

Web – Click Layer 2, VLAN, VLAN Groups, Subnet-based Groups. Define the fields and click Apply.



Subnet-based Groups

IP Address	Prefix	Group ID	Modify	Remove
			✎	□

Figure 3-106. Subnet-Based Groups Page

CLI – The following is an example of the CLI commands used to create IP Based VLAN groups:

```
console(config)# vlan database                                         4-662
console(config-vlan)# map protocol ethernet protocols-group 2000       4-666
```

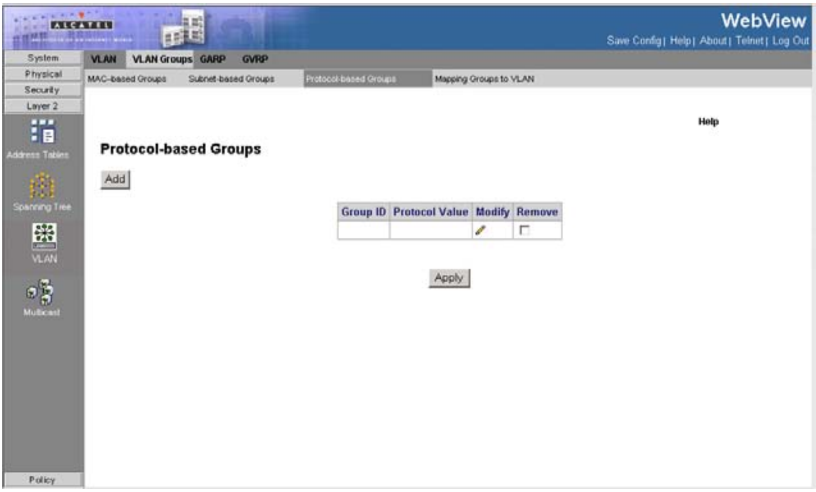
Configuring Protocol Based VLAN Groups

The *Protocol Based Groups Page* contains information regarding protocol names and the VLAN Ethernet type. Interfaces can be classified as a specific protocol based interface. The classification places the interface into a protocol group.

Command Attributes

- **Protocol Value** — User-defined protocol value.
- **Group ID** – Defines the IP based VLAN ID. The possible field range is 1 - 2147483647.
- **Remove** — If checked, deletes the Protocol Based VLAN Group.

Web – Click Layer 2, VLAN, VLAN Groups, Protocol-based Groups. Define the fields and click Apply.



Group ID	Protocol Value	Modify	Remove
		✎	□

Figure 3-107. Protocol Based Groups Page

CLI – The following is an example of the CLI commands used to create Protocol Based VLAN groups:

```
console(config)# vlan database                                        4-662
console(config-vlan)# map protocol protocols-group                    4-666
console(config-vlan)# switchport general map protocols-group vlan     4-667
console(config-vlan)# show vlan protocols-groups                      4-688
```

Mapping Groups to VLANs

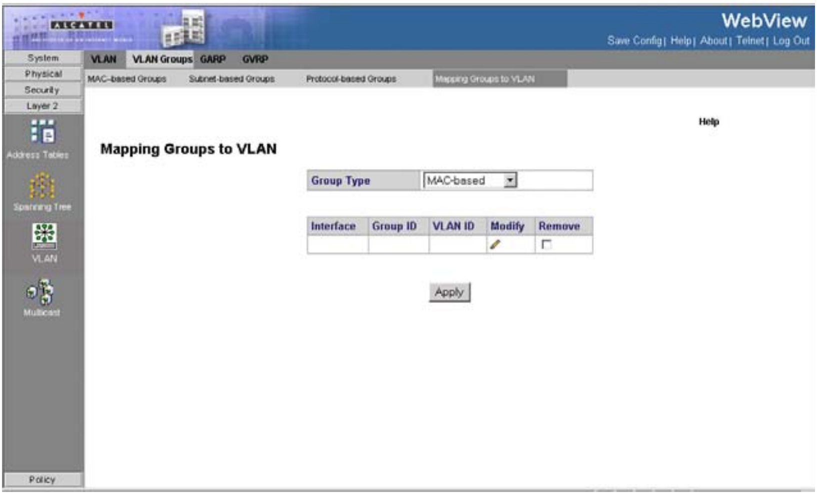
The classification places the interface into a protocol group.

Command Attributes

- **Group Type** – Defines the VLAN Group to which interfaces are mapped. The possible field values are:
  - *MAC-based* – Indicates that interfaces are mapped to MAC based VLAN groups.
  - *Subnet-based* – Indicates that interfaces are mapped to Subnet based VLAN groups.
  - *Protocol-based* – Indicates that interfaces are mapped to Protocol based VLAN groups.
- **Interface** — Indicates the interface type the VLAN group. The possible field values are:
  - *Port* — Indicates the specific port added to the VLAN group.
  - *LAG* —Indicates the specific LAG added to the VLAN group.

- **Group ID** — Defines the protocol group ID to which the interface is added.
- **VLAN ID** — Attaches the interface to a user-defined VLAN ID. VLAN group ports can either be attached to a VLAN ID or a VLAN name. The possible field range is 1-4093, and 4095 (4094 is not available for configuration).
- **Remove** — If checked, removes the VLAN Group mapping.

Web – Click Layer 2, VLAN, VLAN Groups, Mapping Groups to VLAN. Define the fields and click Apply.



Mapping Groups to VLAN

Group Type: MAC-based

Interface	Group ID	VLAN ID	Modify	Remove
			✎	□

Figure 3-108. Mapping Groups to VLAN Page

CLI – The following is an example of the CLI commands used to map interfaces to VLAN groups:

```
Console(config)# switchport general map macs-group vlan           4-677
Console(config)# switchport general map subnets-group vlan        4-679
```

Defining GARP

Generic Attribute Registration Protocol (GARP) protocol is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or multicast address. When configuring GARP, ensure the following:

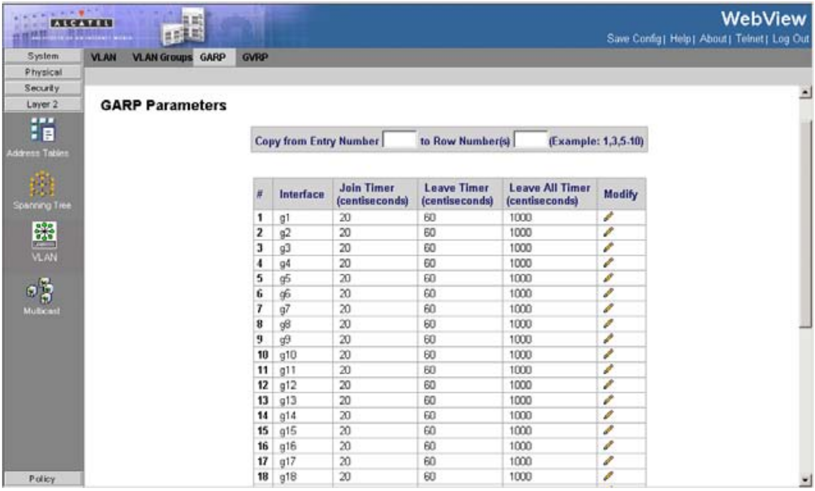
- The leave time must be greater than or equal to three times the join time.
- The leave-all time must be greater than the leave time.
- Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, the GARP application does not operate successfully.

The *GARP Configuration Page* contains parameters for defining network attributes such as VLAN or multicast addresses.

Command Attributes

- **Copy from Entry Number** — Indicates the row number from which GARP parameters are copied.
- **To Entry Number** — Indicates the row number to which GARP parameters are copied.
- **Interface** — Displays the port or LAG on which GARP is enabled.
- **Join Timer**— Indicates the amount of time, in centiseconds, that PDUs are transmitted. The default value is 20 centiseconds.
- **Leave Timer**— Indicates the amount of time lapse, in centiseconds, that 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. The default value is 60 centiseconds.
- **Leave All Timer** — Indicates the amount of time lapse, in centiseconds, that all device waits before leaving the GARP state. The leave all time must be greater than the leave time. The default value is 1000 centiseconds.

Web – Click Layer 2, VLAN, GARP. Enable or disable GARP, and click Apply.



GARP Parameters

Copy from Entry Number ______ to Row Number(s) ______ (Example: 1,3,5-10)

#	Interface	Join Timer (centiseconds)	Leave Timer (centiseconds)	Leave All Timer (centiseconds)	Modify
1	g1	20	60	1000	✎
2	g2	20	60	1000	✎
3	g3	20	60	1000	✎
4	g4	20	60	1000	✎
5	g5	20	60	1000	✎
6	g6	20	60	1000	✎
7	g7	20	60	1000	✎
8	g8	20	60	1000	✎
9	g9	20	60	1000	✎
10	g10	20	60	1000	✎
11	g11	20	60	1000	✎
12	g12	20	60	1000	✎
13	g13	20	60	1000	✎
14	g14	20	60	1000	✎
15	g15	20	60	1000	✎
16	g16	20	60	1000	✎
17	g17	20	60	1000	✎
18	g18	20	60	1000	✎

Figure 3-109. GARP Configuration Page

CLI – The following is an example of the GARP configuration commands:

```
Console(config)# interface ethernet 1/e6
4-376
Console(config-if)# garp timer leave 900
4-401
```

Defining GVRP

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

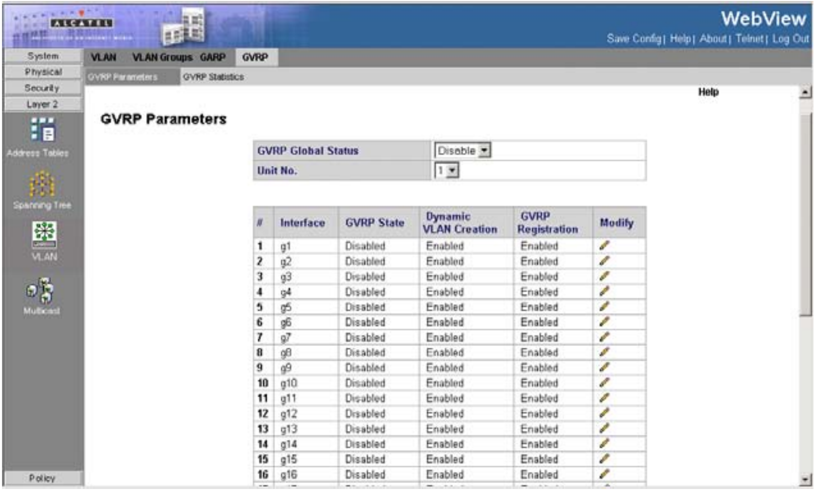
The *GVRP Parameters Page* is divided into port and LAG parameters. The field definitions are the same.

Command Attributes

- **GVRP Global Status** — Indicates if GVRP is enabled on the device. The possible field values are:
  - *Enable* — Enables GVRP on the selected device.
  - *Disable* — Disables GVRP on the selected device.
- **Unit No.** —Indicates the stacking member for which the Multiple Hosts information is displayed.
- **Interface** — Displays the port on which GVRP is enabled. The possible field values are:
  - *Port* — Indicates the port number on which GVRP is enabled.
  - *LAG* — Indicates the LAG number on which GVRP is enabled.
- **GVRP State**— Indicates if GVRP is enabled on the port. The possible field values are:
  - *Enabled* — Enables GVRP on the selected port.
  - *Disabled* — Disables GVRP on the selected port.
- **Dynamic VLAN Creation** — Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
  - *Enabled* — Enables Dynamic VLAN creation on the interface.
  - *Disabled* — Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** — Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
  - *Enabled* — Enables GVRP registration on the device.
  - *Disabled* — Disables GVRP registration on the device.
- **Global System LAGs** — Displays the same field information as the ports, but represent the LAG RSTP.

Web – Click Layer 2, VLAN, VLAN, GVRP Parameters, define the fields, and click

Apply.



GVRP Parameters

GVRP Global Status	Disable
Unit No.	1

#	Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration	Modify
1	g1	Disabled	Enabled	Enabled	✎
2	g2	Disabled	Enabled	Enabled	✎
3	g3	Disabled	Enabled	Enabled	✎
4	g4	Disabled	Enabled	Enabled	✎
5	g5	Disabled	Enabled	Enabled	✎
6	g6	Disabled	Enabled	Enabled	✎
7	g7	Disabled	Enabled	Enabled	✎
8	g8	Disabled	Enabled	Enabled	✎
9	g9	Disabled	Enabled	Enabled	✎
10	g10	Disabled	Enabled	Enabled	✎
11	g11	Disabled	Enabled	Enabled	✎
12	g12	Disabled	Enabled	Enabled	✎
13	g13	Disabled	Enabled	Enabled	✎
14	g14	Disabled	Enabled	Enabled	✎
15	g15	Disabled	Enabled	Enabled	✎
16	g16	Disabled	Enabled	Enabled	✎

Figure 3-110. GVRP Parameters Page

CLI – The following is an example of the GVRP configuration commands:

```
Console(config)# gvrp enable
4-399
Console(config)# interface ethernet 1/e6
4-376
Console(config-if)# gvrp enable
4-399
Console(config-if)# gvrp vlan-creation-forbid
4-402
Console(config-if)# gvrp registration-forbid
4-402
```

Viewing GVRP Statistics

The *GVRP Statistics Page* contains device statistics for GVRP.

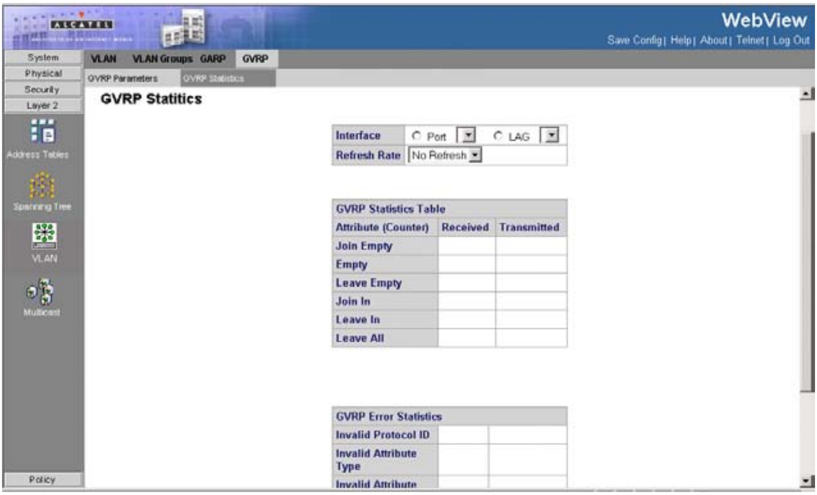
Command Attributes

- **Interface**—Specifies the interface type for which the statistics are displayed.
  - *Port*—Indicates port statistics are displayed.
  - *LAG*—Indicates LAG statistics are displayed.
- **Refresh Rate**—Indicates the amount of time that passes before the GVRP statistics are refreshed. The possible field values are:
  - *15 Sec*—Indicates that the GVRP statistics are refreshed every 15 seconds.
  - *30 Sec*—Indicates that the GVRP statistics are refreshed every 30 seconds.
  - *60 Sec*—Indicates that the GVRP statistics are refreshed every 60 seconds.

- *No Refresh*—Indicates that the GVRP statistics are not refreshed.

- **Join Empty**—Displays the device GVRP Join Empty statistics.
- **Empty**—Displays the device GVRP Empty statistics.
- **Leave Empty**—Displays the device GVRP Leave Empty statistics.
- **Join In**—Displays the device GVRP Join In statistics.
- **Leave In**—Displays the device GVRP Leave in statistics.
- **Leave All**—Displays the device GVRP Leave all statistics.
- **Invalid Protocol ID**—Displays the device GVRP Invalid Protocol ID statistics.
- **Invalid Attribute Type**—Displays the device GVRP Invalid Attribute ID statistics.
- **Invalid Attribute Value**—Displays the device GVRP Invalid Attribute Value statistics.
- **Invalid Attribute Length**—Displays the device GVRP Invalid Attribute Length statistics.
- **Invalid Event**—Displays the device GVRP Invalid Event statistics.

Web – Click Layer 2, VLAN, VLAN, GVRP Statistics. Enable or disable GVRP, define the fields, and click Apply.



GVRP Statitics

Interface	○ Port	○ LAG
Refresh Rate	No Refresh	

GVRP Statistics Table		
Attribute (Counter)	Received	Transmitted
Join Empty		
Empty		
Leave Empty		
Join In		
Leave In		
Leave All		

GVRP Error Statistics		
Invalid Protocol ID		
Invalid Attribute Type		
Invalid Attribute		

Figure 3-111. GVRP Statistics Page

CLI – The following is an example of the GVRP statistics commands:

```
Console# show gvrp statistics
4-405



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
```

Multicast Filtering

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

This section contains information for configuring Multicast forwarding and Multicast TV, and includes the following sections:

- Defining IGMP Snooping
- Specifying Static Interfaces for a Multicast Group
- Displaying Interfaces Attached to a Multicast Router
- Configuring Multicast TV
- Defining Multicast TV Membership

Defining IGMP Snooping

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch or router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering. The IGMP Snooping Querier is used to support IGMP snooping where the multicast traffic is not routed.

The purpose of IP multicast filtering is to optimize a switched network’s performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN). The user can set the IGMP Querier mode to either V2 or V3. (Default is V2). When working in IGMPv3 mode and detecting an IGMPv2 message, the switch will automatically change its mode to IGMPv2.

The *IGMP Snooping Page* contains parameters for configuring switches to forward multicast traffic.

Command Attributes

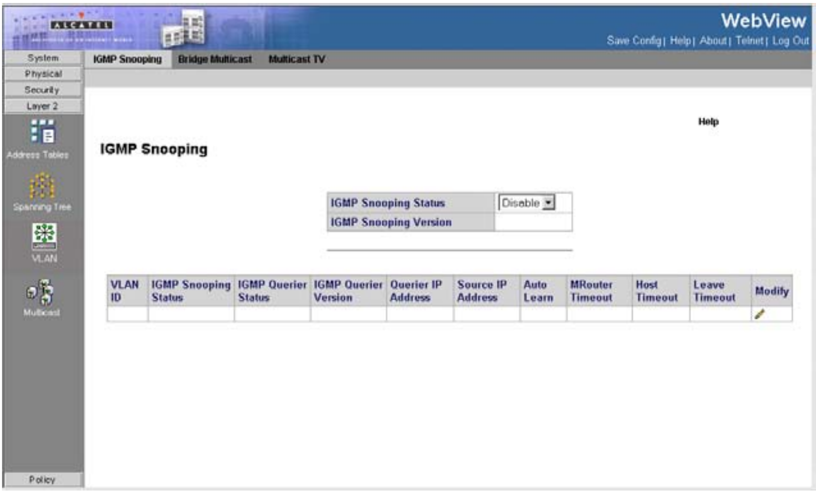
Global Parameters

- **IGMP Snooping Status** — Indicates that the switch monitors network traffic to determine which hosts want to receive multicast traffic.
- **IGMP Snooping Version** — Displays the IGMP Snooping version enabled on the device.

VLAN-level Parameters

- **VLAN ID** — VLAN number of the VLAN on which IGMP is enabled.
- **IGMP Snooping Status** — Indicates if IGMP snooping is enabled on the VLAN. When enabled the switch will monitors network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Disperformance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN). The possible field values are:
  - *Enable* — Enables IGMP Snooping on the VLAN.
  - *Disable* — Disables IGMP Snooping on the VLAN.
- **IGMP Querier Status** — Indicates if the specific VLAN can operate as an IGMP Querier. The possible field values are:
  - *Enable* — Enables IGMP Querying on the VLAN.
  - *Disable* — Disables IGMP Querying on the VLAN.
- **IGMP Querier Version** — Indicates the version of IGMP in the VLAN. The possible values are:
  - *IGMPv2* — Version 2 of the IGMP protocol.
  - *IGMPv3* — The latest version of the IGMP protocol.
- **Querier IP Address** — IP address of the interface which serves as the querier on the VLAN.
- **Source IP address** — Defines the interface source IP address from which queries are sent.
- **Auto Learn** — Indicates if Auto Learn is enabled on the device. If Auto Learn is enabled, the device automatically learns where other Multicast groups are located. Enables or disables Auto Learn on the Ethernet device. The possible field values are:
  - *Enable* — Enables auto learn
  - *Disable* — Disables auto learn.
- **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.
- **Host Timeout** — Indicates the amount of time host waits to receive a message before timing out. The default time is 260 seconds.
- **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic. The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds.

Web – Click Layer 2, Multicast, IGMP Snooping. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)



IGMP Snooping

IGMP Snooping Status	Disable
IGMP Snooping Version	

VLAN ID	IGMP Snooping Status	IGMP Querier Status	IGMP Querier Version	Querier IP Address	Source IP Address	Auto Learn	MRouter Timeout	Host Timeout	Leave Timeout	Modify
										✎

Figure 3-112. IGMP Snooping Page

CLI – The following is an example of the IGMP CLI commands:

```
console(config)# bridge multicast filtering
4-315
console(config)# ip igmp snooping
4-408
```

Specifying Static Interfaces for a Multicast Group

The *Multicast Group Page* displays the ports and LAGs attached to the Multicast service group in the Ports and LAGs tables. The Port and LAG tables also reflect the manner in which the port or LAGs joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The *Multicast Group Page* permits new Multicast service groups to be created. The *Multicast Group Page* also assigns ports to a specific Multicast service address group.

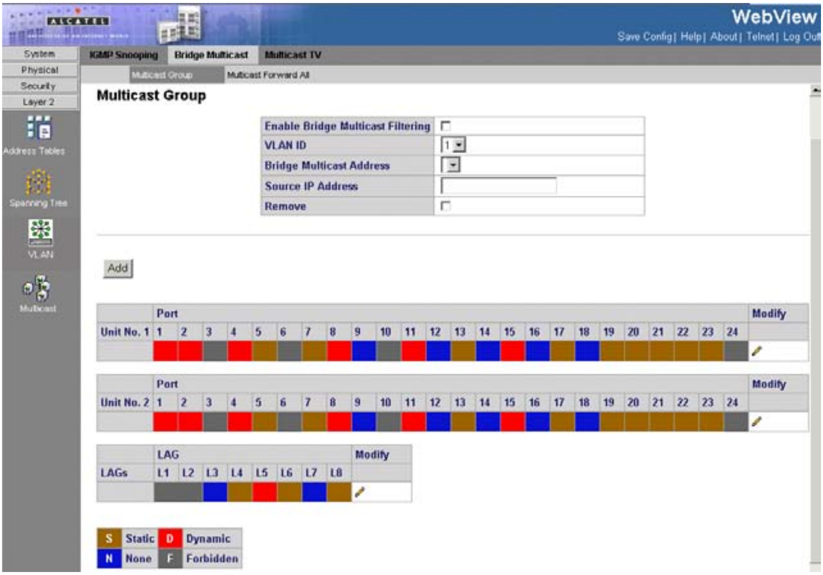
The IGMP port and LAG members management settings are:

- **D** — Dynamically joins ports/LAG to the Multicast group in the *Current* Row.
- **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 ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
- **N** — The port is not attached to a Multicast group.

Command Attributes

- **Enable Bridge Multicast Filtering** — Indicate if bridge Multicast filtering is enabled on the device. The possible field values are:

  - *Checked* — Enables Multicast filtering on the device.
  - *Unchecked* — Disables Multicast filtering on the device. If Multicast filtering is disabled, Multicast frames are flooded to all ports in the relevant VLAN. Disabled is the default value.
- **VLAN ID** — Identifies a VLAN and contains information about the Multicast group address.
- **Bridge Multicast Address** — Identifies the Multicast group MAC address/IP address.
- **Ports** — Displays Port that can be added to a Multicast group.
- **LAGs** — Displays LAGs that can be added to a Multicast Group.



Multicast Group

Enable Bridge Multicast Filtering	□
VLAN ID	1 ▾
Bridge Multicast Address	▾
Source IP Address	
Remove	□

	Port																								Modify
Unit No. 1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
	🟥	🟥	⬛	🟥	🟫	⬛	🟫	🟥	🟦	⬛	🟥	🟦	🟫	🟦	🟥	🟦	🟫	🟦	🟫	🟫	🟫	🟫	🟫	⬛	✎

	Port																								Modify
Unit No. 2	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
	🟥	🟥	⬛	🟥	🟫	⬛	🟫	🟥	🟦	⬛	🟥	🟦	🟫	🟦	🟥	🟦	🟫	🟦	🟫	🟫	🟫	🟫	🟫	⬛	✎

	LAG								Modify
LAGs	L1	L2	L3	L4	L5	L6	L7	L8	
	⬛	⬛	🟦	🟫	🟥	🟫	🟦	🟫	✎

S	Static	D	Dynamic
N	None	F	Forbidden

Figure 3-113. Multicast Group Page

CLI – The following is an example of the Multicast Group CLI commands:

```
Console(config-if)# bridge multicast address 0100.5e02.0203 add
ethernet 1/e11,1/e12
4-316
Console(config-if)# end
4-657
Console# show bridge multicast address-table
4-327


Vlan        MAC Address                     Type          Ports

----        -----------                     -----         ----------
```

```
1            0100.5e02.0203                static        1/e11, 1/
                                                         e12

19           0100.5e02.0208                static        1/e11-16

19           0100.5e02.0208                dynamic       1/e11-12


Forbidden ports for multicast addresses:


Vlan         MAC Address                   Ports

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

1            0100.5e02.0203                1/e8

19           0100.5e02.0208                1/e8
```

Displaying Interfaces Attached to a Multicast Router

The *Multicast Forward All Page* contains fields for attaching ports or LAGs to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN. Unless LAGs are defined, only a Multicast Forward All table displays.

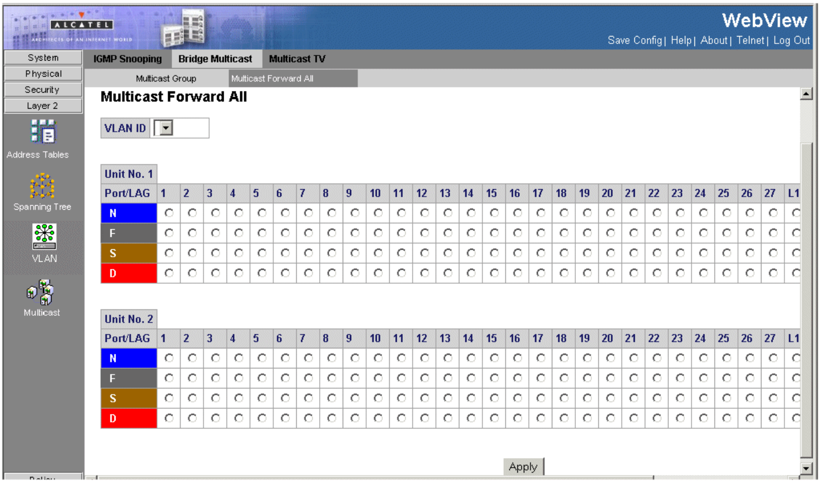
The following table summarizes the Multicast settings which can be assigned to ports in the *Multicast Forward All Page*:

- **D** — Attaches the port to the Multicast router or switch as a dynamic port.
- **S** — Attaches the port to the Multicast router or switch as a static port.
- **F** — Forbidden.
- **N** — The port is not attached to a Multicast router or switch.

Command Attributes

- **VLAN ID** — DIsplays the VLAN for which Multicast parameters are displayed.
- **Ports** — Ports that can be added to a Multicast service.
- **LAGs** — LAGs that can be added to a Multicast service.

Web – Click Layer 2, Multicast, Bridge Multicast, Multicast Forward All. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.



Multicast Forward All

VLAN ID

Unit No. 1

Port/LAG	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	L1
N	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
F	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
S	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
D	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Unit No. 2

Port/LAG	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	L1
N	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
F	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
S	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
D	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 3-114. Multicast Forward All Page

CLI – The following is an example of the Multicast Forward All CLI commands:

```
Console (config)# interface vlan 1
4-664
Console (config-if)# bridge multicast forward-all add ethernet 1/e3

4-319
```

Configuring Multicast TV

Multicast TV allows subscribers to join the same Multicast stream, even if the subscribers are not members of the same VLAN, eliminating television traffic duplication. Ports which receive Multicast Transmissions, or *Receiver Ports*, can be defined in any VLAN, and not just in the Multicast VLAN. Receiver ports can only receive Multicast transmissions, they cannot initiate a Multicast TV transmission. Multicast TV source ports must be a Multicast VLAN members.

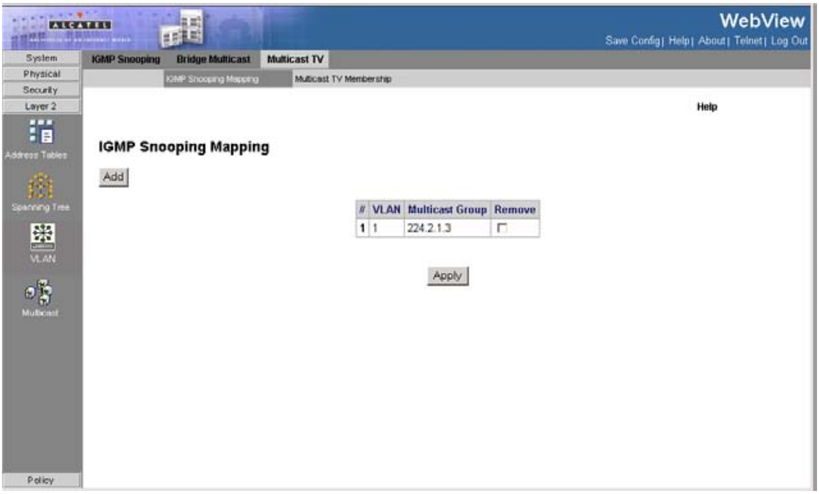
IGMP messages are used to indicate which ports are requesting to join or leave the Multicast group. The *IGMP Snooping Mapping Page* allows network managers to map IGMP snooping to VLANs.

Command Attributes

- **VLAN** — Defines the VLAN attached to the for which the IGMP Snooping mapping is defined.
- **Multicast Group** — Defines the Multicast group IP addressed mapped to the VLAN.
- **Remove** — Removes Multicast TV IGMP mappings. The possible field values are:

- *Checked* — Removes the specific IGMP mapping from the selected VLAN.
- *Unchecked* — Maintains the IGMP mapping.

Web – Click Layer 2, Multicast, Multicast TV, IGMP Snooping Mapping, click Add, define the fields, and click Apply.



IGMP Snooping Mapping

#	VLAN	Multicast Group	Remove
1	1	224.2.1.3	□

Figure 3-115. IGMP Snooping Mapping Page

CLI – The following is an example of the Multicast Forward All CLI commands:

```
console(config)# interface ethernet 1/e21
console(config-if)# switchport access multicast-tv vlan VLAN_ID VLAN ID
of the Multicast TV VLAN
console(config-if)# switchport access multicast-tv vlan 2
console(config-if)# ec % Unrecognized command
console(config-if)# ex
console(config)# IP igmp snooping multicast-tv vlan vlan
console(config)# IP igmp snooping multicast-tv vlan VLAN_ID VLAN ID value
console(config)# IP igmp snooping multicast-tv vlan 2 add add IP
multicast address to multicast-tv vlan remove remove IP multicast address
from multicast-tv vlan
console(config)# IP igmp snooping multicast-tv vlan 2 add A.B.C.D IP
multicast address
console(config)# IP igmp snooping multicast-tv vlan 2 add 224.2.2.2 count
Configure multiple contiguous multicast IP address <cr>
console(config)# IP igmp snooping multicast-tv vlan 2 add 224.2.2.2
console(config)#
```

Defining Multicast TV Membership

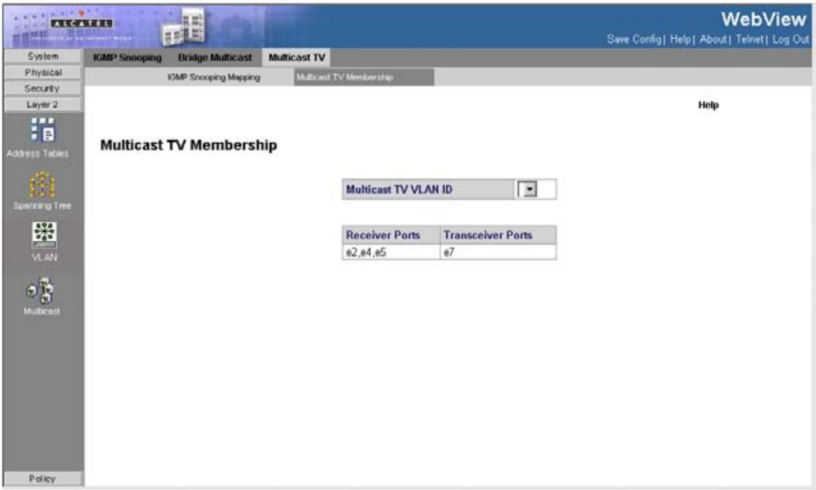
The *Multicast TV Membership Page* allows network managers to display the ports associated with a Multicast TV VLAN.

Note: Ports and trunks are assigned to Multicast VLAN in the Interface Configuration Page.

Command Attributes

- **Multicast TV VLAN ID** — Indicates the Multicast VLAN ID to which the source ports and receiver ports are members.
- **Receiver Ports** — Indicates the port on which Multicast TV transmissions are received.
- **Transceiver Ports** — Indicates the source port from which the Multicast TV transmission originates. The source port is learned through the IGMP messages.

Web – Click Layer 2, Multicast, Multicast TV, Multicast TV Membership, click Add, define the fields, and click Apply.



Multicast TV Membership

Multicast TV VLAN ID

Receiver Ports	Transceiver Ports
e2,e4,e5	e7

Figure 3-116. Multicast TV Membership Page

CLI – The following is an example of the Multicast TV Membership CLI commands:

```
console(config)# switchport customer vlan  10
4-627
Console# show vlan multicast-tv vlan 1000
4-690

Source ports   Receiver Ports
-------------  -----------------------------------------
1/8, 1/9      2/1-18, 3/1-18, 4/1-18
```

Configuring Triple Play

Network Manager can enhance Multicast TV services using the Triple Play

Technology. Triple Plays services catapult networking into the next generation of IT services by combining cable television, VoIP, and high speed internet connections via a single cable. Triple Play service ensure that Layer 2 isolation between subscribers remains intact.

Service provider packets sent to the subscriber arrive from the following VLAN types:

- Subscriber VLANs
- Multicast TV VLANs

Each subscriber on a network maintains a Customer Premise Equipment Multi-Connect (CPE MUX) box. The MUX boxes directs network traffic from uplink ports to MUX access ports. MUX access ports are based on VLAN tags located in packet headers. Service provider's packets are tagged twice. Each packet has an internal tag and an external tag. The external tag indicates if the packet arrived from a Multicast TV VLAN or from a subscriber's VLAN. The internal tag indicates the port within the VLAN to which the packet is addressed.

The VLAN tag identifies:

- The media service type, including:
  - Internet
  - TV
  - Phone
- The service provider.

Configuring Quality of Service

Network traffic is usually unpredictable, and the only basic assurance that can be offered is best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance and entails two basic facilities:

- Classifying incoming traffic into handling classes, based on an attribute, including:
  - The ingress interface
  - Packet content
  - A combination of these attributes
- Providing various mechanisms for determining the allocation of network resources to different handling classes, including:
  - The assignment of network traffic to a particular hardware queue
  - The assignment of internal resources
  - Traffic shaping

In this document, the terms Class of Service (CoS) and QoS are used in the following context:

- CoS provides varying Layer 2 traffic services. CoS refers to classification of traffic to traffic-classes, which are handled as an aggregate whole, with no per-flow settings. CoS is usually related to the 802.1p service that classifies flows according to their Layer 2 priority, as set in the VLAN header.
- QoS refers to Layer 2 traffic and above. QoS handles per-flow settings, even within a single traffic class.

The QoS facility involves the following elements:

- **Access Control Lists (ACLs)** — Used to decide which traffic is allowed to enter the system, and which is to be dropped. Only traffic that meets this criteria are subject to CoS or QoS settings. ACLs are used in QoS and network security.
- **Traffic Classification** — Classifies each incoming packet as belonging to a given traffic class, based on the packet contents and/or the context.
- **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, as defined by the classification mechanism.
- **Traffic Class-Handling Attributes** — Applies QoS/CoS mechanisms to different classes, including:
  - Bandwidth Management
  - Shaping/ Rate Limiting
  - Policing

Access Control Lists

the first element of the QoS facility is the Access Control Lists (ACLs) which inspects incoming packets and classify them into logical groups, based on various criteria. ACL groups have specific actions that are carried out on every packet that is classified to the group. ACLs enable actions which include:

- Forward
- Deny
- Deny and disable port

ACLs are used for the following main purposes:

- As a security mechanism, either permitting or denying entry to packets in a group. This mechanism is described in the section on Network Security.
- As a mechanism to classify packets into traffic classes for which various CoS/QoS handling actions are executed.

ACLs contain multiple classification rules and actions. An Access Control Element (ACE) is composed of a single classification rule and its action. A single ACL may contain one or more ACEs.

The order of the ACEs within an ACL is important, as they are applied in a first-fit manner. The ACEs are processed sequentially, starting with the first ACE. When a packet is matched to an ACE classification, the ACE action is performed and the ACL processing terminates. If more than one ACL is to be processed, the default drop action is applied only after processing all the ACLs. The default drop action requires the user to explicitly allow all the traffic that is permitted, including management traffic, such as telnet, HTTP, or SNMP that is directed to the router itself.

Two types of ACLs are defined:

- **IP ACL** — Applies only to IP packets. All classification fields are related to IP packets.
- **MAC ACL** — Applies to any packet, including non-IP packets. Classification fields are based only on Layer 2.

There are two ways to apply ACLs to an interface:

- **Policy** — In this form, ACLs are grouped together into a more complex structure, called a policy. The policy can contain both ACLs and QoS rules. The user can apply the policy to an interface (see “Advanced QoS Mode”).
- **Simple** — In the simple form, a single (MAC or IP) ACL is applied to an interface. Although a policy cannot be applied to an interface, it is possible to apply basic QoS rules that classify packets to output queues (see “Basic QoS Mode”).

Mapping to Queues

Queues are used in both Basic and Advanced QoS modes. Default settings are applied to maps in Service QoS mode. A Trust Behavior can be selected, or the output service fields can be selected, including:

- **VLAN Priority Tags (VPT)** — VPTs are mapped to an output queues based on the VPT. While queue mapping is user-configurable, the VPT default mapping to the output queue is as follows. In the VPT default mapping, Queue 2 has the lowest priority. The following table contains the VPT to Queue default settings:

Table 3-5. VPT Default Mapping Table

VPT Value	Queue Number
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

Notes:1. Mapping of the VPT to the output queue is performed on a system-wide basis, and can be *enabled* or *disabled* per port.

2. Packets may egress with a different VLAN Priority Tag than the one with which they ingressed. A different tag may be applied to the packets. If no QoS mode is configured, then the VPT for tagged packets remains unchanged. For untagged traffic, a VPT is assigned. When VPT trust mode is configured, untagged packets are mapped to the default port VPT.

- **Default CoS** — Packets arriving untagged are assigned to a default VPT, which can be set by the user on a per port basis. Once the VPT is assigned, the packet is treated as if it had arrived with this tag. The VPT mapping to the output queue is based on the same user-defined 802.1p tag-based definitions.
- **DSCP** — The user can configure the system to use the IP DSCP of the incoming packet to the output priority queues. The mapping of the IP DSCP to priority queue is set on a per system basis. If this mode is active, a non-IP packet is always classified to the best effort queue. The default mapping is shown in the following table:

Table 3-6. DSCP Default Mapping Table

DSCP Value	Queue Number
0-15	q1 (Lowest Priority)
16-31	q2
32-47	q3
48-64	q4

All network traffic which is not assigned a DSCP value is forwarded with Best Effort service.

After packets are assigned to a specific queue, using the chosen classification method various services can be applied. Scheduling for output queues can be configured, including:

- Strict priority.
- Weighted Round Robin (WRR)

Scheduling schemes are specified per system. For each interface or queue, the following output shaping can also be configured:

- Committed Information Rate (CIR)

QoS Modes

The device supports the following QoS modes:

- Basic QoS Mode
- Advanced QoS Mode

Note: When moving to and from basic and advanced QoS modes, some settings may be lost.

Basic QoS Mode

Basic Mode supports activating one of the following Trust settings:

- VLAN Priority Tag
- DiffServ Code Point
- None

In addition, a single MAC-based or IP-based ACL can be attached directly to the interface (see Defining QoS Class Maps for more information). Only packets that have a Forward action are assigned to the output queue, based on the specified classification. By properly configuring the output queues, the following basic mode services can be set:

- **Minimum Delay** — The queue is assigned to a strict priority policy, and traffic is assigned to the highest priority queue.
- **Best Effort** — Traffic is assigned to the lowest priority queue
- **Bandwidth Assignments** — Bandwidths are assigned by configuring the WRR scheduling scheme.

Advanced QoS Mode

Advanced QoS mode provides rules for specifying flow classification and assigning rule actions that relate to bandwidth management.

In advanced QoS mode, ACLs can be applied directly to an interface. However, a policy and ACL cannot be simultaneously applied to an interface. Deny is the default action for packets not matched to a policy classification. Deny All is the default action for packets not matching any of the classifications within the policy.

After assigning packets to a specific queue, services such as configuring output queues for the scheduling scheme, or CIR, per interface can be applied. Note that packets may egress with a different VPT tag than that with which they ingressed. Packets are always assigned a VPT tag of 0 or 1 at the egress. When using trust VPT this caveat does not exist, and packets egress with the same VPT with which they ingressed. When configuring the system to work in Advanced Quality of Service Mode, the system remains in “Trust DSCP” mode.

Enabling QoS

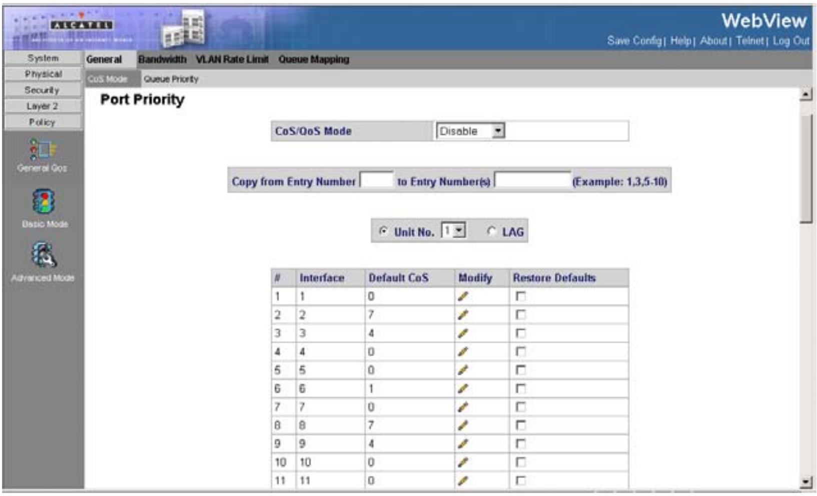
The *CoS Mode Page* contains fields for enabling or disabling QoS.

Command Attributes

- **CoS/QoS Mode** — Indicates if QoS is enabled on the device. The possible values are:
  - *Basic* — Enables QoS on the interface.
  - *Disable* — Disables QoS on the interface.
  - *Advanced* — Enables QoS Advanced mode on the interface.
- **Copy from Entry Number** — Copies the port QoS information from the selected port.
- **To Entry Number** — Indicates the port to which the port QoS information is copied.
- **Unit No./LAG** — Select whether the displayed information refers to one of the stacked member devices (**Unit No.**) or to a **LAG**.
- **Interface** — Displays the interface for which the global QoS parameters are defined.
  - *Port* — Selects the port for which the global QoS parameters are defined.
  - *LAG* — Selects the LAG for which the global QoS parameters are defined.

- **Default CoS** — Determines the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are *0-7*. The default CoS is *0*.
- **Restore Defaults** — Restores the factory QoS default settings to the selected port.
  - *Checked* — Restores the factory QoS default settings to the ports.
  - *Unchecked*— Maintains the current QoS settings.

Web – Click Policy, General QoS, General, CoS Mode, define the fields, and click Apply.



Port Priority

CoS/QoS Mode: Disable

Copy from Entry Number [ ] to Entry Number(s) [ ] (Example: 1,3,5-10)

● Unit No. 1 ○ LAG

#	Interface	Default CoS	Modify	Restore Defaults
1	1	0	✎	□
2	2	7	✎	□
3	3	4	✎	□
4	4	0	✎	□
5	5	0	✎	□
6	6	1	✎	□
7	7	0	✎	□
8	8	7	✎	□
9	9	4	✎	□
10	10	0	✎	□
11	11	0	✎	□

Figure 3-117. CoS Mode Page

CLI – The following is an example of the CLI commands used to enable QoS:

```
Console(config)# qos
4-468
```

Defining Global Queue Settings

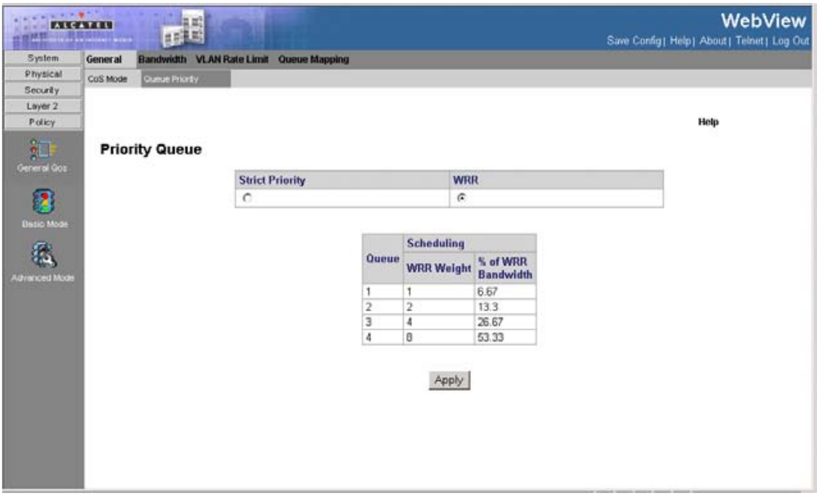
The *Queue Priority Page* contains fields for defining the QoS queue forwarding types. The queue settings are set system wide.

Command Attributes

- **Queue** — Displays the queue for which the queue settings are displayed. The possible range is 1-4.
- **Strict Priority** — Indicates that traffic scheduling for the system is based strictly on the queue priority.
- **WRR —** Indicates that traffic scheduling for the selected queue is based strictly on the WRR. If WRR is selected, the predetermined weights 8, 2, 4, and 1 are assigned to queues 4,3,2 and 1.

- **WRR Weight** — Assigns WRR weights to queues. This field shows the wrr weight assigned to the queue. This field can not be modified.
- **% of WRR Bandwidth** — Indicates the amount of bandwidth assigned to the QoS queue.

Web – Click Policy, General QoS, General, Queue Priority. Define the fields, and click Apply.



Priority Queue

Strict Priority	WRR
○	●

Queue	Scheduling	
	WRR Weight	% of WRR Bandwidth
1	1	6.67
2	2	13.3
3	4	26.67
4	8	53.33

Figure 3-118. Queue Priority Page

CLI – The following is an example of the CLI commands used to enable QoS:

```
console(config)# priority-queue out num-of-queues 4
4-482
```

Defining Bandwidth Settings

The *Bandwidth Configuration Page* allows network managers to define the bandwidth settings for specified egress and ingress interfaces. Modifying queue scheduling affects the queue settings globally.

Rate Limits and Shaping are defined per interface:

- Rate Limit sets the maximum bandwidth allowed on an interface.
- Shaping of network traffic may be defined over LAGs. LAGs can accommodate GE and FE interfaces.

Command Attributes

- **Unit No.** — Indicates the stacking member for which this bandwidth configuration is displayed.
- **Interface** — Indicates the interface for which this bandwidth information is displayed. The possible field values are:

  - *Port* — Indicates the port for which the bandwidth settings are displayed.
  - *LAG* — Indicates the LAG for which the bandwidth settings are displayed.
- **Ingress Rate Limit** — Indicates the traffic limit for ingress interfaces. The possible field values are:
  - *Status — Enables* or *Disables* rate limiting for ingress interfaces. Disable is the default value.
  - *Rate Limit* — Defines the rate limit for ingress ports. The possible field values are:

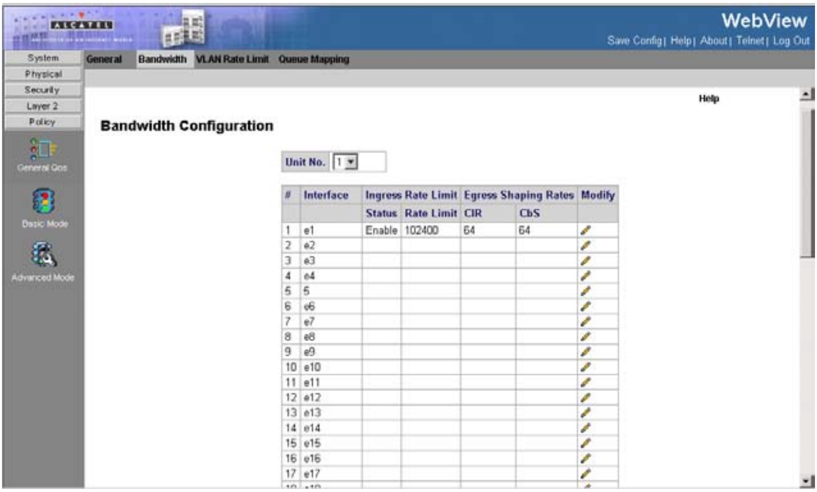
Interface	Rate
FE	70 Kbps - 1 Gbps, depending on the maximum port speed.
GE	3.5 Mbps - 1 Gbps, depending on the maximum port speed.

- **Egress Shaping Rates** — Indicates the traffic shaping type, if enabled, for egress ports. The possible field values are:
  - *CIR* — Defines Committed Information Rate *(*CIR) as the queue shaping type. The possible field values are:

Interface	Rate
FE	0-62.5 Mbps
GE	64 Kbps - 1 Gbps

  - *CbS* — Defines Committed Burst Size (CbS) as the queue shaping type. CbS is supported only on GE interfaces. The possible field values are 4 Kbps - 16 Mbps.

Web – Click Policy, General QoS, Bandwidth Configuration. Define the fields, and click Apply.



Bandwidth Configuration

Unit No. 1

#	Interface	Ingress Rate Limit		Egress Shaping Rates		Modify
		Status	Rate Limit	CIR	CbS	
1	e1	Enable	102400	64	64	✎
2	e2					✎
3	e3					✎
4	e4					✎
5	5					✎
6	e6					✎
7	e7					✎
8	e8					✎
9	e9					✎
10	e10					✎
11	e11					✎
12	e12					✎
13	e13					✎
14	e14					✎
15	e15					✎
16	e16					✎
17	e17					✎

Figure 3-119. Bandwidth Configuration Page

CLI – The following is an example of the CLI commands used to configure traffic shaping:

```
Console(config)# interface ethernet 1/e5
4-376
Console(config-if) traffic-shape 124000 96000
4-483
```

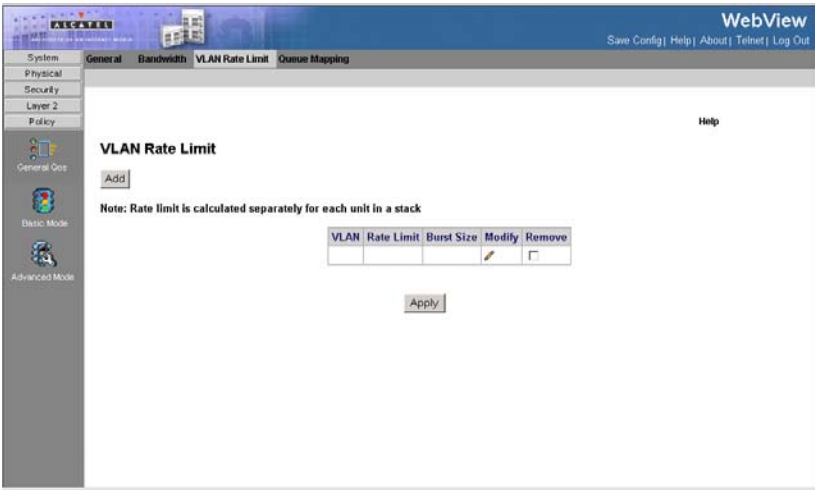
Configuring VLAN Rate Limit

Rate limiting per VLAN allows network administrators to limit traffic on VLANs. Rate limiting is calculated separately for each unit in a stack, and for each packet processor in a unit. QoS rate limiting has priority over VLAN rate limiting. For example, if a packet is subject to QoS rate limits but is also subject to VLAN rate limiting, and the rate limits conflict, the QoS rate limits take precedence.

Command Attributes

- **VLAN** – Indicates the VLAN on which the Rate Limit is applied
- **Rate Limit** – Defines the maximum rate (CIR) in kbits per second (bps) that forwarding traffic is permitted in the VLAN.
- **Burst Size** – Defines the maximum burst size (CbS) in bytes that forwarding traffic is permitted through the VLAN.

Web – Click Policy, General QoS, VLAN Rate Limit, and Add. Define the fields, and click Apply.



VLAN Rate Limit

Note: Rate limit is calculated separately for each unit in a stack

VLAN	Rate Limit	Burst Size	Modify	Remove
			✎	☐

Figure 3-120.   VLAN Rate Limit Page

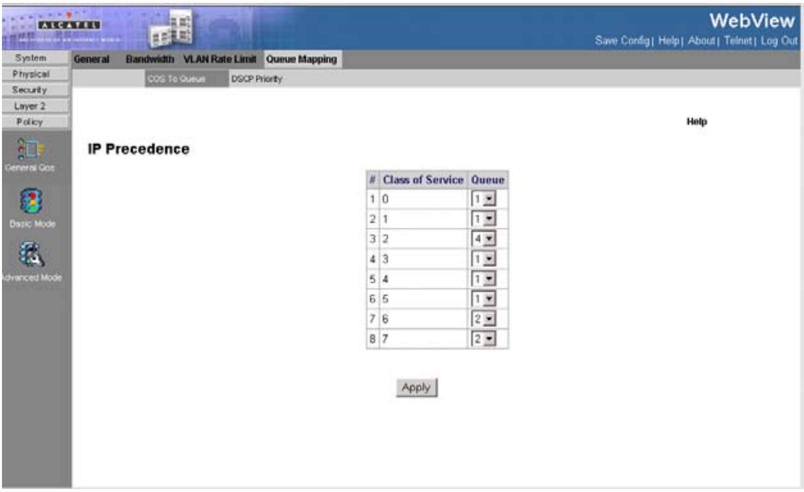
Mapping CoS Values to Queues

The *CoS to Queue Page* contains fields for classifying CoS settings to traffic queues.

Command Attributes

- **Class of Service** — Specifies the VLAN (CoS) priority tag values, where zero is the lowest and 8 is the highest.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. In a standalone device, four traffic priority queues are supported, where Queue 4 has the highest priority and Queue 1 has the lowest priority. In stacked units, three priority queues are supported.

Web – Click Policy, General QoS, Queue Mapping, Cos to Queue. Define the fields, and click Apply.



IP Precedence

#	Class of Service	Queue
1	0	1
2	1	1
3	2	4
4	3	1
5	4	1
6	5	1
7	6	2
8	7	2

Figure 3-121. CoS to Queue Page

CLI – The following is an example of the CLI commands used to map CoS values to forwarding queues:

```
Console(config)# wrr-queue cos-map 2 7
4-481
```

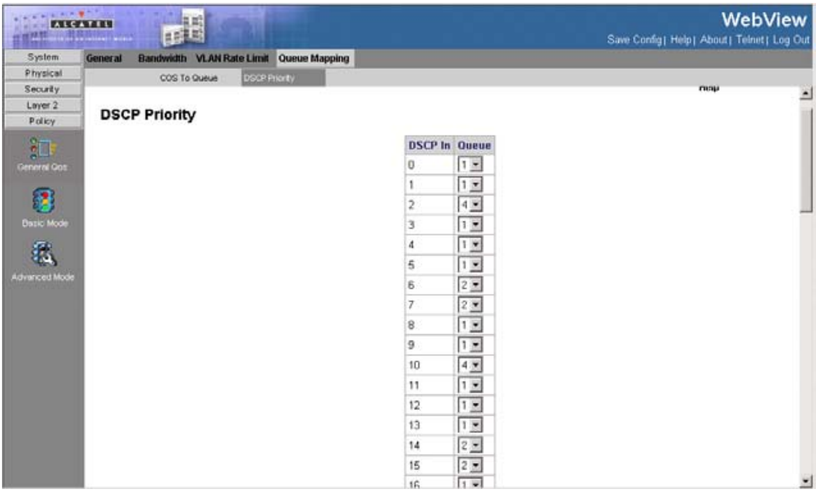
Mapping DSCP Values to Queues

The *DSCP Priority Page* contains fields for classifying DSCP settings to traffic queues.

Command Attributes

- **DSCP In** — Displays the incoming packet's DSCP value.
- **Queue** — Defines the traffic forwarding queue to which the DSCP priority is mapped. In a standalone device, four traffic priority queues are supported. In stacked devices, three priority queues are supported.

Web – Click Policy, General QoS, Queue Mapping, DSCP Priority. DSCP Priority define the fields, and click Apply.



DSCP Priority

DSCP In	Queue
0	1
1	1
2	4
3	1
4	1
5	1
6	2
7	2
8	1
9	1
10	4
11	1
12	1
13	1
14	2
15	2
16	1

Figure 3-122. DSCP Priority Page

CLI – The following is an example of the CLI commands used to map DSCP values to queues:

```
Console(config)# qos map dscp-queue 33 40 41 to 1
4-488
```

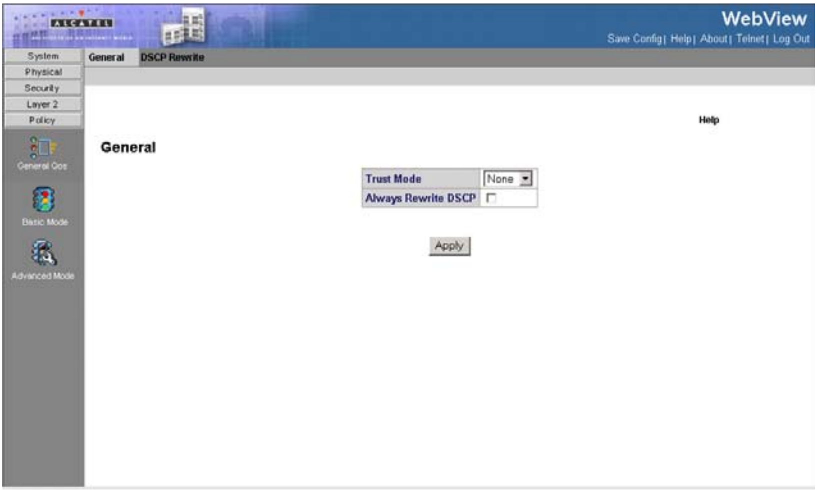
Defining Basic QoS Settings

The *QoS General Page* contains information for enabling Trust on the device. Packets entering a QoS domain are classified at the edge of the QoS domain.

Command Attributes

- **Trust Mode** — Selects the trust mode. If a packet's CoS tag and DSCP tag are mapped to different queues, the Trust mode determines the queue to which the packet is assigned. The possible field values are:
  - *None* — Sets the Trust mode to none. All packets are sent to the lowest queue.
  - *CoS* — Sets the Trust mode to CoS. Packets are queued based on their CoS field value.
  - *DSCP* — Sets the Trust mode to CoS. Packets are queued based on their DSCP tag value.
- **Always Rewrite DSCP** — Rewrites the packet DSCP tag according to the QoS DSCP Rewriting configuration. *Always Rewrite DSCP* can only be checked if the Trust Mode is set to *DSCP*.

Web – Click Policy, Basic Mode, General, define the fields, and click Apply.



General

Trust Mode	None
Always Rewrite DSCP	□

Figure 3-123. QoS General Page

CLI – The following is an example of the CLI commands used to configure QoS Basic Mode’s general parameters:

```
Console(config)# qos trust dscp
4-489
```

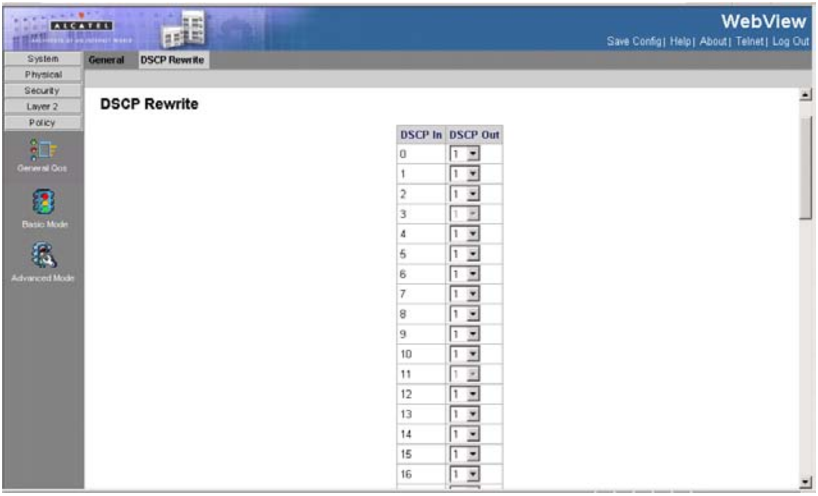
Defining QoS DSCP Rewriting Settings

The *DSCP Rewrite Page* allows network administrators to rewrite DSCP values.

Command Attributes

- **DSCP In** — DSCP field on incoming packets.
- **DSCP Out** — DSCP field on outgoing packets.

Web – Click Policy, Basic Mode, DSCP Rewrite, define the fields, and click Apply.



DSCP Rewrite

DSCP In	DSCP Out
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

Figure 3-124. DSCP Rewrite Page

CLI – The following is an example of the CLI commands used to rewrite DSCP values:

```
Console(config)# qos dscp-mutation
4-491
```

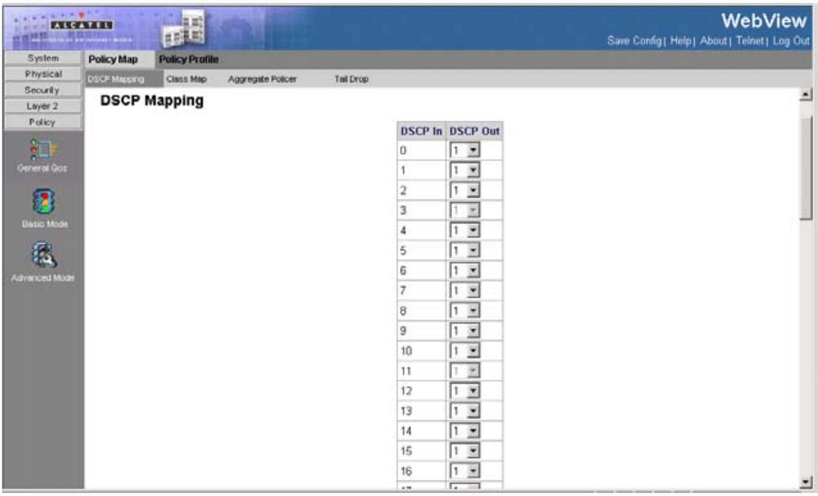
Defining QoS DSCP Mapping Settings

When traffic exceeds user-defined limits, use the *DSCP Mapping Page* to configure the DSCP tag to use in place of the incoming DSCP tags.

Command Attributes

- **DSCP In** — DSCP tag on incoming packets.
- **DSCP Out** — Sets a new DSCP tag on outgoing packets.

Web – Click Policy, Advanced Mode, Policy Map, DSCP Mapping. Define the fields, and click Apply.



DSCP Mapping

DSCP In	DSCP Out
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

Figure 3-125. DSCP Mapping Page

CLI – The following is an example of the CLI commands used to map DSCP values:

```
Console(config)# qos map dscp-mutation 1 2 4 5 6 to 63
4-492
```

Defining QoS Class Maps

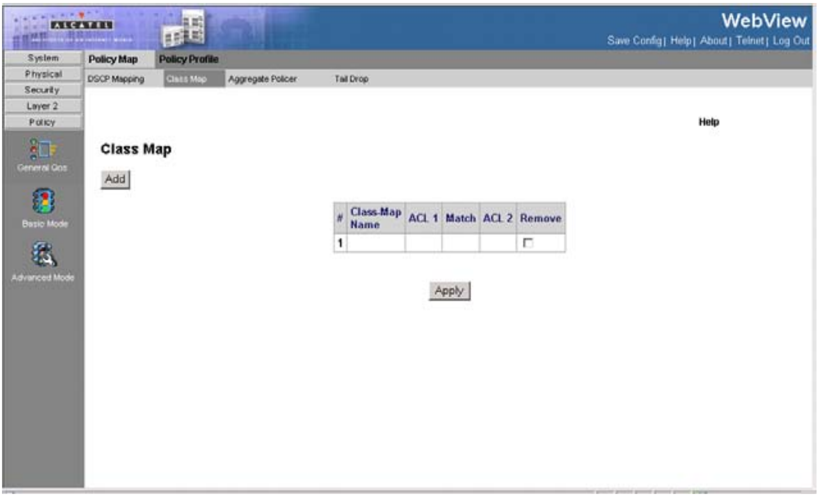
One IP ACL and/or one MAC ACL comprise a class map. Class maps are configured to match packet criteria, and are matched to packets on a first-fit basis. For example, Class Map A is assigned to packets based only on an IP-based ACL or a MAC-based ACL. Class Map B is assigned to packets based on both an IP-based and a MAC-based ACL.

The *Class Map Page* contains parameters for defining class maps.

Command Attributes

- **Class-Map Name** — Displays the user-defined name of the class map.
- **Preferred ACL** — Indicates if packets are first matched to an IP based ACL or a MAC based ACL.
- **ACL 1** — Contains a list of the user defined ACLs.
- **Match** — Indicates the criteria used to match class maps. Possible values are:
  - *And* — Matches both ACL 1 and ACL 2 to the packet fields.
  - *Or* — Matches either ACL 1 or ACL 2 to the packet fields.
- **ACL 2** — Contains a list of the user defined ACLs.
- **Remove** — If checked, deletes the Class Map.

Web – Click Policy, Advanced Mode, Policy Map, Class Map. Define the fields, and click Apply.



Class Map

#	Class-Map Name	ACL 1	Match	ACL 2	Remove
1					□

Figure 3-126. Class Map Page

CLI – The following is an example of the CLI commands used to define class maps:

```
Console(config)# qos advance
4-468
Console(config)#class-map class
4-469
Console(config-cmap)# match access-group royrogers
4-471
```

Defining Policies

A policy is a collection of classes, each of which is a combination of a class map and a QoS action to apply to matching traffic. Classes are applied in a first-fit manner within a policy.

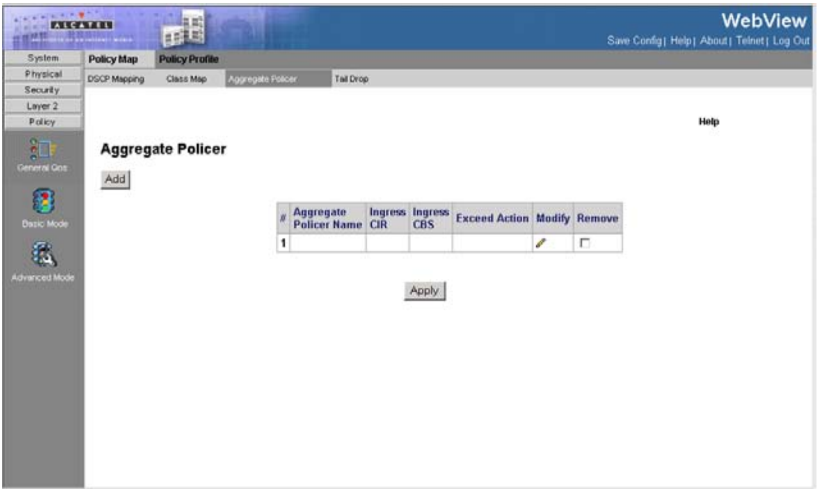
Before configuring policies for classes whose match criteria are defined in a class map, a class map must first be defined, or the name of the policy map to be created, added to, or modified must first be specified. Class policies can be configured in a policy map only if the classes have defined match criteria.

An aggregate policer can be applied to multiple classes in the same policy map, but an aggregate policer cannot be used across different policy maps. Define an aggregate policer if the policer is shared with multiple classes. Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

Command Attributes

- **Aggregate Policer** — User-defined aggregate policers.
- **Ingress Committed Information Rate (CIR)** — CIR in bits per second. This field is only relevant when the Police value is *Single*.
- **Ingress Committed Burst Size (CBS)** — CBS in bytes per second. This field is only relevant when the Police value is *Single*.
- **Exceed Action** — Action assigned to incoming packets when limits (CIR) are exceeded. This field is only relevant when the Police value is *Single*. Possible values are:
  - *Drop* — Drops packets exceeding the defined CIR value.
  - *Remark DSCP* — Remarks packets' DSCP values exceeding the defined CIR value.
  - *None* — Forwards packets exceeding the defined CIR value.
- **Remove** — Removes policies. The possible field values are:
  - *Checked* — Removes the selected policy.
  - *Unchecked* — Maintains the selected policy.

Web – Click Policy, Advanced Mode, Policy Map, Aggregate Policer. Define the fields and click Apply.



Aggregate Policer

#	Aggregate Policer Name	Ingress CIR	Ingress CBS	Exceed Action	Modify	Remove
1					✎	☐

Figure 3-127. Aggregate Policer Page

CLI – The following is an example of the CLI commands used for defining policy maps:

```
Console(config)# policy-map policy1
4-472
Console(config-pmap)# class class1                               4-472
Console(config-pmap-c)# police 124000 9600 exceed-action drop     4-477
```

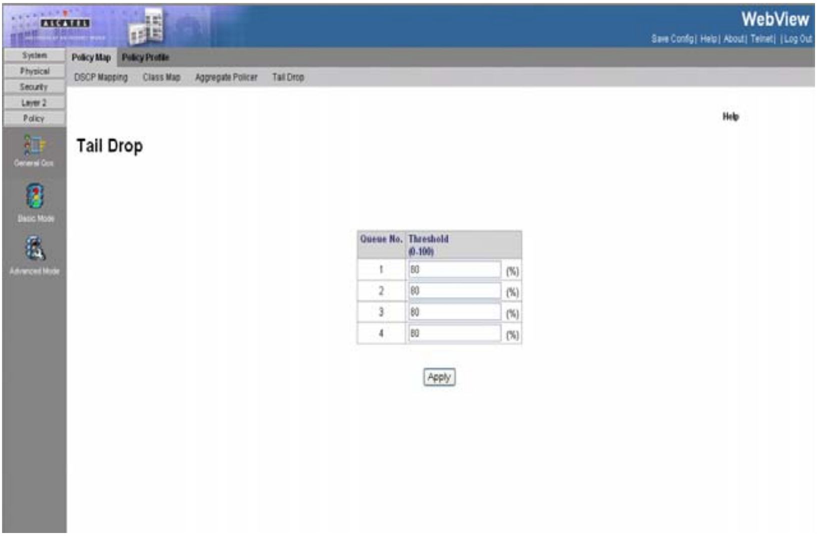
Defining Tail Drop

The *Tail Drop Page* permits network managers to set the device to drop packets which exceed the threshold size. Tail drop is only configurable on Giga Ethernet ports. Tail Drop is configured per queue.

Command Attributes

- **Queue No.** — Indicates the traffic queue for which the tail drop settings are defined.
- **Threshold (0-100)** — Defines the bandwidth amount after which packets are dropped.

Web – Click Policy, Advanced Mode, Policy Map, Tail Drop. Define the fields, and click Apply.



Tail Drop

Queue No.	Threshold (0-100)
1	80 (%)
2	80 (%)
3	80 (%)
4	80 (%)

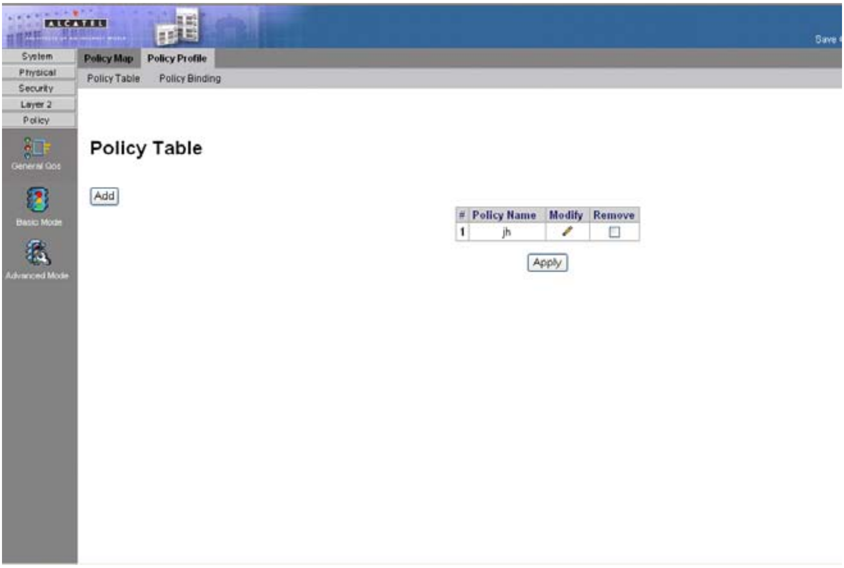
Figure 3-128. Tail Drop Page

Viewing the Policy Table

The *Policy Table Page* provides parameters for defining policies.

Command Attributes

- **Policy Name** — Contains a list of user-defined policies that can be attached to the interface.
- **Remove** — Removes policies.
  - *Checked* — Removes the selected policies.
  - *Unchecked* — Maintains the policies.



Policy Table

Add

#	Policy Name	Modify	Remove
1	jh	✎	□

Apply

Figure 3-129. Policy Table Page

In addition to the fields in the *Policy Table Page*, the *Add QoS Policy Profile Page* contains the following fields:

- **Class Map** — Selects a class map for the class.
- **Action** — Indicates the action performed on incoming packets matching the policy profile. The possible field values are:
  - *Trust* - Applies the selected Trust settings.
  - *Set* - Redefines the DSCP settings.
- **Police** — Policer type for the class. Possible values are:
  - *Aggregate* — Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.
  - *Single* — Configures the class to use manually configured information rates and

exceed actions.

- **Aggregate Policer** — User-defined aggregate policers.
- **Ingress Committed Information Rate (CIR)** — CIR in bits per second. This field is only relevant when the **Police** value is **Single**.
- **Ingress Committed Burst Size (CBS)** — CBS in bytes per second. This field is only relevant when the **Police** value is **Single**.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the **Police** value is **Single**. Possible values are:
  - *Drop* — Drops packets exceeding the defined CIR value.
  - *Remark DSCP* — Remarks packets' DSCP values exceeding the defined CIR value.

CLI – The following is an example of the CLI commands used to bind policies:

```
Console# show policy-map
4-474
Policy Map policy1
   class class1
       set Ip dscp 7
Policy Map policy2
   class class 2
       police 96000 4800 exceed-action drop
   class class3
       police 124000 96000 exceed-action policed-dscp-transmit
```

Viewing Policy Bindings

The *Policy Binding Page* provides parameters for defining policies.

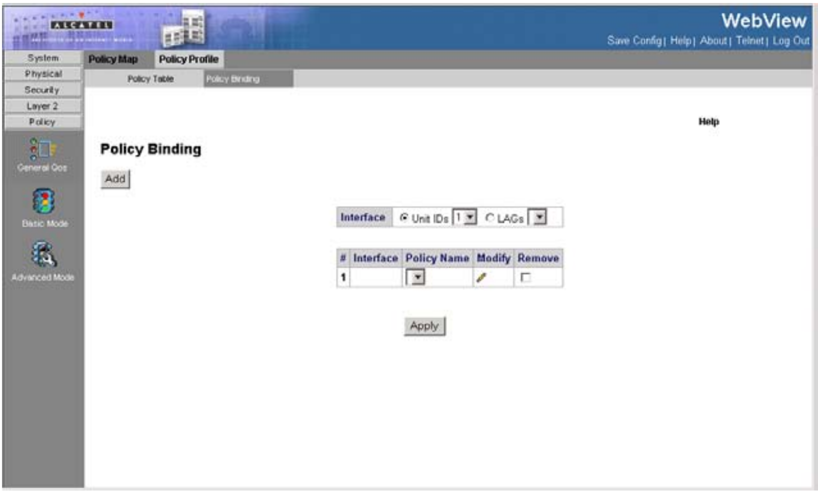
Command Attributes

- **Interface** — Select the type of unit for which policy information is displayed. The possible field values are:
  - – *Unit IDs* — Displays the stacking members and their policy names.
  - – *LAGs* — Displays the LAGs and their policy names.

The Policy Binding table contains the following fields:

- **Interface** — Selects an interface.
- **Policy Name** — Contains a list of user-defined policies that can be attached to the interface.
- **Remove** — Removes policies.
  - *Checked* — Removes the selected policies.
  - *Unchecked* — Maintains the policies.

Web – Click Policy, Advanced Mode, Policy Profile, Policy Binding. Define the fields, and click Apply.



Policy Binding

Interface ● Unit IDs 1 ○ LAGs

#	Interface	Policy Name	Modify	Remove
1			✎	□

Figure 3-130. Policy Binding Page

CLI – The following is an example of the CLI commands used to bind policies:

```
Console# show policy-map
4-474
Policy Map policy1
   class class1
       set Ip dscp 7
Policy Map policy2
   class class 2
       police 96000 4800 exceed-action drop
   class class3
       police 124000 96000 exceed-action policed-dscp-transmit
```

{[A

Chapter 4: Command Line Interface

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

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server’s console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are “admin” and “guest” with corresponding passwords of “admin” and “guest.”) When the administrator user name and password is entered, the CLI displays the “Console#” prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the “Console>” prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the “quit” or “exit” command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

       CLI session with the OmniStack 6300 is opened.
       To end the CLI session, enter [Exit].
Console#
```

Telnet Connection

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

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

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

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

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

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

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

       CLI session with the OmniStack 6300-24 is opened.
       To end the CLI session, enter [Exit].

```

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

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

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

You can enter commands as follows:

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

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

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

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

Minimum Abbreviation

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

Command Completion

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

Getting Help on Commands

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

Showing Commands

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

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

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

```
Console#show interfaces ?
  counters       Information of interfaces counters
  protocol-vlan  Protocol-vlan information
  status         Information of interfaces status
  switchport     Information of interfaces switchport
Console#
```

Partial Keyword Lookup

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

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

Negating the Effect of Commands

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

Using Command History

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

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

Understanding Command Modes

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

Table 4-1. Command Modes

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

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

Exec Commands

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

To enter Privileged Exec mode, enter the following user names and passwords:

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

       CLI session with the OmniStack 6300-24 is opened.
       To end the CLI session, enter [Exit].

Console#
```

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

       CLI session with the OmniStack 6300-24 is opened.
       To end the CLI session, enter [Exit].

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

Configuration Commands

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

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- VLAN Configuration - Includes the command to create VLAN groups.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

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

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 4-2. Configuration Command Modes

Mode	Command	Prompt
Line	line (console)	Console(config-line)#

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

Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)#
VLAN	vlan database	Console(config-vlan)
MSTP	spanning-tree mst-configuration	Console(config-mstp)#
QoS	class-map	Console(config-cmap)#

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

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

Command Line Processing

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

Table 4-3. Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.

Table 4-3. Keystroke Commands

Keystroke	Function
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

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

Table 4-4. Command Groups

Command Group	Description	Page
802.1x Commands	Configures Port based authentication for authenticating system users on a per-port basis via a external server.	4-263
AAA Commands	Configures connection security including authorization and passwords.	4-288
ACL Commands	Configures and displays ACL information.	4-300
Address Table Commands	Configures bridging address tables.	4-313
LLDP Commands	Configures AMAP protocol for discovering adjacent switches by sending and receiving AMAP "Hello" packets on active Spanning Tree ports.	4-333
Clock Commands	Configures system time parameters for both the local hardware clock and the external SNTP clock.	4-348
Configuration and Image File Commands	Manages the device configuration files.	4-365
Ethernet Configuration Commands	Configures all port configuration options for example ports, storm control, port speed and auto-negotiation.	4-376
GVRP Commands	Configures and displays GVRP configuration and information.	4-399
IGMP Snooping Commands	Configures IGMP snooping and displays IGMP configuration and IGMP information.	4-408
IP Addressing Commands	Configures and manages IP addresses on the device.	4-418
LACP Commands	Configures and displays LACP information.	4-431
Line Commands	Configures the console and remote Telnet connection.	4-437
Management ACL Commands	Configures and displays management access-list information.	4-445
PHY Diagnostics Commands	Diagnoses and displays the interface status.	4-451
Port Channel Commands	Configures and displays Port channel information.	4-455
Port Monitor Commands	Monitors activity on specific target ports.	4-458
Power over Ethernet Commands	Configuring PoE interfaces, including the interface PoE operation status and the interface’s power consumption.	4-460
QoS Commands	Configures and displays QoS information.	4-467
RADIUS Commands	Configures and displays RADIUS information.	4-495
RMON Commands	Displays RMON statistics.	4-503
SNMP Commands	Configures SNMP communities, traps and displays SNMP information.	4-518
Spanning-Tree Commands	Configures and reports on Spanning Tree protocol.	4-538
SSH Commands	Configures SSH authentication.	4-580
Syslog Commands	Manages and displays syslog messages.	4-591

Table 4-4. Command Groups

Command Group	Description	Page
System Management Commands	Configures the device clock, name and authorized users.	4-604
TACACS+ Commands	Configures Terminal Access Controller Access Control System (TACACS+) which provides centralized security user access validation.	4-622
Triple Play Commands	Configures Triple Play.	4-627
DHCP Snooping, IP Source Guard and ARP Inspection Commands	Configures the DHCP Snooping, IP Source Guard, and the ARP Inspection Commands	4-631
User Interface Commands	Describes user commands used for entering CLI commands.	4-652
VLAN Commands	Configures VLANS and displays VLAN information.	4-661
Web Server Commands	Configures Web based access to the device.	4-691

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

NE (Normal Exec)
PE (Privileged Exec)
GC (Global Configuration)
ACL (Access Control List Configuration)
I**CE** (Interface Configuration Ethernet)
ICV (Interface Configuration VLAN)
PCC (Policy-Map Class Configuration)
SPK (SSH Public Key-string)

IC (Interface Configuration)
LC (Line Configuration)
VC (VLAN Database Configuration)
MST (Multiple Spanning Tree)
UE (User Exec)
CMC (Class-Map Configuration
PMC (Policy-Map Configuration)

802.1x Commands

.

Table 4-5. 802.1x Commands

Command	Function	Mode	Page
aaa authentication dot1x	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. To return to the default configuration, use the **no** form of this command	GC	4-264
dot1x system-auth-control	Enables 802.1x globally. To return to the default configuration, use the **no** form of this command	GC	4-265
dot1x port-controll	Auto - Enables 802.1X authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the port and the client. Force-authorized - Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1X-based authentication of the client. Force-unauthorized -Denies all access through this interface by forcing the port to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.	ICE	4-266
dot1x re-authentication	Enables periodic re-authentication of the client. To return to the default configuration, use the **no** form of this command.	ICE	4-267
dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts. To return to the default configuration, use the **no** form of this command.	ICE	4-268
dot1x re-authenticate	Manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port	PE	4-269
dot1x timeout quiet-period	Sets the number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). To return to the default configuration, use the no form of this command	ICE	4-269
dot1x timeout tx-period	Sets the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request. To return to the default configuration, use the no form of this command	ICE	4-270
dot1x max-req	Sets the maximum number of times that the device sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client, before restarting the authentication process. To return to the default configuration, use the no form of this command	ICE	4-271
dot1x timeout supp-timeout	Sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client. To return to the default configuration, use the no form of this command	ICE	4-272

Table 4-5. 802.1x Commands

Command	Function	Mode	Page
dot1x timeout server-timeout	Sets the time that the device waits for a response from the authentication server. To return to the default configuration, use the no form of this command	ICE	4-273
show dot1x	Displays the 802.1X status of the device or specified interface	PE	4-274
show dot1x users	Displays active 802.1X authenticated users for the device.	PE	4-277
show dot1x statistics	Displays 802.1X statistics for the specified interface.	PE	4-279
dot1x auth-not-req	Enables unauthorized devices access to the VLAN. To disabled access to the VLAN, use the no form of this command.	ICV	4-281
dot1x multiple-hosts	Enables multiple hosts (clients) on an 802.1X-authorized port, where the authorization state of the port is set to **auto**. To return to the default configuration, use the **no** form of this command	ICE	4-282
dot1x single-host-violation	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.	ICE	4-283
dot1x guest-vlan	Defines a guest VLAN. To return to the default configuration, use the **no** form of this command.	ICV	4-284
dot1x guest-vlan enable	Enables unauthorized users on the interface access to the Guest VLAN. To disable access, use the **no** form of this command.	ICE	4-285
dot1x mac-authentication	Enables authentication based on the station's MAC address	ICE	4-285
show dot1x advanced	Displays 802.1X advanced features for the device or specified interface	PE	4-286

aaa authentication dot1x

The **aaa authentication dot1x** Global Configuration mode command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication dot1x default *method1* [*method2*...]

no aaa authentication dot1x default

Parameters

- *method1* [*method2*...] — At least one from the following table:

Keyword	Description
Radius	Uses the list of all RADIUS servers for authentication
None	Uses no authentication

Default Setting

No authentication method is defined.

Command Mode

Global Configuration

Command Usage

Additional methods of authentication are used only if the previous method returns an error and not if the request for authentication is denied. To ensure that authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

The RADIUS server must support MD-5 challenge and EAP type frames.

Example

The following example uses the **aaa authentication dot1x default** command with no authentication.

```
Console(config)# aaa authentication dot1x default none
```

Related Commands

aaa authentication enable

dot1x system-auth-control

The **dot1x system-auth-control** Global Configuration mode command enables 802.1x globally. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Default Configuration

802.1x is disabled globally.

Command Modes

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Examples

The following example enables 802.1x globally.

```
Console(config)# dot1x system-auth-control
```

Related Commands

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout server-timeout

show dot1x

show dot1x users

dot1x port-control

The **dot1x port-control** Interface Configuration mode command enables manually controlling the authorization state of the port. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

Parameters

- **auto** — Enables 802.1X authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the port and the client.
- **force-authorized —** Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1X-based authentication of the client.
- **force-unauthorized —** Denies all access through this interface by forcing the port to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.

Default Configuration

Port is in the force-authorized state

Command Mode

Interface Configuration (Ethernet)

Command Usage

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations), in order to get immediately to the forwarding state after successful authentication.

Example

The following example enables 802.1X authentication on Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x port-control auto
```

Related Commands

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout server-timeout

show dot1x

show dot1x users

dot1x re-authentication

The **dot1x re-authentication** Interface Configuration mode command enables periodic re-authentication of the client. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x re-authentication

no dot1x re-authentication

Default Setting

Periodic re-authentication is disabled.

Command Mode

Interface Configuration (Ethernet)

Command Usage

There are no user guidelines for this command.

Example

The following example enables periodic re-authentication of the client.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x re-authentication
```

Related Commands

dot1x port-control

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout server-timeout

show dot1x

show dot1x users

dot1x timeout re-authperiod

The **dot1x timeout re-authperiod** Interface Configuration mode command sets the number of seconds between re-authentication attempts. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Parameters

- *seconds* — Number of seconds between re-authentication attempts. (Range: 300 - 4294967295)

Default Setting

Re-authentication period is 3600 seconds.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following example sets the number of seconds between re-authentication attempts, to 300.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x timeout re-authperiod 300
```

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout-server-timeout

show dot1x

show dot1x users

dot1x re-authenticate

The **dot1x re-authenticate** Privileged EXEC mode command manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.

Syntax

dot1x re-authenticate [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command manually initiates a re-authentication of 802.1X-enabled Ethernet port 1/e16.

```
Console# dot1x re-authenticate ethernet 1/e16
```

Related Commands

dot1x system-auth-control

dot1x port-control

dot1x timeout quiet-period

The **dot1x timeout quiet-period** Interface Configuration mode command sets the number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). To return to the default configuration, use the **no** form of this command.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameters

- *seconds* — Specifies the time in seconds that the device remains in the quiet state following a failed authentication exchange with the client. (Range: 0 - 65535 seconds)

Default Setting

Quiet period is 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide a faster response time to the user, a smaller number than the default value should be entered.

Example

The following example sets the number of seconds that the device remains in the quiet state following a failed authentication exchange to 3600.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x timeout quiet-period 3600
```

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout server-timeout

show dot1x

show dot1x users

dot1x timeout tx-period

The **dot1x timeout tx-period** Interface Configuration mode command sets the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameters

- *seconds* — Specifies the time in seconds that the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 1-65535 seconds)

Default Configuration

Timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients. and authentication servers

Example

The following command sets the number of seconds that the device waits for a response to an EAP-request/identity frame, to 3600 seconds.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x timeout tx-period 3600
```

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout server-timeout

show dot1x

show dot1x users

dot1x max-req

The **dot1x max-req** Interface Configuration mode command sets the maximum number of times that the device sends an Extensible Authentication Protocol

(EAP)-request/identity frame (assuming that no response is received) to the client, before restarting the authentication process. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x max-req *count*

no dot1x max-req

Parameters

- *count* — Number of times that the device sends an EAP-request/identity frame before restarting the authentication process. (Range: 1-10)

Default Configuration

The default number of times is 2.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients. and authentication servers.

Example

The following example sets the number of times that the device sends an EAP-request/identity frame to 6 .

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x max-req 6
```

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x timeout supp-timeout

dot1x timeout server-timeout

show dot1x

show dot1x users

dot1x timeout supp-timeout

The **dot1x timeout supp-timeout** Interface Configuration mode command sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameters

- *seconds* — Time in seconds that the device waits for a response to an EAP-request frame from the client before resending the request. (Range: 1- 65535 seconds)

Default Configuration

Default timeout period is 30 seconds.

Command Mode

Interface configuration (Ethernet) mode

Command Usage

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients. and authentication servers.

Example

The following example sets the timeout period before retransmitting an EAP-request frame to the client to 3600 seconds.

```
Console(config-if)# dot1x timeout supp-timeout 3600
```

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout server-timeout

show dot1x

show dot1x users

dot1x timeout server-timeout

The **dot1x timeout server-timeout** Interface Configuration mode command sets the time that the device waits for a response from the authentication server. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameters

- *seconds* — Time in seconds that the device waits for a response from the authentication server. (Range: 1-65535 seconds)

Default Configuration

The timeout period is 30 seconds.

Command Mode

Interface configuration (Ethernet) mode

Command Usage

The actual timeout can be determined by comparing the **dot1x timeout server-timeout** value and the result of multiplying the **radius-server retransmit** value with the **radius-server timeout** value and selecting the lower of the two values.

Example

The following example sets the time for the retransmission of packets to the authentication server to 3600 seconds.

```
Console(config-if)# dot1x timeout server-timeout 3600
```

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

show dot1x

show dot1x users

show dot1x

The **show dot1x** Privileged EXEC mode command displays the 802.1X status of the device or specified interface.

Syntax

show dot1x [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the status of 802.1X-enabled Ethernet ports.

```
Console# show dot1x

802.1x is enabled

Port   Admin Mode   Oper Mode        Reaut   Reauth   Username
                                     h       Period
                                     Contr
                                     ol
----   ----------   ---------        -----   ------   --------
                                     --
1/e1   Auto         Authorized       Ena     3600     Bob
1/e2   Auto         Authorized       Ena     3600     John
1/e3   Auto         Unauthorized     Ena     3600     Clark
1/e4   Force-auth   Authorized       Dis     3600     n/a
1/e5   Force-auth   Unauthorized*    Dis     3600     n/a

* Port is down or not present.

Console# show dot1x ethernet 1/e3

802.1x is enabled.

Port   Admin Mode   Oper Mode        Reaut   Reauth   Username
                                     h       Period
                                     Contr
                                     ol
```

```
----   ----------    ---------      -----    ------   --------
                                    --

1/e3   Auto          Unauthorized    Ena      3600     Clark


Quiet period: 60 Seconds
Tx period:30 Seconds
Max req: 2
Supplicant timeout: 30 Seconds
Server timeout: 30 Seconds
Session Time (HH:MM:SS): 08:19:17
MAC Address: 00:08:78:32:98:78
Authentication Method: Remote
Termination Cause: Supplicant logoff


Authenticator State Machine
State: HELD


Backend State Machine
State: IDLE
Authentication success: 9
Authentication fails: 1
```

The following table describes significant fields shown above:

Field	Description
Port	The port number.
Admin mode	The port admin mode. Possible values: Force-auth, Force-unauth, Auto.
Oper mode	The port oper mode. Possible values: Authorized, Unauthorized or Down.
Reauth Control	Reauthentication control.
Reauth Period	Reauthentication period.
Username	The username representing the identity of the Supplicant. This field shows the username in case the port control is auto. If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user that was authenticated successfully.

Quiet period	The number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Tx period	The number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.
Max req	The maximum number of times that the device sends an Extensible Authentication Protocol (EAP)-request frame (assuming that no response is received) to the client before restarting the authentication process.
Supplicant timeout	Time in seconds the switch waits for a response to an EAP-request frame from the client before resending the request.
Server timeout	Time in seconds the switch waits for a response from the authentication server before resending the request.
Session Time	The amount of time the user is logged in.
MAC address	The supplicant MAC address.
Authentication Method	The authentication method used to establish the session.
Termination Cause	The reason for the session termination.
State	The current value of the Authenticator PAE state machine and of the Backend state machine.
Authentication success	The number of times the state machine received a Success message from the Authentication Server.
Authentication fails	The number of times the state machine received a Failure message from the Authentication Server.

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout server-timeout

show dot1x users

show dot1x users

The **show dot1x users** Privileged EXEC mode command displays active 802.1X authenticated users for the device.

Syntax

show dot1x users [**username** *username*]

Parameters

- *username* — Supplicant username (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays 802.1X users.

```
Console# show dot1x users


Por    Username    Session        Auth          MAC Address
t                  Time           Method

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

1/     Bob         1d:03:08.58    Remote        0008:3b79:8787
e1

1/     John        08:19:17       None          0008:3b89:3127
e2


Console# show dot1x users username Bob


Username: Bob

Por    Username    Session        Auth          MAC Address
t                  Time           Method

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

1/     Bob         1d:03:08.58    Remote        0008:3b79:8787
e1
```

The following table describes significant fields shown above:

Field	Description
Port	The port number.
Username	The username representing the identity of the Supplicant.
Session Time	The period of time the Supplicant is connected to the system.
Authentication Method	Authentication method used by the Supplicant to open the session.
MAC Address	MAC address of the Supplicant.

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout server-timeout

show dot1x

show dot1x statistics

The **show dot1x statistics** Privileged EXEC mode command displays 802.1X statistics for the specified interface.

Syntax

show dot1x statistics ethernet *interface*

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays 802.1X statistics for the specified interface.

```
Console# show dot1x statistics ethernet 1/e1


EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 12

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 00:08:78:32:98:78
```

The following table describes the significant fields shown in the display:

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

Related Commands

dot1x port-control

dot1x re-authentication

dot1x timeout re-authperiod

dot1x timeout quiet-period

dot1x timeout tx-period

dot1x max-req

dot1x timeout supp-timeout

dot1x timeout server-timeout

ADVANCED FEATURES

dot1x auth-not-req

The **dot1x auth-not-req** Interface Configuration mode command enables unauthorized devices access to the VLAN. To disable access to the VLAN, use the **no** form of this command.

Syntax

dot1x auth-not-req

no dot1x auth-not-req

Default Configuration

Access is enabled.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

An access port cannot be a member in an unauthenticated VLAN.

The native VLAN of a trunk port cannot be an unauthenticated VLAN.

For a general port, the PVID can be an unauthenticated VLAN (although only tagged packets would be accepted in the unauthorized state.)

Examples

The following example enables access to the VLAN to unauthorized devices.

```
Console(config-if)# dot1x auth-not-req
```

Related Commands

show dot1x advanced

dot1x multiple-hosts

The **dot1x multiple-hosts** Interface Configuration mode command enables multiple hosts (clients) on an 802.1X-authorized port, where the authorization state of the port is set to **auto**. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x multiple-hosts [**authentication**]]

no dot1x multiple-hosts

Parameters

- **authentication** — Specifies that each station should be 802.1x authenticated.

Default Configuration

Multiple hosts are disabled.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

This command enables the attachment of multiple clients to a single 802.1X-enabled port.

If you use this command without the authentication keyword, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

If you use this command with the authentication keyword, each host must be successfully authorized in order to grant network access. Please note that packets are NOT encrypted, and after success full authentication filtering is based on the source MAC address only.

For unauthenticated VLANs multiple hosts are always enabled.

Port security on a port cannot be enabled if the port if multiple hosts are disabled or multiple hosts are enabled with authentication per host.

Example

The following command enables multiple hosts (clients) on an 802.1X-authorized port.

```
Console(config-if)# dot1x multiple-hosts
```

Related Commands

dot1x single-host-violation

show dot1x advanced

dot1x single-host-violation

The **dot1x single-host-violation** Interface Configuration mode command 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.

Syntax

dot1x single-host-violation {**forward** | **discard** | **discard-shutdown**} [**trap** *seconds*]

no port dot1x single-host-violation

Parameters

- **forward** — Forwards frames with source addresses that are not the supplicant address, but does not learn the source addresses.
- **discard** — Discards frames with source addresses that are not the supplicant address.
- **discard-shutdown** — Discards frames with source addresses that are not the supplicant address. The port is also shut down.
- **trap** — Indicates that SNMP traps are sent.
- *seconds* — Specifies the minimum amount of time in seconds between consecutive traps. (Range: 1- 1000000)

Default Setting

Frames with source addresses that are not the supplicant address are discarded.

No traps are sent.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

The command is relevant when multiple hosts is disabled and the user has been successfully authenticated.

Examples

The following example forwards frames with source addresses that are not the supplicant address and sends consecutive traps at intervals of 100 seconds.

```
Console(config-if)# dot1x single-host-violation forward trap 100
```

Related Commands

dot1x multiple-hosts

show dot1x advanced

dot1x guest-vlan

The **dot1x guest-vlan** Interface Configuration mode command defines a guest VLAN. To return to the default configuration, use the **no** form of this command.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Default Setting

No VLAN is defined as a guest VLAN.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

Use the **dot1x guest-vlan enable** Interface Configuration mode command to enable unauthorized users on an interface to access the guest VLAN.

If the guest VLAN is defined and enabled, the port automatically joins the guest VLAN when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave the guest VLAN, the port should not be a static member of the guest VLAN.

Example

The following example defines VLAN 2 as a guest VLAN.

```
Console#
Console# configure
Console(config)# vlan database
Console(config-vlan)# vlan 2
Console(config-vlan)# exit
Console(config)# interface vlan 2
Console(config-if)# dot1x guest-vlan
```

Related Commands

dot1x guest-vlan enable

show dot1x advanced

dot1x guest-vlan enable

The **dot1x vlans guest-vlan enable** Interface Configuration mode command enables unauthorized users on the interface access to the Guest VLAN. To disable access, use the **no** form of this command

Syntax

dot1x guest-vlan enable

no dot1x guest-vlan enable

Default Setting

Disabled.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

A device can have only one global guest VLAN. The guest VLAN is defined using the **dot1x guest-vlan** Interface Configuration mode command.

Example

The following example enables unauthorized users on Ethernet port 1/e1 to access the guest VLAN.

```
Console# configure
Console(config)# interface ethernet 1/e1
Console(config-if)# dot1x guest-vlan enable
```

Related Commands

dot1x guest-vlan

show dot1x advanced

dot1x mac-authentication

Use the mac-authentication interface configuration command to enable authentication based on the station's MAC address. Use the no form of this command to disable MAC authentication.

Syntax

dot1x mac-authentication {mac-only | mac-and-802.1x}

no dot1x mac-authentication

Parameters

- **mac-only** — Enable authentication based on the station's MAC address only. 802.1X frames are ignored.
- **mac-and-802.1x** — Enable 802.1X authentication and MAC address authentication on the interface.

Default

Disabled.

·Command Modes

Interface configuration (Ethernet)

Usage Guidelines

Guest VLAN must be enabled when MAC authentication is enabled.

Static MAC addresses cannot be authorized on a guest VLAN when MAC authentication is enabled. Do not change an authenticated MAC address to a static address.

It is not recommended to delete authenticated MAC addresses.

Reauthentication must be enabled when working in this mode.

·Examples

TBA

show dot1x advanced

The **show dot1x advanced** Privileged EXEC mode command displays 802.1X advanced features for the device or specified interface.

Syntax

show dot1x advanced [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Examples

The following example displays 802.1X advanced features for the device.

```
Switch# show dot1x advanced


Guest VLAN: 3978

Unauthenticated VLANs: 91,92


Port               Multiple Hosts     Guest VLAN         MAC
                                                         Authentication

---------          --------------     ----------         ---------------
```

```
1/e1              Disabled          Enabled           MAC-and-802.1x

1/e2              Enabled           Disabled          Disabled


Switch# show dot1x advanced ethernet 1/e12


Port              Multiple Hosts    Guest VLAN        MAC
                                                      Authentication

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

1/e12             Disabled          Disabled          Disabled


Single host parameters

Violation action: Discard

Trap: Disabled

Trap frequency: 10

Status: Not in auto mode

Violations since last trap: 9
```

Related Commands

dot1x auth-not-req

dot1x multiple-hosts

dot1x single-host-violation

dot1x guest-vlan

dot1x guest-vlan enable

AAA Commands

Table 4-6. AAA Commands

Command	Function	Mode	Page
aaa authentication login	Defines login authentication. To return to the default configuration, use the **no** form of this command.	GC	4-288
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels. To return to the default configuration, use the **no** form of this command.	GC	4-290
login authentication	Specifies the login authentication method list for a remote telnet or console. To return to the default configuration specified by the **aaa authentication login** command, use the **no** form of this command.	LC	4-291
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console. To return to the default configuration specified by the aaa authentication enable command, use the **no** form of this command.	LC	4-292
ip http authentication	Specifies authentication methods for HTTP server users. To return to the default configuration, use the **no** form of this command.	GC	4-293
ip https authentication	Specifies authentication methods for HTTPS server users. To return to the default configuration, use the **no** form of this command.	GC	4-294
show authentication methods	Displays information about the authentication methods.	PE	4-294
password	Specifies a password on a line. To remove the password, use the **no** form of this command.	LC	4-296
enable password	Sets a local password to control access to user and privilege levels. To remove the password requirement, use the **no** form of this command.t	GC	4-296
username	Creates a user account in the local database. To remove a user name, use the **no** form of this command.	GC	4-297
show users accounts	Displays information about the local user database.	PE	4-298

aaa authentication login

The **aaa authentication login** Global Configuration mode command defines login authentication. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*}

Parameters

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- *list-name* — Character string used to name the list of authentication methods activated when a user logs in. (Range: 1-12 characters).
- *method1* [*method2*...] — Specify at least one from the following table:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Setting

The local user database is checked. This has the same effect as the command **aaa authentication login** *list-name local.*

Note: On the console, login succeeds without any authentication check if the authentication method is not defined.

Command Mode

Global Configuration mode

Command Usage

The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example configures the authentication login.

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

Related Commands

aaa authentication enable

login authentication

show authentication methods

aaa authentication enable

The **aaa authentication enable** Global Configuration mode command defines authentication method lists for accessing higher privilege levels. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication enable {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication enable {**default** | *list-name*}

Parameters

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
- *list-name* — Character string used to name the list of authentication methods activated, when using access higher privilege levels. (Range: 1-12 characters)
- *method1* [*method2*...] — Specify at least one from the following table:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication. Uses username $enabx$., where x is the privilege level.
tacacs	Uses the list of all TACACS+ servers for authentication. Uses username "$enabx$." where x is the privilege level.

Default Setting

If the **default** list is not set, only the enable password is checked. This has the same effect as the command **aaa authentication enable** *default enable*.

On the console, the enable password is used if it exists. If no password is set, the process still succeeds. This has the same effect as using the command **aaa authentication enable** *default enable none*.

Command Mode

Global Configuration mode

Command Usage

The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable** *default* requests sent by the device to a RADIUS or TACACS+ server include the username $enabx$., where x is the requested privilege level.

Example

The following example sets the enable password for authentication when accessing higher privilege levels.

```
Console(config)# aaa authentication enable default enable
```

Related Commands

aaa authentication dot1x

aaa authentication login

login authentication

show authentication methods

login authentication

The **login authentication** Line Configuration mode command specifies the login authentication method list for a remote telnet or console. To return to the default configuration specified by the **aaa authentication login** command, use the **no** form of this command.

Syntax

login authentication {**default** | *list-name*}

no login authentication

Parameters

- **default** — Uses the default list created with the **aaa authentication login** command.
- *list-name* — Uses the indicated list created with the **aaa authentication login** command.

Default Setting

Uses the default set with the command **aaa authentication login**.

Command Mode

Line Configuration mode

Command Usage

Changing login authentication from default to another value may disconnect the telnet session.

Example

The following example specifies the default authentication method for a console.

```
Console(config)# line console
Console(config-line)# login authentication default
```

Related Commands

aaa authentication login

aaa authentication enable

show authentication methods

enable authentication

The **enable authentication** Line Configuration mode command specifies the authentication method list when accessing a higher privilege level from a remote telnet or console. To return to the default configuration specified by the **aaa authentication enable** command, use the **no** form of this command.

Syntax

enable authentication {**default** | *list-name*}

no enable authentication

Parameters

- **default** — Uses the default list created with the **aaa authentication enable** command.
- *list-name* — Uses the indicated list created with the **aaa authentication enable** command.

Default Setting

Uses the default set with the **aaa authentication enable** command.

Command Mode

Line Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example specifies the default authentication method when accessing a higher privilege level from a console.

```
Console(config)# line console
Console(config-line)# enable authentication default
```

Related Commands

show authentication methods

ip http authentication

The **ip http authentication** Global Configuration mode command specifies authentication methods for HTTP server users. To return to the default configuration, use the **no** form of this command.

Syntax

ip http authentication *method1* [*method2*...]

no ip http authentication

Parameters

- *method1* [*method2*...] — Specify at least one from the following table:

Keyword	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Setting

The local user database is checked. This has the same effect as the command **ip http authentication** *local.*

Command Mode

Global Configuration mode

Command Usage

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example configures the HTTP authentication.

```
Console(config)# ip http authentication radius local
```

Related Commands

show authentication methods

ip https authentication

The **ip https authentication** Global Configuration mode command specifies authentication methods for HTTPS server users. To return to the default configuration, use the **no** form of this command.

Syntax

ip https authentication *method1* [*method2*...]

no ip https authentication

Parameters

- *method1* [*method2*...] — Specify at least one from the following table:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Setting

The local user database is checked. This has the same effect as the command **ip https authentication** *local*.

Command Mode

Global Configuration mode

Command Usage

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example configures HTTPS authentication.

```
Console(config)# ip https authentication radius local
```

Related Commands

show authentication methods

show authentication methods

The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

Syntax

show authentication methods

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the authentication configuration.

```
Console# show authentication methods
Login Authentication Method Lists
---------------------------------
Default: Radius, Local, Line
Console_Login: Line, None

Enable Authentication Method Lists
----------------------------------
Default: Radius, Enable
Console_Enable: Enable, None

Line                        Login Method List           Enable Method
                                                        List
--------------              -----------------           ----------------
                                                        --
Console                     Console_Login               Console_Enable
Telnet                      Default                     Default
SSH                         Default                     Default

http: Radius, Local
https: Radius, Local
dot1x: Radius
```

Related Commands

aaa authentication login

aaa authentication enable

login authentication

enable authentication

ip http authentication

ip https authentication

password

The **password** Line Configuration mode command specifies a password on a line. To remove the password, use the **no** form of this command.

Syntax

password *password* [**encrypted**]

no password

Parameters

- *password* — Password for this level (Range: 1-159 characters).
- **encrypted** — Encrypted password to be entered, copied from another device configuration.

Default Setting

No password is defined.

Command Mode

Line Configuration mode

Command Usage

If a password is defined as encrypted, the required password length is 32 characters.

Example

The following example specifies password **secret** on a console.

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

Related Commands

show privilege

enable password

The **enable password** Global Configuration mode command sets a local password to control access to user and privilege levels. To remove the password requirement, use the **no** form of this command.

Syntax

enable password [**level** *level*] *password* [**encrypted**]

no enable password [**level** *level*]

Parameters

- *password* — Password for this level (Range: 1-159 characters).

- *level* — Level for which the password applies. If not specified the level is 15 (Range: 1-15).
- **encrypted** — Encrypted password entered, copied from another device configuration.

Default Setting

No enable password is defined.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example sets local level 15 password **secret** to control access to user and privilege levels.

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

Related Commands

show privilege

username

The **username** Global Configuration mode command creates a user account in the local database. To remove a user name, use the **no** form of this command.

Syntax

username *name* [**password** *password*] [**level** *level*] [**encrypted**]

no username *name*

Parameters

- *name* — The name of the user (Range: 1- 20 characters).
- *password* — The authentication password for the user. (Range: 1-159 characters)
- *level* — The user level (Range: 1-15).
- **encrypted** — Encrypted password entered, copied from another device configuration.

Default Setting

No user is defined.

Command Mode

Global Configuration mode

Command Usage

User account can be created without a password.

Example

The following example configures user **bob** with password **lee** and user level 15 to the system.

```
Console(config)# username bob password lee level 15
```

Related Commands

show privilege

show users accounts

The **show users accounts** Privileged EXEC mode command displays information about the local user database.

Syntax

show users accounts

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the local users configured with access to the system.

```
Console# show users accounts


Username     Privilege     Password        Password Expiry     Lockout
                           Aging           date

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

Bob          1             120             Jan 21 2005         -

Admin        15            120             Jan 21 2005         -
```

The following table describes significant fields shown above.

Field	Description
Username	Name of the user.
Privilege	User’s privilege level.
Password Aging	User’s password expiration time in days.
Password Expiry Date	Expiration date of the user’s password.

Lockout	If lockout control is enabled, specifies the number of failed authentication attempts since the user last logged in successfully. If the user account is locked, specifies LOCKOUT.

ACL Commands

.

Table 4-7. ACL Commands

Command	Function	Mode	Page
ip-access-list	Enables the IP-Access Configuration mode and creates Layer 3 ACLs. To delete an ACL, use the **no** form of this command.	GC	4-300
permit (ip)	Permits traffic if the conditions defined in the permit statement match.	ACL	4-301
deny (IP)	Denies traffic if the conditions defined in the deny statement match.	ACL	4-304
mac access-list	Enables the MAC-Access List Configuration mode and creates Layer 2 ACLs. To delete an ACL, use the **no** form of this command.	GC	4-306
permit (MAC)	Defines permit conditions of an MAC ACL.	ACL	4-307
deny (MAC)	Denies traffic if the conditions defined in the deny statement match.	ACL	4-308
service-acl	Applies an ACL to the input interface. To detach an ACL from an input interface, use the **no** form of this command.	IC	4-310
show access-lists	Displays access control lists (ACLs) defined on the device.	PE	4-310
show interfaces access-lists	Displays access lists applied on interfaces.	PE	4-311

ip-access-list

The **ip-access-list** Global Configuration command enables the IP-Access Configuration mode and creates Layer 3 ACLs. To delete an ACL, use the **no** form of this command.

Syntax

ip-access-list *name*

no ip-access-list *name*

Parameters

- *name* — Specifies the name of the ACL.

Default Setting

The default for all ACLs is **deny-all**.

Command Mode

Global Configuration mode

Command Usage

Up to 1018 rules can be defined on the device, depending on the type of rule defined.

Examples

The following example shows how to create an IP ACL.

```
Console(config)# ip-access-list ip-acl1
Console(config-ip-al)#
```

Related Commands

permit (ip)

deny (IP)

show access-lists

service-acl

match

permit (ip)

The **permit** IP-Access List Configuration mode command permits traffic if the conditions defined in the permit statement match.

Syntax

permit {**any** | *protocol*} {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

permit-icmp {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} {**any** | i*cmp-type*} {**any** | *icmp-code*} [**dscp** *number* | **ip-precedence** *number*]

permit-igmp {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} {**any** | i*gmp-type*} [**dscp** *number* | **ip-precedence** *number*]

permit-tcp {**any** | { *source source-wildcard*}} {**any** | *source-port*} {**any** |{ *destination destination-wildcard*}} {**any** | *destination-port*} [**dscp** *number* | **ip-precedence** *number*] [**flags** *list-of-flags*]

permit-udp {**any** | { *source source-wildcard*}} {**any** | *source-port*} {**any** | {*destination destination-wildcard*}} {**any** | *destination-port*} [**dscp** *number* | **ip-precedence** *number*]

Parameters

- *source* — Specifies the source IP address of the packet. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *source-wildcard* — Specifies wildcard to be applied to the source IP address. Use 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination* — Specifies the destination IP address of the packet. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination-wildcard* — Specifies wildcard to be applied to the destination IP address. Use 1s in bit positions to be ignored. . Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.

- *protocol* — Specifies the abbreviated name or number of an IP protocol. (Range: 0-255)

The following table lists protocols that can be specified:

IP Protocol	Abbreviated Name	Protocol Number
Internet Control Message Protocol	icmp	1
Internet Group Management Protocol	igmp	2
IP in IP (encapsulation) Protocol	ipinip	4
Transmission Control Protocol	tcp	6
Exterior Gateway Protocol	egp	8
Interior Gateway Protocol	igp	9
User Datagram Protocol	udp	17
Host Monitoring Protocol	hmp	20
Reliable Data Protocol	rdp	27
Inter-Domain Policy Routing Protocol	idpr	35
Inter-Domain Routing Protocol	idrp	45
Reservation Protocol	rsvp	46
General Routing Encapsulation	gre	47
Encapsulating Security Payload (50)	esp	50
Authentication Header	ah	51
EIGRP routing protocol	eigrp	88
Open Shortest Path Protocol	ospf	89
Protocol Independent Multicast	pim	103
Layer Two Tunneling Protocol	l2tp	115
ISIS over IPv4	isis	124
(any IP protocol)	any	(25504)

- **dscp** — Indicates matching the dscp number with the packet dscp value.
- **ip-precedence** — Indicates matching ip-precedence with the packet ip-precedence value.
- *icmp-type* — Specifies an ICMP message type for filtering ICMP packets. Enter a value or one of the following values: **echo-reply**, **destination-unreachable**, **source-quench**, **redirect**, **alternate-host-address**, **echo-request**, **router-advertisement**, **router-solicitation**, **time-exceeded**, **parameter-problem**, **timestamp,**

timestamp-reply, **information-request**, **information-reply**,**address-mask-request**, **address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request**, **mobile-registration-reply**, **domain-name-request**, **domain-name-reply**, **skip** and **photuris**. (Range: 0-255)

- *icmp-code* — Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. (Range: 0-255)
- *igmp-type* — IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: **dvmrp**, **host-query**, **host-report**, **pim** or **trace**, **host-report-v2**, **host-leave-v2**, **host-report-v3** (Range: 0-255)
- *destination-port* — Specifies the UDP/TCP destination port. (Range: 0-65535)
- *source-port* — Specifies the UDP/TCP source port. (Range: 0-65535)
- *list-of-flags* — Specifies a list of TCP flags that can be triggered. If a flag is set, it is prefixed by "+". If a flag is not set, it is prefixed by "-". Possible values: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** and **-fin**. The flags are concatenated into one string. For example: **+fin-ack**.

Default Setting

No IPv4 ACL is defined.

Command Mode

IP-Access List Configuration mode

Command Usage

Use the **ip-access-list** Global Configuration mode command to enable the IP-Access List Configuration mode.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

Examples

The following example shows how to define a permit statement for an IP ACL.

```
Console(config)# ip-access-list ip-acl1
Console(config-ip-al)# permit rsvp 192.1.1.1 0.0.0.0 any dscp 56
```

Related Commands

ip-access-list

permit (ip)

show access-lists

deny (IP)

The **deny** IP-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

Syntax

deny [**disable-port**] {**any** | *protocol*} {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*] [**in-port** *port-num* | **out-port** *port-num*]

deny-icmp [**disable-port]** {**any**|{*source source-wildcard*}} {**any**|{*destination destination-wildcard*}} {**any**|*icmp-type*} {**any**|*icmp-code*} [**dscp number** | *ip-precedence number*]

deny-igmp [**disable-por**t] {**any**|{*source source-wildcard*}} {**any**|{*destination destination-wildcard*}} {**any**|*igmp-type*} [**dscp number** | *ip-precedence number*]

deny-tcp [**disable-port**] {**any|**{ *source source-wildcard*}} {**any**|*source-port*} {**any**|{ *destination destination-wildcard*}} {**any**|*destination-port*} [**dscp number** | *ip-precedence number*] [**flags** *list-of-flags*]

deny-udp [**disable-port**] {**any**|{ *source source-wildcard*}} {**any|** *source-port*} {**any**|{*destination destination-wildcard*}} {**any**|*destination-port*} [**dscp number** | *ip-precedence number*]

Parameters

- disable-port — Specifies the ethernet interface is disabled if the condition is matched.
- *source* — Specifies the IP address or host name from which the packet was sent. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *source-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination* — Specifies the IP address or host name to which the packet is being sent. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *protocol* — Specifies the abbreviated name or number of an IP protocol.
- **in-port** *port-num* — (Optional) Specifies the output port of the devise. In case of egress classification this port will be devise input port.
- **out-port** *port-num* — (Optional) Specifies the input port of the devise.
- **dscp** *number* — Specifies the DSCP value.
- **ip-precedence** *number* — Specifies the IP precedence value.
- **fragments** — Displays the set of conditions would be applied only to noninitial fragments.
- *icmp-type* — Specifies an ICMP message type for filtering ICMP packets.

Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request,domain-name-reply,skip,photuris.

- *icmp-code* — Specifies an ICMP message code for filtering ICMP packets.
- *igmp-type* — IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3.
- *destination-port* — Specifies the UDP/TCP destination port.
- *source-port* — Specifies the UDP/TCP source port.
- **flags** *list-of-flags* — List of TCP flags that should occur. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Avaiable options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.

The following table lists protocols that can be specified:

IP Protocol	Abbreviated Name	Protocol Number
Internet Control Message Protocol	icmp	1
Internet Group Management Protocol	igmp	2
IP in IP (encapsulation) Protocol	ip	4
Transmission Control Protocol	tcp	6
Exterior Gateway Protocol	egp	8
Interior Gateway Protocol	igp	9
User Datagram Protocol	udp	17
Host Monitoring Protocol	hmp	20
Reliable Data Protocol	rdp	27
Inter-Domain Policy Routing Protocol	idpr	35
Inter-Domain Routing Protocol	idrp	45
Reservation Protocol	rsvp	46
General Routing Encapsulation	gre	47
Encapsulating Security Payload (50)	esp	50
Authentication Header	ah	51
EIGRP routing protocol	eigrp	88

IP Protocol	Abbreviated Name	Protocol Number
Open Shortest Path Protocol	ospf	89
Protocol Independent Multicast	pim	103
Layer Two Tunneling Protocol	l2tp	115
ISIS over IPv4	isis	124
(any IP protocol)	any	(25504)

Default Setting

This command has no default configuration

Command Mode

IP-Access List Configuration mode

Command Usage

Use the **ip-access-list** Global Configuration mode command to enable the IP-Access List Configuration mode.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the defined conditions are denied.

Examples

The following example shows how to define a permit statement for an IP ACL.

```
Console(config)# ip-access-list ip-acl1
Console(config-ip-al)# deny rsvp 192.1.1.1 0.0.0.255 any
```

Related Commands

ip-access-list

permit (ip)

show access-lists

mac access-list

The **mac access-list** Global Configuration mode command enables the MAC-Access List Configuration mode and creates Layer 2 ACLs. To delete an ACL, use the **no** form of this command.

Syntax

mac access-list *name*

no mac access-list *name*

Parameters

- *name* — Specifies the name of the ACL.

Default Setting

The default for all ACLs is **deny all**.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example shows how to create a MAC ACL.

```
Console(config)# mac access-list macl-acl1
Console(config-mac-al)#
```

Related Commands

permit (MAC)

deny (MAC)

show access-lists

service-acl

match

permit (MAC)

The **permit** MAC-Access List Configuration mode command defines permit conditions of an MAC ACL.

Syntax

permit {**any** | {**host** *source source-wildcard*} **any** | {*destination destination-wildcard*}} [**vlan** *vlan-id*] [**cos** *cos cos-wildcard*] [**ethtype** *eth-type*] [**inner-vlan** *vlan-id*]

Parameters

- *source* — Specifies the source MAC address of the packet.
- *source-wildcard* — Specifies wildcard bits to be applied to the source MAC address. Use 1s in bit positions to be ignored.
- *destination* — Specifies the MAC address of the host to which the packet is being sent.
- *destination-wildcard* — Specifies wildcard bits to be applied to the destination MAC address. Use 1s in bit positions to be ignored.
- *vlan-id* — Specifies the ID of the packet vlan. (Range: 0-4095)
- *cos* — Specifies the Class of Service (CoS) for the packet. (Range: 0-7)
- *cos-wildcard* — Specifies wildcard bits to be applied to the CoS.
- *eth-type* — Specifies the Ethernet type of the packet.(Range: 0-0xFFFF)

- **inner vlan** *eth-type* — The inner VLAN of a double tagged packet.

Default Setting

No MAC ACL is defined.

Command Mode

MAC-Access List Configuration mode

Command Usage

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.

The inner-vlan field can be assigned only on:

- Fast Ethernet customer interfaces (the port mode is customer).
- Service provider interfaces when ALL the traffic is double tagged.

Example

The following example shows how to create a MAC ACL with permit rules.

```
Console(config)# mac access-list macl-acl1
Console(config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 6
```

Related Commands

mac access-list

deny (MAC)

show access-lists

deny (MAC)

The **deny** MAC-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

deny *destination*

deny [**disable-port**] {**any** | {*source source-wildcard*} {**any** | {*destination destination- wildcard*}}[**vlan** *vlan-id*] [**cos** *cos cos-wildcard*] [**ethtype** *eth-type*] [**inner-vlan** *vlan id*]

Parameters

- **disable-port** — Indicates that the port is disabled if the statement is deny.
- *source* — Specifies the MAC address of the host from which the packet was sent.
- *source-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored.
- *destination* — Specifies the MAC address of the host to which the packet is

being sent.

- *destination-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1s in bit positions to be ignored.
- *vlan-id* — Specifies the ID of the packet vlan. (Range: 0-4095).
- *cos* — Specifies the packets's Class of Service (CoS) (Range: 0-7).
- *cos-wildcard* — Specifies wildcard bits to be applied to the CoS.
- *eth-type* — Specifies the packet's Ethernet type (Range: 0-0xFFFF).
- **inner-vlan** *vlan id* — The inner VLAN ID of a double tagged packet.

Default Setting

This command has no default configuration.

Command Mode

MAC-Access List Configuration mode

Command Usage

MAC BPDU packets cannot be denied.

This command defines an Access Control Element (ACE). An ACE can only be removed by deleting the ACL, using the **no mac access-list** Global Configuration mode command. Alternatively, the Web-based interface can be used to delete ACEs from an ACL.

The inner-vlan field can be assigned only on:

- Fast Ethernet customer interfaces (the port mode is customer).
- Service provider interfaces when ALL the traffic is double tagged.

Use the following user guidelines:

- Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.
- If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.

Example

The following example shows how to create a MAC ACL with deny rules on a device.

```
Console(config)# mac access-list macl1
Console (config-mac-acl)# deny 6:6:6:6:6:6:0:0:0:0:0:0 any
```

Related Commands

mac access-list

permit (MAC)

show access-lists

service-acl

The **service-acl** Interface Configuration mode command applies an ACL to the input interface. To detach an ACL from an input interface, use the **no** form of this command.

Syntax

service-acl {**input** *acl-name*}

no service-acl {**input**}

Parameters

- *acl-name* — Specifies the ACL to be applied to the input interface.

Default Setting

This command has no default configuration.

Command Mode

Interface (Ethernet, port-channel) Configuration mode.

Command Usage

In advanced mode, when an ACL is bound to an interface, the port trust mode is set to trust L2-L3 and not to L2.

Example

The following example, binds (services) an ACL to port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# service-acl input macl1
```

Related Commands

show interfaces access-lists

show access-lists

The **show access-lists** Privileged EXEC mode command displays access control lists (ACLs) defined on the device.

Syntax

show access-lists [*name*]

Parameters

- *name* — Name of the ACL.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Examples

The following example displays access lists on a device.

```
Console# show access-lists
IP access list ACL1
permit ip host 172.30.40.1 any
permit rsvp host 172.30.8.8 any
```

Related Commands

ip-access-list

permit (ip)

deny (IP)

mac access-list

permit (MAC)

deny (MAC)

show interfaces access-lists

The **show interfaces access-lists** Privileged EXEC mode command displays access lists applied on interfaces.

> **show interfaces access-lists** [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*).
- *port-channel-number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays ACLs applied to the interfaces of a device:

```
Console# show interfaces access-lists


Interface        Input ACL

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

1/e1             ACL1

2/e1             ACL3
```

Related Commands

service-acl

Address Table Commands

.

Table 4-8. Address Table Commands

Command	Function	Mode	Page
bridge address	Adds a MAC-layer station source address to the bridge table. To delete the MAC address, use the **no** form of this command.	ICV	4-314
bridge multicast filtering	Enables filtering multicast addresses. To disable filtering multicast addresses, use the **no** form of this command.	GC	4-315
bridge multicast address	Registers a MAC-layer multicast address in the bridge table and statically adds ports to the group. To unregister the MAC address, use the **no** form of this command	ICV	4-316
bridge multicast forbidden address	Forbids adding a specific multicast address to specific ports. Use the **no** form of this command to return to the default configuration.	ICV	4-317
bridge multicast forward-all	Use the bridge multicast ip-address interface configuration command to register IP-layer multicast address to the bridge table, and to add statically ports to the group.	ICV	4-318
bridge multicast forward-all	Enables forwarding all multicast packets on a port. To restore the default configuration, use the **no** form of this command.	ICV	4-318
bridge multicast forbidden forward-all	Forbids a port to be a forward-all-multicast port. To restore the default configuration, use the **no** form of this command.	ICV	4-319
bridge aging-time	Sets the address table aging time. To restore the default configuration, use the **no** form of this command.	GC	4-319
clear bridge	Removes any learned entries from the forwarding database.	PE	4-320
port security	Locks the port, thereby, blocking unknown traffic and preventing the port from learning new addresses. To return to the default configuration, use the **no** form of this command.	IC	4-321
port security mode	Configures the port security mode. To return to the default configuration, use the **no** form of this command.	IC	4-321
port security max	Configures the maximum number of addresses that can be learned on the port while the port is in port security mode. To return to the default configuration, use the **no** form of this command.	IC	4-322
port security routed secure-address	Adds a MAC-layer secure address to a routed port. Use the **no** form of this command to delete a MAC address.	IC	4-323
show bridge address-table	Displays all entries in the bridge-forwarding database.	PE	4-324
show bridge address-table static	Displays statically created entries in the bridge-forwarding database.	PE	4-325
show bridge address-table countt	Displays the number of addresses present in the Forwarding Database.	PE	4-326
show bridge multicast address-tablet	Displays bridge multicast address table information	UE	4-327

Table 4-8. Address Table Commands

Command	Function	Mode	Page
show bridge multicast address-table statict	Displays the statically configured multicast addresses.	UE	4-328
show bridge multicast filtering	Displays the multicast filtering configuration.	UE	4-329
show ports security	Displays the port-lock status.	PE	4-330
show ports security addresses	Displays the current dynamic addresses in locked ports.	PE	4-331

bridge address

The **bridge address** Interface Configuration (VLAN) mode command adds a MAC-layer station source address to the bridge table. To delete the MAC address, use the **no** form of this command.

Syntax

bridge address *mac-address* {**ethernet** *interface* | **port-channel** *port-channel-number*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]

no bridge address [*mac-address*]

Parameters

- *mac-address* — A valid MAC address.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.
- **permanent —** The address can only be deleted by the **no bridge address** command.
- **delete-on-reset** — The address is deleted after reset.
- **delete-on-timeout —** The address is deleted after "age out" time has expired.
- **secure** — The address is deleted after the port changes mode to unlock learning (**no port security** command). This parameter is only available when the port is in the learning locked mode.

Default Setting

No static addresses are defined. The default mode for an added address is **permanent**.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

Using the **no** form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

Example

The following example adds a permanent static MAC-layer station source address 3aa2.64b3.a245 on port 1/e16 to the bridge table.

```
Console(config)# interface vlan 2
Console(config-if)# bridge address 3aa2.64b3.a245 ethernet 1/e16
permanent
```

Related Commands

clear bridge

show bridge address-table static

show bridge address-table count

bridge multicast filtering

The **bridge multicast filtering** Global Configuration mode command enables filtering multicast addresses. To disable filtering multicast addresses, use the **no** form of this command.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Setting

Filtering multicast addresses is disabled. All multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

Command Usage

If multicast devices exist on the VLAN, do not change the unregistered multicast addresses state to drop on the switch ports.

If multicast devices exist on the VLAN and IGMP-snooping is not enabled, the **bridge multicast forward-all** command should be used to enable forwarding all multicast packets to the multicast switches.

Example

In this example, bridge multicast filtering is enabled.

```
Console(config)# bridge multicast filtering
```

Related Commands

bridge multicast address

bridge multicast forbidden address

bridge multicast forward-all

bridge multicast forbidden forward-all

show bridge multicast filtering

bridge multicast address

The **bridge multicast address** Interface Configuration (VLAN) mode command registers a MAC-layer multicast address in the bridge table and statically adds ports to the group. To unregister the MAC address, use the **no** form of this command.

Syntax

bridge multicast address {*mac-multicast-address*}

bridge multicast address {*mac-multicast-address* [**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast address {*mac-multicast-address*}

Parameters

- **add** — Adds ports to the group. If no option is specified, this is the default option.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — A valid MAC multicast address.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of ports.

Default Setting

No multicast addresses are defined.

Command Mode

Interface configuration (VLAN) mode

Command Usage

If the command is executed without **add** or **remove**, the command only registers the group in the bridge database.

Static multicast addresses can only be defined on static VLANs.

Examples

The following example registers the MAC address:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
```

The following example registers the MAC address and adds ports statically.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03 add
ethernet 1/e1-e9, 2/e2
```

Related Commands

bridge multicast filtering

bridge multicast forbidden address

bridge multicast forward-all

bridge multicast forbidden forward-all

bridge multicast forbidden address

The **bridge multicast forbidden address** Interface Configuration (VLAN) mode command forbids adding a specific multicast address to specific ports. Use the **no** form of this command to return to the default configuration.

Syntax

bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forbidden address {*mac-multicast-address*}

Parameters

- **add** — Adds ports to the group.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — A valid MAC multicast address.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Setting

No forbidden addresses are defined.

Command Modes

Interface Configuration (VLAN) mode

Command Usage

Before defining forbidden ports, the multicast group should be registered.

Examples

In this example, MAC address 0100.5e02.0203 is forbidden on port 2/e9 within VLAN 8.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 0100.5e.02.0203
Console(config-if)# bridge multicast forbidden address 0100.5e02.0203
add ethernet 2/e9
```

Related Commands

bridge multicast filtering

bridge multicast address

bridge multicast forward-all

bridge multicast forbidden forward-all

show bridge multicast filtering

bridge multicast forward-all

The **bridge multicast forward-all** Interface Configuration (VLAN) mode command enables forwarding all multicast packets on a port. To restore the default configuration, use the **no** form of this command.

Syntax

bridge multicast forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forward-all

Parameters

- **add** — Force forwarding all multicast packets.
- **remove** — Do not force forwarding all multicast packets.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Setting

This setting is disabled.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

There are no user guidelines for this command.

Example

In this example, all multicast packets on port 1/e8 are forwarded.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forward-all add ethernet 1/e8
```

Related Commands

bridge multicast filtering

bridge multicast address

bridge multicast forbidden address

bridge multicast forbidden forward-all

show bridge multicast filtering

bridge multicast forbidden forward-all

The **bridge multicast forbidden forward-all** Interface Configuration (VLAN) mode command forbids a port to be a forward-all-multicast port. To restore the default configuration, use the **no** form of this command.

Syntax

bridge multicast forbidden forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forbidden forward-all

Parameters

- **add** — Forbids forwarding all multicast packets.
- **remove** — Does not forbid forwarding all multicast packets.
- *interface-list* — Separates nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separates nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Setting

This setting is disabled.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

IGMP snooping dynamically discovers multicast device ports. When a multicast device port is discovered, all the multicast packets are forwarded to it unconditionally.

This command prevents a port from becoming a multicast device port.

Example

In this example, forwarding all multicast packets to 1/e1 with VLAN 2 is forbidden.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forbidden forward-all add
ethernet 1/e1
```

Related Commands

bridge multicast filtering

bridge multicast address

bridge multicast forbidden address

bridge multicast forward-all

show bridge multicast filtering

bridge aging-time

The **bridge aging-time** Global Configuration mode command sets the address table aging time. To restore the default configuration, use the **no** form of this command.

Syntax

bridge aging-time *seconds*

no bridge aging-time

Parameters

- *seconds* — Time in seconds. (Range: 10-630 seconds)

Default Setting

The default is 300 seconds.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

In this example the bridge aging time is set to 250.

```
Console(config)# bridge aging-time 250
```

Related Commands

bridge address

clear bridge

clear bridge

The **clear bridge** Privileged EXEC mode command removes any learned entries from the forwarding database.

Syntax

clear bridge

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

In this example, the bridge tables are cleared.

```
Console# clear bridge
```

Related Commands

bridge address

port security

The **port security** Interface Configuration mode command locks the port, thereby, blocking unknown traffic and preventing the port from learning new addresses. To return to the default configuration, use the **no** form of this command.

Syntax

port security [**forward** | **discard | discard-shutdown**] [**trap** *seconds*]

no port security

Parameters

- **forward** — Forwards packets with unlearned source addresses, but does not learn the address.
- **discard** — Discards packets with unlearned source addresses. This is the default if no option is indicated.
- **discard-shutdown** — Discards packets with unlearned source addresses. The port is also shut down.
- *seconds* — Sends SNMP traps and defines the minimum amount of time in seconds between consecutive traps. (Range: 1-1000000)

Default Setting

This setting is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

Port must be set to dot1x multiple-hosts in order to perform Port Security.

Example

In this example, port 1/e1 forwards all packets without learning addresses of packets from unknown sources and sends traps every 100 seconds if a packet with an unknown source address is received.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# port security forward trap 100
```

Related Commands

port security mode

show ports security

port security mode

The port security mode Interface Configuration (Ethernet, port-channel) mode command configures the port security learning mode. To restore the default configuration, use the no form of this command.

Syntax

port security mode {**lock** | mac-addresses}

no port security mode

Parameters

- **lock** — Saves the current dynamic MAC addresses associated with the port and disables learning, relearning and aging.
- **mac-addresses** — Deletes the current dynamic MAC addresses associated with the port and learns up to the maximum number addresses allowed on the port. Relearning and aging are enabled.

Default Setting

This setting is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

In this example, port security mode is set to dynamic for Ethernet interface 1/e7.

```
Console(config)# interface ethernet 1/e7
Console(config-if)# port security mac-addresses
```

Related Commands

port security max

show ports security

port security max

The **port security max** Interface Configuration (Ethernet, port-channel) mode command configures the maximum number of addresses that can be learned on the port while the port is in port security mode. To return to the default configuration, use the **no** form of this command.

Syntax

port security max *max-addr*

no port security max

Parameters

- *max-addr*— Maximum number of addresses that can be learned by the port. (Range: 1-128)

Default Setting

The default is 1 address.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

This command is only relevant in dynamic learning modes.

Example

In this example, the maximum number of addresses that are learned on port 1/e7 before it is locked is set to 20.

```
Console(config)# interface ethernet 1/e7
Console(config-if)# port security mode dynamic
Console(config-if)# port security max 20
```

Related Commands

port security mode

show ports security

port security routed secure-address

The **port security routed secure-address** Interface Configuration (Ethernet, port-channel) mode command adds a MAC-layer secure address to a routed port. Use the **no** form of this command to delete a MAC address.

Syntax

port security routed secure-address *mac-address*

no port security routed secure-address *mac-address*

Parameters

- *mac-address* — A valid MAC address.

Default Setting

No addresses are defined.

Command Mode

Interface Configuration (Ethernet, port-channel) mode. Cannot be configured for a range of interfaces (range context).

Command Usage

The command enables adding secure MAC addresses to a routed port in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

Example

In this example, the MAC-layer address 66:66:66:66:66:66 is added to port 1/e1.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# port security routed secure-address
66:66:66:66:66:66
```

Related Commands

show ports security addresses

show bridge address-table

The **show bridge address-table** Privileged EXEC mode command displays all entries in the bridge-forwarding database.

Syntax

show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

Internal usage VLANs (VLANs that are automatically allocated on ports with a defined Layer 3 interface) are presented in the VLAN column by a port number and not by a VLAN ID.

"Special" MAC addresses that were not statically defined or dynamically learned are displayed in the MAC address table. This includes, for example, MAC addresses defined in ACLS.

Example

In this example, all classes of entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table


Aging time is 300 sec


interface     mac address                  Port          Type
```

```
---------     --------------                ----          -------
1             00:60:70:4C:73:FF             5/e8          dynamic
1             00:60:70:8C:73:FF             5/e8          dynamic
200           00:10:0D:48:37:FF             5/e9          static
```

Related Commands

bridge address

show bridge address-table static

The **show bridge address-table static** Privileged EXEC mode command displays statically created entries in the bridge-forwarding database.

Syntax

show bridge address-table static [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port*.*
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

In this example, all static entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table static

Aging time is 300 sec

vlan       mac address               port            type
----       -----------------         ----            -----------------
1          00:60:70:4C:73:FF         1/e8            Permanent
1          00:60.70.8C.73:FF         1/e8            delete-on-timeout
200        00:10:0D:48:37:FF         1/e9            delete-on-reset
```

Related Commands

bridge address

show bridge address-table count

The **show bridge address-table count** Privileged EXEC mode command displays the number of addresses present in the Forwarding Database.

Syntax

show bridge address-table count [**vlan** *vlan*][**ethernet** *interface-number* | **port-channel** *port-channel-number*]

Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port*.*
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

In this example, the number of addresses present in all VLANs are displayed.

```
Console# show bridge address-table count


Capacity: 8192

Free: 8083

Used: 109


Secure addresses: 2

Static addresses: 1

Dynamic addresses: 97

Internal addresses: 9
```

Related Commands

bridge address

show bridge multicast address-table

The **show bridge multicast address-table** User EXEC mode command displays multicast MAC address or IP address table information.

Syntax

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *mac-multicast-address* | *ip-multicast-address*] [**format ip** | **format mac**] [**source** *ip address*]

Parameters

- *vlan-id* — A valid VLAN ID value.
- *mac-multicast-address* — A valid MAC multicast address.
- *ip-multicast-address* — A valid IP multicast address.
- **format** *ip|mac* — Multicast address format. This is relevant only f the bridging mode is mac group. Can be **ip** or **mac**. If the format is unspecified, the default is **mac**.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

A MAC address can be displayed in IP format only if it is in the range of 0100.5e00.0000-0100.5e7f.ffff.

Example

In this example, multicast MAC address and IP address table information is displayed.

```
Console# show bridge multicast address-table format ip

Vlan       IP/MAC Address         Type          Ports
----       -----------------      ------        ---------
1          0100.9923.8787         static        1/e1,2/e2
1          224-239.130|2.2.3      dynamic       1/e1,2/e2
19         224-239.130|2.2.8      static        1/e1-e8
19         224-239.130|2.2.8      dynamic       1/e9-e11

Forbidden ports for multicast addresses:

Vlan       IP/MAC Address         Ports
```

```
----        -----------------     ------

1           224-239.130|2.2.3     2/e8

19          224-239.130|2.2.8     2/e8
```

Note: A multicast MAC address maps to multiple IP addresses as shown above.

Related Commands

bridge multicast address

show bridge multicast address-table static

The **show bridge multicast address-table static** Privileged EXEC mode command displays the statically configured multicast addresses.

show bridge multicast address-table static [**vlan** *vlan-id*] [**address** *mac-multicast-address* | *ip-multicast-address*] [**source** *ip-address*]

Parameters

- *vlan-id* — Indicates the VLAN ID. This has to be a valid VLAN ID value.
- *mac-multicast-address* — A valid MAC multicast address.
- *ip-multicast-address* — A valid IP multicast address.
- *ip-address* — Source IP address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it's in the range 0100.5e00.0000 through 0100.5e7f.ffff.

Example

```
Console# show bridge multicast address-table static


MAC-GROUP table


Vlan            MAC Address     Type            Ports
----            -------------   -------         ----------
                -
1               0100.9923.878   static          1/1, 2/2
                7


Forbidden ports for multicast addresses:


Vlan            MAC Address     Ports
----            -------------   -----
                -
```

show bridge multicast filtering

The **show bridge multicast filtering** User EXEC mode command displays the multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

Parameters

- *vlan-id* — VLAN ID value.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

In this example, the multicast configuration for VLAN 1 is displayed.

```
Console# show bridge multicast filtering 1


Filtering: Enabled

VLAN: 1


Port          Forward-Unregistered        Forward-All

              Static        Status        Static           Status

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

1/e1          Forbidden     Filter        Forbidden        Filter

1/e2          Forward       Forward(s)    Forward          Forward(s)

1/e3          -             Forward(d)    -                Forward(d)
```

Related Commands

bridge multicast filtering

bridge multicast forbidden address

bridge multicast forward-all

bridge multicast forbidden forward-all

show ports security

The **show ports security** Privileged EXEC mode command displays the port-lock status.

Syntax

show ports security [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port*.*
- *port-channel-number* — A valid port-channel number*.*

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

In this example, all classes of entries in the port-lock status are displayed:

```
Console# show ports security


Port    Status      Learning    Action      Maximum    Trap        Frequency

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

1/e1    Locked      Dynamic     Discard     3          Enable      100

1/e2    Unlocked    Dynamic     -           28         -           -

1/e3    Locked      Disabled    Discard,    8          Disable     -
                                Shutdown
```

The following tables describes the fields shown above.

Field	Description
Port	Port number
Status	Locked/Unlocked
Learning	Learning mode
Action	Action on violation
Maximum	Maximum addresses that can be associated on this port in Static Learning mode or in Dynamic Learning mode
Trap	Indicates if traps are sent in case of a violation
Frequency	Minimum time between consecutive traps

Related Commands

port security mode

port security max

show ports security addresses

The **show ports security addresses** Privileged EXEC mode command displays the current dynamic addresses in locked ports.

Syntax

show ports security addresses [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

In this example, dynamic addresses in currently locked ports are displayed.

```
Console# show ports security addresses

Port      Status        Learning        Current        Maximum
----      --------      --------        -------        -------
1/e1      Disabled      Lock            -              1
1/e2      Disabled      Lock            -              1
1/e3      Enabled       Max-addresses   0              1
1/e4      Port is a member in port-channel ch1
1/e5      Disabled      Lock            -              1
1/e6      Enabled       Max-addresses   0              10
ch1       Enabled       Max-addresses   0              50
ch2       Enabled       Max-addresses   0              128
```

In this example, dynamic addresses in currently locked port 1/e1 are displayed.

```
Console# show ports security addresses ethernet 1/e1

Port      Status          Learning      Current        Maximum
----      --------        --------      -------        -------
1/e1      Disabled        Lock          -              1
```

LLDP Commands

Table 4-9. LLDP Commands			
Command	Function	Mode	Page
lldp optional-tlv	To specify which optional TLVs from the basic set should be transmitted, use the lldp optional-tlv command in interface configuration mode.	ICE	4-333
lldp med enable	To enable Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) on an interface, use the lldp med enable command in interface configuration mode.	ICE	4-334
lldp med network-policy (global)	To define LLDP MED network policy, use the lldp med network-policy command in global configuration mode.	GC	4-334
lldp med network-policy (interface)	To attach an LLDP MED network policy to a port, use the lldp med network-policy command in interface configuration mode.	ICE	4-335
lldp med location	To configure location information for the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) for an interface, use the lldp med location command in interface configuration mode.	ICE	4-335
clear lldp rx	To restart the LLDP RX state machine and clearing the neighbors table	PE	4-336
show lldp configuration	To display the Link Layer Discovery Protocol (LLDP) configuration.	PE	4-337
show lldp med configuration	To display the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) configuration, use the show lldp med configuration command in privileged EXEC mode.	PE	4-337
show lldp local	To display the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port, use the show lldp local command in privileged EXEC mode.	PE	4-338
show lldp neighbors	To display information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP), use the show lldp neighbors command in privileged EXEC mode.	PE	4-340

lldp optional-tlv

The **lldp optional-tlv** Interface Configuration (Ethernet) mode command specifies which optional TLVs from the basic set should be transmitted. To revert to the default setting, use the **no** form of this command.

Syntax

lldp optional-tlv *tlv1* [***tlv2*** … *tlv5*]

no lldp optional-tlv

Parameters

- *tlv* — Specifies TLV that should be included. Available optional TLVs are:

port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy.
(Range 1-8192 seconds)

Default Configuration

No optional TLV is transmitted.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no guidelines for this command.

lldp med enable

The **lldp med enable** Interface Configuration (Ethernet) mode command enables the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) on an interface. To disable LLDP MED on an interface, use the **no** form of this command.

Syntax

lldp med enable [tlv1 … tlv3]

no lldp med enable

Parameters

- *tlv* — Specifies TLV that should be included. Available TLVs are: network-policy, location, poe-pse. The capabilities TLV is always included if LLDP-MED is enabled.

Default Configuration

The default configuration is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no guidelines for this command.

lldp med network-policy (global)

The **lldp med network-policy** Global Configuration mode command defines the LLDP MED network policy. To remove LLDP MED network policy, use the **no** form of this command.

Syntax

lldp med network-policy *number application* [**vlan id**] [**vlan-type** {**tagged** | **untagged**}][**up** *priority*] [**dscp** *value*]

no lldp med network-policy *number*

Parameters

- *number* — Network policy sequential number (Range: 1-32).
- *application* — The name or the number of the primary function of the

application defined for this network policy. Available application names are: **voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling**.

- **vlan** *id* — VLAN identifier for the application.
- **vlan-type** — Specifies if the application is using a 'tagged' or an 'untagged' VLAN.
- **up** *priority* — User Priority (Layer 2 priority) to be used for the specified application.
- **dscp** *value* — DSCP value to be used for the specified application.

Default Configuration

No network policy is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the lldp med network-policy interface configuration command to attach a network policy to a port.

lldp med network-policy (interface)

The **lldp med network-policy** Interface Configuration (Ethernet) mode command attaches a LLDP MED network policy to a port. To remove an LLDP MED network policy from a port, use the **no** form of this command.

Syntax

lldp med network-policy *number*

no lldp med network-policy *number*

Parameters

- *number* — Network policy sequential number.

Default Configuration

No network policy is attached.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no guidelines for this command.

lldp med location

The **lldp med location** Interface Configuration (Ethernet) mode configures the location information for the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) for an interface. To delete location information for an interface, use the **no** form of this command.

Syntax

lldp med location coordinate *data*

no lldp med location coordinate

lldp med location civic-address data

no lldp med location civic-address

lldp med location ecs-elin *data*

no lldp med location ecs-elin

Parameters

- **coordinate** — Displays the location is specified as coordinates.
- **civic-address** — Displays the location is specified as civic address.
- **ecs-elin** — Displays the location is specified as ECS ELIN.
- *data* — Displays the data format is as defined in ANSI/TIA 1057. Specifies the location as dotted hexadecimal data: Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. For coordinated: 16. For civic address: 6 - 160 hexadecimal digits . For ECS ELIN: 10 - 25 hexadecimal digits.

Default Configuration

The location is not configured.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no guidelines for this command.

clear lldp rx

The **clear lldp rx** Privileged EXEC mode command restarts the LLDP RX state machine and clearing the neighbors table.

Syntax

clear lldp rx [**ethernet** interface]

Parameters

- *interface* — Ethernet port

Command Mode

Privileged EXEC

User Guidelines

There are no guidelines for this command.

show lldp configuration

The **show lldp configuration** Privileged EXEC mode command displays the Link Layer Discovery Protocol (LLDP) configuration.

Syntax

show lldp configuration [**ethernet** *interface*]

Parameters

interface — Ethernet port

Command Mode

Privileged EXEC

User Guidelines

There are no guidelines for this command.

show lldp med configuration

The **show lldp med configuration** Privileged EXEC mode command displays the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) configuration.

Syntax

show lldp med configuration [**ethernet** *interface*]

Parameters

- *interface* — Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no guidelines for this command.

Example

```
 Switch# show lldp med configuration
 Network policy 1
-------------------
 Application type: Voice
 VLAN ID: 2 tagged
 Layer 2 priority: 0
 DSCP: 0
```

```
Port         Capabilities Network      Location     PoE
                          Policy
----------   ----------   ----------   ----------   ----------
1/1          Yes          Yes          Yes          Yes
1/2          Yes          Yes          Yes          Yes
1/3          Yes          No           No           Yes

Switch# show lldp med configuration ethernet 1/1

Port         Capabilities Network      Location     PoE
                          Policy
----------   ----------   ----------   ----------   ----------
1/1          Yes          Yes          Yes          Yes

Network Policies: 1
```

show lldp local

The **show lldp local** Privileged EXEC mode command in privileged EXEC mode displays the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port.

Syntax

show lldp local ethernet *interface*

Parameters

- *interface* — Ethernet port

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

There are no guidelines for this command.

Example

```
Switch# show lldp local ethernet 1/1

Device ID: 0060.704C.73FF
Port ID: 1
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8

802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full
duplex, 1000BASE-T full duplex
Operational MAU type: 1000BaseTFD

LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity

LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0

LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts


LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
```

show lldp neighbors

The **show lldp neighbors** Privileged EXEC mode command displays information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP).

Syntax

show lldp neighbors [**ethernet** *interface*]

Parameters

- *interface* — Ethernet port

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no guidelines for this command.

Example

```
Switch# show lldp neighbors


Port       Device ID  Port ID    Hold Time  Capabiliti System
                                            es         Name

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

1/1        0060.704C. 1          117        B          ts-7800-2
           73F E

1/1        0060.704C. 1          93         B          ts-7800-2
           73FD

1/2        0060.704C. 9          1          B, R       ts-7900-1
           73F C

1/3        0060.704C. 1          92         W          ts-7900-2
           73FB
```

```
Switch# show lldp neighbors ethernet 1/1

Device ID: 0060.704C.73FE
Port ID: 1
Hold Time: 117
Capabilities: B
System Name: ts-7800-2
System description:
Port description:
Management address: 172.16.1.1

802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported.
Auto-negotiation status: Enabled.
Auto-negotiation Advertised Capabilities: 100BASE-TX full
 duplex, 1000BASE-T full duplex.
Operational MAU type: 1000BaseTFD

LLDP-MED capabilities: Network Policy.
LLDP-MED Device type: Endpoint class 2.

LLDP-MED Network policy
Application type: Voice
Flags: Unknown policy
VLAN ID: 0
Layer 2 priority: 0
DSCP: 0

LLDP-MED Power over Ethernet
Device Type: Power Device
Power source: Primary power
Power priority: High
Power value: 9.6 Watts

LLDP-MED Inventory
Hardware revision: 2.1
Firmware revision: 2.3
Software revision: 2.7.1
```

Location information, if exists, should be displayed too.

The following table describes significant LLDP fields:

Field	Description
Port	The port number.
Device ID	The configured ID (name) or MAC address of the neighbor device.
Port ID	The port ID of the neighbor device.
Hold time	The remaining amount of time, in seconds, the current device will hold the LLDP advertisement from the neighbor device before discarding it.
Capabilities	The capabilities discovered on the neighbor device. Possible values are: B - Bridge R - Router W - WLAN Access Point T - Telephone D - DOCSIS cable device H - Hostr - Repeater O - Other
System name	The neighbor device administratively assigned name.
System description	The system description of the neighbor device.
Port description	The port description of the neighbor device.
Management address	The management address of the neighbor device.
Auto-negotiation support	Specify if the port support auto-negotiation.
Auto-negotiation status	Specify if auto-negotiation is enabled on the port.
Auto-negotiation Advertised Capabilities	The speed/duplex/flow-control capabilities of the port that are advertised by the auto-negotiation.
Operational MAU type	Indicates the MAU type of the port.
LLDP MED	
Capabilities	Define the sender's LLDP-MED capabilities.
Device type	Contains a value that indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, which Endpoint Class it belongs to.

LLDP MED - Network Policy	
Application type	Indicates the primary function of the application defined for this network policy.
Flags	Unknown policy: Policy is required by the device, but is currently unknown. Tagged VLAN: whether the specified application type is using a 'tagged' or an 'untagged' VLAN.
VLAN ID	VLAN identifier for the application.
Layer 2 priority	Layer 2 priority to be used for the specified application.
DSCP	DSCP value to be used for the specified application.
LLDP MED - Power Over Ethernet	
Power type	Indicates whether the device is a Power Sourcing Entity (PSE) or Power Device (PD).
Power Source	Indicates the power source being utilized by a PSE or PD device. A PSE device would advertise its power capability. Available values are: Primary power source and Backup power source. A PD device would advertise its power source. Available values are: Primary power, Local power, Primary and Local power. Power priorityIndicates the priority of the PD device. A PSE device would advertise the power priority configured for the port. A PD device would advertise the power priority configured for the device. Available values are: Critical, High and Low.
Power priority	Indicates the priority of the PD device. A PSE device would advertise the power priority configured for the port. A PD device would advertise the power priority configured for the device. Available values are: Critical, High and Low.
Power value	Indicates the total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
LLDP MED - Location	
Coordinates, Civic address, ECS ELIN.	Displays the raw data of the location information.

AMAP Commands

The AMAP protocol discovers adjacent switches by sending and receiving AMAP "Hello" packets on active Spanning Tree ports. Each port can be defined as being in one of three logical states of processing the AMAP "Hello" packets:

- Discovery — The initial state where a port transmits a "Hello" packet to detect an adjacent switch and then waits for a response.
- Common — The port has detected an adjacent switch and periodically sends "Hello" packets to determine that it is still present.
- Passive — A port enters this state if there is no response to a Discovery "hello" packet. This is a receive-only state and no "Hello" packets are transmitted. If a "Hello" packet is received from an adjacent switch, the port enters the Common state and then transmits a "Hello" packet in reply.

Use the AMAP Global Configuration screen to enable/disable AMAP and configure timeout parameters.

Table 4-10. AMAP Commands

Command	Function	Mode	Page
amap enable	Enables, or disables AMAP on the switch	GC	4-345
amap discovery time	Sets the discovery transmission time interval	GC	4-346
amap common timer	Sets the common phase transmission time interval	GC	4-346
show amap	Displays the current AMAP settings	PE	4-346

amap enable

This command enables AMAP on the switch. Use the **amap disable** command to disable the feature.

Syntax

amap {**enable**}

Parameters

- **enable** — Enables AMAP.

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#amap enable
Console(config)
```

amap discovery time

The time (in seconds) that switch ports in the Discovery state wait for a response to a “Hello” packet from an adjacent switch.

Syntax

amap discovery time *seconds*

no amap discovery time

Parameters

- *seconds* — Discovery transmission timeout value in seconds (Range: 1-65535 seconds)

Default Setting

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#amap discovery time 3000
Console(config)#
```

amap common time

This command sets the time (in seconds) that switch ports in the Common state wait before sending a “Hello” packet to an adjacent switch. If there is no reply packet from an adjacent switch after two timeout intervals, the switch entry for the port will be removed and port will revert to the Discovery state.

Syntax

amap common time *seconds*

Parameters

- *seconds* — Common transmission timeout value in seconds (Range: 1-65535 seconds)

Default Setting

300 seconds

Command Mode

Global Configuration

Example

```
Console(config)#amap common time 5000
Console(config)#
```

show amap

This command displays the current AMAP settings on the switch.

Syntax

show amap

Default Setting

None

Command Mode

Priviledged Executive

Example

```
Console#sh amap
AMAP is currently enabled
AMAP Common Phase Timeout Interval (seconds) = 5000
AMAP Discovery Phase Timeout Interval (seconds) = 3000
Console#
```

Clock Commands

.

Table 4-11. Clock Commands

Command	Function	Mode	Page
clock set	Manually sets the system clock.	PE	4-349
clock source	Configures an external time source for the system clock. Use **no** form of this command to disable external time source.	GC	4-350
clock timezone	Configures an external time source for the system clock. Use **no** form of this command to disable external time source.	GC	4-350
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time). To configure the software not to automatically switch to summer time, use the **no** form of this command.	GC	4-351
sntp authentication-key	Defines an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the **no** form of this command.	GC	4-353
sntp authenticate	Grants authentication for received Simple Network Time Protocol (SNTP) traffic from servers. To disable the feature, use the **no** form of this command.	GC	4-353
sntp trusted-key	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command	GC	4-354
sntp client poll timer	Sets the polling time for the Simple Network Time Protocol (SNTP) client. To return to default configuration, use the **no** form of this command.	GC	4-355
sntp broadcast client enable	Enables Simple Network Time Protocol (SNTP) broadcast clients. To disable SNTP broadcast clients, use the **no** form of this command.t	GC	4-356
sntp anycast client enable	Enables SNTP anycast client. To disable the SNTP anycast client, use the **no** form of this command.	GC	4-357
sntp client enable (Interface)	Enables the Simple Network Time Protocol (SNTP) client on an interface. This applies to both receive broadcast and anycast updates. To disable the SNTP client, use the **no** form of this command.	IC	4-357
sntp unicast client enable	Enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers. To disable requesting and accepting SNTP traffic from servers, use the **no** form of this command.	GC	4-358
sntp unicast client poll	Enables polling for the Simple Network Time Protocol (SNTP) predefined unicast servers. To disable the polling for SNTP client, use the **no** form of this command.	GC	4-359
sntp server	Configures the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from a specified server. To remove a server from the list of SNTP servers, use the **no** form of this command.	GC	4-360
show clock	Displays the time and date from the system clock.	UE	4-361

Table 4-11. Clock Commands			
Command	Function	Mode	Page
show sntp configuration	Shows the configuration of the Simple Network Time Protocol (SNTP).	PE	4-362
show sntp status	Shows the status of the Simple Network Time Protocol (SNTP).	PE	4-363

clock set

The **clock set** Privileged EXEC mode command manually sets the system clock.

Syntax

clock set *hh:mm:ss day month year*

or

clock set *hh:mm:ss month day year*

Parameters

- *hh:mm:ss* — Current time in hours (military format), minutes, and seconds (hh: 0 - 23, mm: 0 - 59, ss: 0 - 59).
- *day* — Current day (by date) in the month (1 - 31).
- *month* — Current month using the first three letters by name (Jan, …, Dec).
- *year* — Current year (2000 - 2097).

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example sets the system time to 13:32:00 on the 7th March 2002.

```
Console# clock set 13:32:00 7 Mar 2002
```

Related Commands

clock source

clock timezone

clock summer-time

clock source

The **clock source** Global Configuration mode command configures an external time source for the system clock. Use **no** form of this command to disable external time source.

Syntax

clock source {**sntp**}

no clock source

Parameters

- **sntp** — SNTP servers

Default Setting

No external clock source

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Examples

The following example configures an external time source for the system clock.

```
Console(config)# clock source sntp
```

Related Commands

clock set

clock timezone

clock summer-time

clock timezone

The **clock timezone** Global Configuration mode command sets the time zone for display purposes. To set the time to the Coordinated Universal Time (UTC), use the **no** form of this command.

Syntax

clock timezone *hours-offset* [**minutes** *minutes-offset*] [**zone** *acronym*]

no clock timezone

Parameters

- *hours-offset* — Hours difference from UTC. (Range: -12 – +13)
- *minutes-offset* — Minutes difference from UTC. (Range: 0 – 59)
- *acronym* — The acronym of the time zone. (Range: Up to 4 characters)

Default Setting

Clock set to UTC.

Command Mode

Global Configuration mode

Command Usage

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Example

The following example sets the timezone to 6 hours difference from UTC.

```
Console(config)# clock timezone -6 zone CST
```

Related Commands

clock set

clock source

clock summer-time

clock summer-time

The **clock summer-time** Global Configuration mode command configures the system to automatically switch to summer time (daylight saving time). To configure the software not to automatically switch to summer time, use the **no** form of this command.

Syntax

clock summer-time recurring {**usa** | **eu** | {*week day month hh:mm week day month hh:mm*}} [**offset** *offset*] [**zone** *acronym*]

clock summer-time date *date month year hh:mm date month year hh:mm* [**offset** *offset*] [**zone** *acronym*]

clock summer-time date *month date year hh:mm month date year hh:mm* [**offset** *offset*] [**zone** *acronym*]

no clock summer-time recurring

Parameters

- **recurring** — Indicates that summer time should start and end on the corresponding specified days every year.
- **date** — Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
- **usa** — The summer time rules are the United States rules.
- **eu** — The summer time rules are the European Union rules.
- *week* — Week of the month. (Range: 1 - 5, **first**, **last**)
- *day* — Day of the week (Range: first three letters by name, like **sun**)
- *date* — Date of the month. (Range:1 - 31)

- *month* — Month. (Range: first three letters by name, like Jan)
- *year* — year - no abbreviation (Range: 2000 - 2097)
- *hh:mm* — Time in military format, in hours and minutes. (Range: hh: 0 - 23, mm:0 - 59)
- *offset* — Number of minutes to add during summer time. (Range: 1 - 1440)
- *acronym* — The acronym of the time zone to be displayed when summer time is in effect. (Range: Up to 4 characters)

Default Setting

Summer time is disabled.

offset — Default is 60 minutes.

acronym — If unspecified default to the timezone acronym.

If the timezone has not been defined, the default is UTC.

Command Mode

Global Configuration mode

Command Usage

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rule for daylight savings time:

- Start: First Sunday in April
- End: Last Sunday in October
- Time: 2 am local time

EU rule for daylight savings time:

- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00)

Example

The following example sets summer time starting on the first Sunday in April at 2 am and finishing on the last Sunday in October at 2 am.

```
Console(config)# clock summer-time recurring first sun apr 2:00 last sun
oct 2:00
```

Related Commands

clock set

clock source

clock timezone

sntp authentication-key

The **sntp authentication-key** Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the **no** form of this command.

Syntax

sntp authentication-key *number* **md5** *value*

no sntp authentication-key *number*

Parameters

- *number* — Key number (Range: 1-4294967295)
- *value* — Key value (Range: 1-8 characters)

Default Setting

No authentication key is defined.

Command Mode

Global Configuration mode

Command Usage

Multiple keys can be generated.

Examples

The following example defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
```

Related Commands

sntp authenticate

sntp trusted-key

sntp client poll timer

sntp broadcast client enable

sntp anycast client enable

sntp unicast client enable

sntp unicast client poll

sntp authenticate

The **sntp authenticate** Global Configuration mode command grants authentication for received Simple Network Time Protocol (SNTP) traffic from servers. To disable the feature, use the **no** form of this command.

Syntax

sntp authenticate

no sntp authenticate

Default Setting

No authentication

Command Mode

Global Configuration mode

Command Usage

The command is relevant for both unicast and broadcast.

Examples

The following example defines the authentication key for SNTP and grants authentication.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

Related Commands

sntp authentication-key

sntp trusted-key

sntp client poll timer

sntp broadcast client enable

sntp anycast client enable

sntp unicast client enable

sntp unicast client poll

sntp trusted-key

The **sntp trusted-key** Global Configuration mode command authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. To disable authentication of the identity of the system, use the **no** form of this command.

Syntax

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

Parameters

- *key-number* — Key number of authentication key to be trusted. (Range: 1 - 4294967295)

Default Setting

No keys are trusted.

Command Mode

Global Configuration mode

Command Usage

The command is relevant for both received unicast and broadcast.

If there is at least 1 trusted key, then unauthenticated messages will be ignored.

Examples

The following example authenticates key 8.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

Related Commands

sntp authentication-key

sntp authenticate

sntp client poll timer

sntp broadcast client enable

sntp anycast client enable

sntp unicast client enable

sntp unicast client poll

sntp client poll timer

The **sntp client poll timer** Global Configuration mode command sets the polling time for the Simple Network Time Protocol (SNTP) client. To return to default configuration, use the **no** form of this command.

Syntax

sntp client poll timer *seconds*

no sntp client poll timer

Parameters

- *seconds* — Polling interval in seconds (Range: 60-86400)

Default Setting

Polling interval is 1024 seconds.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example sets the polling time for the Simple Network Time Protocol (SNTP) client to 120 seconds.

```
Console(config)# sntp client poll timer 120
```

Related Commands

sntp authentication-key

sntp authenticate

sntp trusted-key

sntp broadcast client enable

sntp anycast client enable

sntp unicast client enable

sntp unicast client poll

sntp broadcast client enable

The **sntp broadcast client enable** Global Configuration mode command enables Simple Network Time Protocol (SNTP) broadcast clients. To disable SNTP broadcast clients, use the **no** form of this command.

Syntax

sntp broadcast client enable

no sntp broadcast client enable

Default Setting

The SNTP broadcast client is disabled.

Command Mode

Global Configuration mode

Command Usage

Use the **sntp client enable (Interface)** Interface Configuration mode command to enable the SNTP client on a specific interface.

Examples

The following example enables the SNTP broadcast clients.

```
Console(config)# sntp broadcast client enable
```

Related Commands

sntp authentication-key

sntp authenticate

sntp trusted-key

sntp client poll timer

sntp anycast client enable

sntp unicast client enable

sntp unicast client poll

sntp anycast client enable

The **sntp anycast client enable** Global Configuration mode command enables SNTP anycast client. To disable the SNTP anycast client, use the **no** form of this command.

Syntax

sntp anycast client enable

no sntp anycast client enable

Default Setting

The SNTP anycast client is disabled.

Command Mode

Global Configuration mode

Command Usage

Use the **sntp client enable (Interface)** Interface Configuration mode command to enable the SNTP client on a specific interface.

Example

The following example enables SNTP anycast clients.

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

Related Commands

sntp authentication-key

sntp authenticate

sntp trusted-key

sntp client poll timer

sntp broadcast client enable

sntp unicast client enable

sntp unicast client poll

sntp client enable (Interface)

The **sntp client enable** Interface Configuration (Ethernet, port-channel, VLAN) mode command enables the Simple Network Time Protocol (SNTP) client on an interface. This applies to both receive broadcast and anycast updates. To disable the SNTP client, use the **no** form of this command.

Syntax

sntp client enable

no sntp client enable

Default Setting

The SNTP client is disabled on an interface.

Command Mode

Interface configuration (Ethernet, port-channel, VLAN) mode

Command Usage

Use the **sntp broadcast client enable** Global Configuration mode command to enable broadcast clients globally.

Use the **sntp anycast client enable** Global Configuration mode command to enable anycast clients globally.

Examples

The following example enables the SNTP client on Ethernet port 1/e3.

```
Console(config)# interface ethernet 1/e3
Console(config-if)# sntp client enable
```

Related Commands

sntp broadcast client enable

sntp unicast client enable

The **sntp unicast client enable** Global Configuration mode command enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers. To disable requesting and accepting SNTP traffic from servers, use the **no** form of this command.

Syntax

sntp unicast client enable

no sntp unicast client enable

Default Setting

The SNTP unicast client is disabled.

Command Mode

Global Configuration mode

Command Usage

Use the **sntp server** Global Configuration mode command to define SNTP servers.

Example

The following example enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers.

```
Console(config)# sntp unicast client enable
```

Related Commands

sntp authentication-key

sntp authenticate

sntp trusted-key

sntp client poll timer

sntp broadcast client enable

sntp anycast client enable

sntp unicast client poll

sntp unicast client poll

The **sntp unicast client poll** Global Configuration mode command enables polling for the Simple Network Time Protocol (SNTP) predefined unicast servers. To disable the polling for SNTP client, use the **no** form of this command.

Syntax

sntp unicast client poll

no sntp unicast client poll

Default Setting

Polling is disabled.

Command Mode

Global Configuration mode

Command Usage

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

Examples

The following example enables polling for Simple Network Time Protocol (SNTP) predefined unicast clients.

```
Console(config)# sntp unicast client poll
```

Related Commands

sntp authentication-key

sntp authenticate

sntp trusted-key

sntp client poll timer

sntp broadcast client enable

sntp anycast client enable

sntp unicast client enable

sntp server

The **sntp server** Global Configuration mode command configures the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from a specified server. To remove a server from the list of SNTP servers, use the **no** form of this command.

Syntax

sntp server {*ip-address* **|** *hostname*}[**poll**] [**key** *keyid*]

no sntp server *host*

Parameters

- *ip-address* — IP address of the server.
- *hostname* — Hostname of the server. (Range: 1-158 characters)
- **poll** — Enable polling.
- *keyid* — Authentication key to use when sending packets to this peer. (Range:1-4294967295)

Default Setting

No servers are defined.

Command Mode

Global Configuration mode

Command Usage

Up to 8 SNTP servers can be defined.

Use the **sntp unicast client enable** Global Configuration mode command to enable predefined unicast clients globally.

To enable polling you should also use the **sntp unicast client poll** Global Configuration mode command for global enabling.

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

Examples

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1.

```
Console(config)# sntp server 192.1.1.1
```

Related Commands

sntp anycast client enable

sntp unicast client enable

show clock

The **show clock** User EXEC mode command displays the time and date from the system clock.

Syntax

show clock [detail]

Parameters

- **detail** — Shows timezone and summertime configuration.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

The symbol that precedes the show clock display indicates the following:

Symbol	Description
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but SNTP is not synchronized.

Example

The following example displays the time and date from the system clock.

```
Console> show clock
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Console> show clock detail
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
```

Related Commands

clock set

clock source

clock timezone

clock summer-time

show sntp configuration

The **show sntp configuration** Privileged EXEC mode command shows the configuration of the Simple Network Time Protocol (SNTP).

Syntax

show sntp configuration

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the current SNTP configuration of the device.

```
Console# show sntp configuration


Polling interval: 7200 seconds


MD5 Authentication keys: 8, 9

Authentication is required for synchronization.

Trusted Keys: 8, 9


Unicast Clients: Enabled

Unicast Clients Polling: Enabled


Server                Polling           Encryption Key

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

176.1.1.8             Enabled           9

176.1.8.179           Disabled          Disabled
```

```
Broadcast Clients: Enabled

Anycast Clients: Enabled

Broadcast and Anycast Interfaces: 1/e1, 1/e3
```

Related Commands

sntp server

sntp authentication-key

sntp authenticate

sntp trusted-key

sntp client poll timer

sntp broadcast client enable

sntp anycast client enable

sntp client enable (Interface)

sntp unicast client enable

show sntp status

The **show sntp status** Privileged EXEC mode command shows the status of the Simple Network Time Protocol (SNTP).

Syntax

show sntp status

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example shows the status of the SNTP.

```
Console# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast

Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)


Unicast servers:
```

```
Server        Status     Last response                  Offset    Delay
                                                        [mSec]    [mSec]

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

176.1.1.8     Up         19:58:22.289 PDT Feb 19 2002   7.33      117.79

176.1.8.17    Unknown    12:17.17.987 PDT Feb 19 2002   8.98      189.19
9


Anycast server:

Server        Interfa    Sta    Last response           Offset    Delay
              ce         tus

                                                        [mSec]    [mSec]

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

176.1.11.8    VLAN       Up     9:53:21.789 PDT Feb 19  7.19      119.89
              118               2002


Broadcast:

Interface     Interfa           Last response
              ce

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

176.9.1.1     VLAN              19:17:59.792 PDT Feb 19 2002
              119
```

Related Commands

sntp server

sntp authentication-key

sntp authenticate

sntp trusted-key

sntp client poll timer

sntp broadcast client enable

sntp anycast client enable

sntp client enable (Interface)

sntp unicast client enable

Configuration and Image File Commands

Table 4-12. Configuration and Image File Commands

Command	Function	Mode	Page
copy	Copies files from a source to a destination.	PE	4-365
delete	Deletes a file from a flash memory device.	PE	4-368
dir	Displays the list of files on a flash file system	PE	4-369
more	Displays a file.	PE	4-370
rename	Renames the file.	PE	4-371
boot system	Specifies the system image that the device loads at startup.	PE	4-372
show running-config	Displays the contents of the currently running configuration file.	PE	4-373
show startup-config	Displays the contents of the startup configuration file.	PE	4-373
show startup-config	Displays the active system image file that is loaded by the device at startup.	PE	4-374

copy

The **copy** Privileged EXEC mode command copies files from a source to a destination.

Syntax

copy *source-url destination-url*

Parameters

- *source-url* — The source file location URL or reserved keyword of the source file to be copied. (Range: 1-160 characters)
- *destination-url* — The destination file URL or reserved keyword of the destination file. (Range: 1-160 characters)

  The following table displays keywords and URL prefixes:

Keyword	Source or Destination
flash:	Source or destination URL for flash memory. It's the default in case a URL is specified without a prefix.
running-config	Represents the current running configuration file.
startup-config	Represents the startup configuration file.
image	If the source file, represents the active image file. If the destination file, represents the non-active image file.
boot	Boot file.
tftp://	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:**//*host/[directory]/filename*. The host can be represented by its IP address or hostname.

xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
unit://*member*/**image**	Image file on one of the units. To copy from the master to all units, specify * in the member field.
unit://*member*/**boot**	Boot file on one of the units. To copy from the master to all units, specify * in the member field.
null:	Null destination for copies or files. A remote file can be copied to null to determine its size.
backup-config	Represents the backup configuration file.This is a user-defined name for up to four backup configuration files.
unit://*member*/**backup-config**	Backup configuration on one of the units.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

Up to five backup configuration files are supported on the device.

The location of a file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

*.prv and *.sys files cannot be copied.

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy if one of the following conditions exist:

The source file and destination file are the same file.

xmodem: is the destination file. The source file can be copied to **image**, **boot** and **null:** only.

tftp:// is the source file and destination file on the same copy.

The following table describes copy characters:

Character	Description

!	For network transfers, indicates that the copy process is taking place. Each exclamation point indicates successful transfer of ten packets (512 bytes each).
.	For network transfers, indicates that the copy process timed out. Generally, many periods in a row means that the copy process may fail.

Copying an Image File from a Server to Flash Memory

To copy an image file from a server to flash memory, use the **copy** *source-url* **image** command.

Copying a Boot File from a Server to Flash Memory

To copy a boot file from a server to flash memory, enter the **copy** *source-url* **boot** command.

Copying a Configuration File from a Server to the Running Configuration File

To load a configuration file from a network server to the running configuration file of the device, enter the **copy** *source-url* **running-config** command. The commands in the loaded configuration file are added to those in the running configuration file as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file is a combination of the previous running configuration and the loaded configuration files with the loaded configuration file taking precedence.

Copying a Configuration File from a Server to the Startup Configuration

To copy a configuration file from a network server to the startup configuration file of the device, enter **copy** *source-url* **startup-config**. The startup configuration file is replaced by the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy running-config** *destination-url* command to copy the current configuration file to a network server using TFTP. Use the **copy startup-config** *destination-url* command to copy the startup configuration file to a network server.

Saving the Running Configuration to the Startup Configuration

To copy the running configuration to the startup configuration file, enter the **copy running-config startup-config** command.

Backing up the Running or Startup Configuration to a Backup Configuration File

To copy the running configuration file to a backup configuration file, enter the **copy running-config file** command. To copy the startup configuration file to a backup configuration file, enter the **copy startup-config file** command.

Before copying from the backup configuration file to the running configuration file, make sure that the backup configuration file has not been corrupted.

Example

The following example copies system image file1 from the TFTP server 172.16.101.101 to a
non-active image file.

```
Console# copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

Related Commands

delete

show running-config

show startup-config

delete

The **delete** Privileged EXEC mode command deletes a file from a flash memory device.

Syntax

delete *url*

Parameters

- *url* — The location URL or reserved keyword of the file to be deleted. (Range: 1-160 characters)

The following table displays keywords and URL prefixes:

Keyword	Source or Destination
flash:	Source or destination URL for flash memory. It’s the default in case a URL is specified without a prefix.
startup-config	Represents the startup configuration file.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

*.sys, *.prv, image-1 and image-2 files cannot be deleted.

Examples

The following example deletes file **test** from flash memory.

```
Console# delete flash:test
Delete flash:test? [confirm]
```

Related Commands

copy

show running-config

show startup-config

dir

The **dir** Privileged EXEC mode command displays the list of files on a flash file system.

Syntax

dir

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the list of files on a flash file system.

```
Console# dir

Directory of
flash:

File Name      Permission. DataSize  FlashSize Modified

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

bb             rw          97        500000    13-Feb-2005
                                               10:30:21

cc             rw          97        500000    13-Feb-2005
                                               10:30:35

dd             rw          97        500000    13-Feb-2005
                                               10:30:50
```

```
ee              rw          97         500000    13-Feb-2005
                                                 10:31:04

image-1         rw          --         5767168   07-Feb-2005
                                                 10:15:56

image-2         rw          --         5767168   07-Feb-2005
                                                 10:15:56

aaafile.prv     --          --         262144    07-Feb-2005
                                                 10:16:02

syslog1.sys     r-          --         262144    07-Feb-2005
                                                 10:16:02

syslog2.sys     r-          --         262144    07-Feb-2005
                                                 10:16:02

directory.prv   --          --         262144    07-Feb-2005
                                                 10:15:56

startup-config rw           95         400000    13-Feb-2005
                                                 18:46:34


Total size of flash: 33292288 bytes

Free size of flash: 20708893 bytes
```

more

The **more** Privileged EXEC mode command displays a file.

Syntax

more *url*

Parameters

- *url* — The location URL or reserved keyword of the source file to be copied. (Range: 1-160 characters)

The following table displays keywords and URL prefixes:

Keyword	Source or Destination
flash:	Source or destination URL for flash memory. It’s the default in case a URL is specified without a prefix
running-config	Represents the current running configuration file.
startup-config	Represents the startup configuration file.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Files are displayed in ASCII format, except for the images, which are displayed in a hexadecimal format.

Note: *.prv files cannot be displayed.

Example

The following example displays the contents of the running configuration file.

.

```
Console# more configuration.bak
!
version 12.1
!
.
.
.
interface FastEthernet1/1
ip address 176.242.100.100 255.
ip pim dense-mode
duplex auto
speed auto
!
.
.
.
end
```

rename

The **rename** Privileged EXEC mode command renames the file.

Syntax

rename *url new-url*

Parameters

- *url* — The location URL. (Range: 1-160 characters)
- *new-url* — New URL. (Range: 1-160 characters)

The following table displays keywords and URL prefixes:

Keyword	Source or Destination

flash:	Source or destination URL for flash memory. It’s the default in case a URL is specified without a prefix

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

*.sys and *.prv files cannot be renamed.

Example

The following example renames the configuration file.

```
Console# rename configuration.bak m-config.bak
```

boot system

The **boot system** Privileged EXEC mode command specifies the system image that the device loads at startup.

Syntax

boot system [**unit** *unit*] {**image-1** | **image-2**}

Parameters

- *unit* — Specifies the unit number.
- **image-1** — Specifies image 1 as the system startup image.
- **image-2** — Specifies image 2 as the system startup image.

Default Setting

If the unit number is unspecified, the default setting is the master unit number.

Command Mode

Privileged EXEC mode

Command Usage

Use the **show bootvar** command to find out which image is the active image.

Example

The following example loads system image 1 at device startup.

```
Console# boot system image-1
```

Related Commands

show bootvar

show running-config

The **show running-config** Privileged EXEC mode command displays the contents of the currently running configuration file.

Syntax

show running-config

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the contents of the running configuration file.

```
Console# show running-config
software version 1.1



hostname device



interface ethernet 1/e1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000



interface ethernet 1/e2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
```

Related Commands

copy

delete

show startup-config

show startup-config

The **show startup-config** Privileged EXEC mode command displays the contents of the startup configuration file.

Syntax

show startup-config

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the contents of the running configuration file.

```
Console# show startup-config
software version 1.1



hostname device



interface ethernet 1/e1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000



interface ethernet 1/e2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
```

Related Commands

copy

delete

show running-config

show bootvar

The **show bootvar** Privileged EXEC mode command displays the active system image file that is loaded by the device at startup.

Syntax

show bootvar [**unit** *unit*]

Parameters

- *unit* — Specifies the unit number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the active system image file that is loaded by the device at startup.

```
Console# show bootvar

Images currently available on the FLASH

image-1       active

image-2       not active (selected for next boot)


Unit          Active Image       Selected for next boot

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

1             image-1            image-2

2             image-1            image-1
```

Related Commands

boot system

Ethernet Configuration Commands

Table 4-13. Ethernet Configuration Commands

Command	Function	Mode	Page
interface ethernet	Enters the interface configuration mode to configure an Ethernet type interface.	GC	4-376
interface range ethernet	Configures multiple Ethernet type interfaces at the same time.	GC	4-377
shutdown	Disables an interface.	IC	4-378
description	Adds a description to an interface.	IC	4-379
speed	Configures the speed of a given Ethernet interface when not using auto-negotiation.	IC	4-380
duplex	Configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation.	ICE	4-381
negotiation	Enables auto-negotiation operation for the speed and duplex parameters of a given interface.	IC	4-382
flowcontrol	Configures flow control on a given interface.	IC	4-383
mdix	Enables cable crossover on a given interface.	ICE	4-383
back-pressure	Enables back pressure on a given interface.	IC	4-384
clear counters	Clears statistics on an interface.	UE	4-385
set interface active	Reactivates an interface that was shutdown.	PE	4-386
show interfaces advertise	Displays autonegotiation data.	PE	4-386
show interfaces configuration	Displays the configuration for all configured interfaces.	PE	4-388
show interfaces status	Displays the status of all configured interfaces.	PE	4-390
show interfaces description	Displays the description for all configured interfaces.	PE	4-392
show interfaces counters	Displays traffic seen by the physical interface.	UE	4-392
port storm-control broadcast enable	Counts multicast packets in broadcast storm control.	ICE	4-395
port storm-control broadcast enable	Enables broadcast storm control.	ICE	4-395
port storm-control broadcast rate	Configures the maximum broadcast rate.	ICE	4-396
show ports storm-control	Displays the storm control configuration.	UE	4-397

interface ethernet

The **interface ethernet** Global Configuration mode command enters the interface configuration mode to configure an Ethernet type interface. The system supports up-to five IP addresses per device.

Syntax

interface ethernet *interface*

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables configuring Ethernet port 5/e18.

```
Console(config)# interface ethernet 5/e18
```

Related Commands

shutdown

description

speed

duplex

negotiation

flowcontrol

mdix

back-pressure

show interfaces status

interface range ethernet

The **interface range ethernet** Global Configuration mode command configures multiple Ethernet type interfaces at the same time.

Syntax

interface range ethernet {*port-range* | **all**}

Parameters

- *port-range* — List of valid ports. Where more than one port is listed, separate nonconsecutive ports with a comma and no spaces, use a hyphen to designate a range of ports and group a list separated by commas in brackets.
- **all** — All Ethernet ports.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

Example

The following example shows how ports 5/e18 to 5/e20 and 3/e1 to 3/24 are grouped to receive the same command.

```
Console(config)# interface range ethernet 5/e18-5/e20,3/e1-3/e24
Console(config-if)#
```

Related Commands

shutdown

description

speed

duplex

negotiation

flowcontrol

mdix

back-pressure

show interfaces status

shutdown

The **shutdown** Interface Configuration (Ethernet, port-channel) mode command disables an interface. To restart a disabled interface, use the **no** form of this command.

Syntax

shutdown

no shutdown

Default Setting

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example disables Ethernet port 1/e5 operations.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# shutdown
```

The following example restarts the disabled Ethernet port.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# no shutdown
```

Related Commands

speed

duplex

negotiation

flowcontrol

mdix

back-pressure

show interfaces configuration

show interfaces status

description

The **description** Interface Configuration (Ethernet, port-channel) mode command adds a description to an interface. To remove the description, use the **no** form of this command.

Syntax

description *string*

no description

Parameters

- *string* — Comment or a description of the port to enable the user to remember what is attached to the port. (Range: 1-64 characters)

Default Setting

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example adds a description to Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# description "RD SW#3"
```

Related Commands

show interfaces description

speed

The **speed** Interface Configuration (Ethernet, port-channel) mode command configures the speed of a given Ethernet interface when not using auto-negotiation. To restore the default configuration, use the **no** form of this command.

Syntax

speed {**10** | **100** | **1000**}

no speed

Parameters

- **10** — Forces10 Mbps operation.
- **100** — Forces 100 Mbps operation.
- **1000** — Forces 1000 Mbps operation.

Default Setting

Maximum port capability

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

The **no speed** command in a port-channel context returns each port in the port-channel to its maximum capability.

Example

The following example configures the speed operation of Ethernet port 1/e5 to 100 Mbps operation.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# speed 100
```

Related Commands

shutdown

duplex

negotiation

flowcontrol

mdix

back-pressure

show interfaces configuration

show interfaces status

duplex

The **duplex** Interface Configuration (Ethernet) mode command configures the full/ half duplex operation of a given Ethernet interface when not using auto-negotiation. To restore the default configuration, use the **no** form of this command.

Syntax

duplex {**half** | **full**}

Parameters

- **no duplex**
- **half** — Forces half-duplex operation
- **full** — Forces full-duplex operation

Default Setting

The interface is set to full duplex.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

When configuring a particular duplex mode on the port operating at 10/100 Mbps, disable the auto-negotiation on that port.

Half duplex mode can be set only for ports operating at 10 Mbps or 100 Mbps.

Example

The following example configures the duplex operation of Ethernet port 1/e5 to full duplex operation.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# duplex full
```

Related Commands

shutdown

speed

negotiation

flowcontrol

mdix

back-pressure

show interfaces configuration

show interfaces status

negotiation

The **negotiation** Interface Configuration (Ethernet, port-channel) mode command enables auto-negotiation operation for the speed and duplex parameters of a given interface. To disable auto-negotiation, use the **no** form of this command.

Syntax

negotiation *[capability1 [capability2…capability5]]*

no negotiation

Parameters

- *capability* — Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h,100f, 1000f)

Default Setting

Auto-negotiation is enabled.

If unspecified, the default setting is to enable all capabilities of the port.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

If capabilities were specified when auto-negotiation was previously entered, not specifying capabilities when currently entering auto-negotiation overrides the previous configuration and enables all capabilities.

Example

The following example enables auto-negotiation on Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# negotiation
```

Related Commands

shutdown

speed

duplex

flowcontrol

mdix

back-pressure

show interfaces advertise

show interfaces configuration

show interfaces status

flowcontrol

The **flowcontrol** Interface Configuration (Ethernet, port-channel) mode command configures flow control on a given interface. To disable flow control, use the **no** form of this command.

Syntax

flowcontrol {**auto | on** | **off**}

no flowcontrol

Parameters

- **auto** — Indicates auto-negotiation
- **on** — Enables flow control.
- **off** — Disables flow control.

Default Setting

Flow control is off.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

Negotiation should be enabled for **flow control auto**.

Flow control can be configured only in full duplex mode.

Example

In the following example, flow control is enabled on port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# flowcontrol on
```

Related Commands

shutdown

speed

duplex

negotiation

mdix

back-pressure

show interfaces configuration

show interfaces status

mdix

The **mdix** Interface Configuration (Ethernet) mode command enables cable crossover on a given interface. To disable cable crossover, use the **no** form of this command.

Syntax

mdix {on | auto}

no mdix

Parameters

- **on** — Manual mdix
- **auto** — Automatic mdi/mdix

Default Setting

The default is **on**.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

Auto: All possibilities to connect a PC with cross or normal cables are supported and are automatically detected.

On: It is possible to connect to a PC only with a normal cable and to connect to another device only with a cross cable.

No: It is possible to connect to a PC only with a cross cable and to connect to another device only with a normal cable.

Example

In the following example, automatic crossover is enabled on port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# mdix auto
```

Related Commands

shutdown

speed

duplex

negotiation

flowcontrol

back-pressure

show interfaces configuration

show interfaces status

back-pressure

The **back-pressure** Interface Configuration (Ethernet) mode command enables back pressure on a given interface. To disable back pressure, use the **no** form of this command.

Syntax

back-pressure

no back-pressure

Default Setting

Back pressure is enabled.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

The back pressure Interface Configuration mode command enables back pressure on half duplex mode only, therefore it can not be configured on a channel port.

Example

In the following example back pressure is enabled on port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# back-pressure
```

Related Commands

shutdown

speed

duplex

negotiation

flowcontrol

mdix

show interfaces configuration

show interfaces status

clear counters

The **clear counters** User EXEC mode command clears statistics on an interface.

Syntax

clear counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

In the following example, the counters for interface 1/e1 are cleared.

```
Console> clear counters ethernet 1/e1
```

Related Commands

shutdown

set interface active

The **set interface active** Privileged EXEC mode command reactivates an interface that was shutdown.

Syntax

set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

This command is used to activate interfaces that were configured to be active, but were shutdown by the system for some reason (e.g., **port security)**.

Example

The following example reactivates interface 1/e5.

```
Console# set interface active ethernet 1/e5
```

Related Commands

show interfaces status

show interfaces advertise

The **show interfaces advertise** Privileged EXEC mode command displays autonegotiation data.

Syntax

show interfaces advertise [ethernet *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Modes

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Examples

The following examples display autonegotiation information.

```
Console# show interfaces advertise


Port     Type            Neg          Operational Link Advertisement
----     -----------     -------      ------------------------------
e1       100M-Copper     Enabled      --
e2       100M-Copper     Enabled      --
e3       100M-Copper     Enabled      --
e4       100M-Copper     Enabled      --
e5       100M-Copper     Enabled      100f, 100h, 10f, 10h
e6       100M-Copper     Enabled      --
e7       100M-Copper     Enabled      --
e8       100M-Copper     Enabled      --
e9       100M-Copper     Enabled      --
e10      100M-Copper     Enabled      --
e11      100M-Copper     Enabled      --
e12      100M-Copper     Enabled      --
e13      100M-Copper     Enabled      --
e14      100M-Copper     Enabled      --
e15      100M-Copper     Enabled      --
```

```
e16      100M-Copper      Enabled      --

e17      100M-Copper      Enabled      --

e18      100M-Copper      Enabled      --

e19      100M-Copper      Enabled      --

e20      100M-Copper      Enabled      --
```

Related Commands

negotiation

show interfaces configuration

The **show interfaces configuration** Privileged EXEC mode command displays the configuration for all configured interfaces.

Syntax

show interfaces configuration [ethernet *interface* | **port-channel** *port-channel-number* | *interface*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Modes

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the configuration of all configured interfaces:

```
Console# show interfaces configuration



Por   Type          Duple   Spee   Neg       Fl    Lin   Back       Mdix
t                   x       d                ow    k     Pressur    Mode
                                             Ct    Sta   e
                                             rl    te

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

e1    100M-Coppe    Full    100    Enable    Of    Up    Disable    Auto
      r                            d         f           d

e2    100M-Coppe    Full    100    Enable    Of    Up    Disable    Auto
      r                            d         f           d
```

e3	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e4	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e5	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e6	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e7	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e8	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e9	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e10	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e11	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e12	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e13	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e14	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e15	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e16	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e17	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e18	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto
e19	100M-Copper	Full	100	Enabled	Off	Up	Disabled	Auto

Related Commands

shutdown

speed

duplex

negotiation

flowcontrol

mdix

back-pressure

show interfaces status

show interfaces status

The **show interfaces status** Privileged EXEC mode command displays the status of all configured interfaces.

Syntax

show interfaces status [ethernet *interface*| **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the status of all configured interfaces:

```
Console# show interfaces status


Por   Type          Duple   Spee   Neg      Fl    Link   Back      Mdix
t                   x       d               ow    Stat   Pressur   Mode
                                            Ct    e      e
                                            rl

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

e1    100M-Coppe    --      --     --       --    Down   --        --
      r

e2    100M-Coppe    --      --     --       --    Down   --        --
      r

e3    100M-Coppe    --      --     --       --    Down   --        --
      r

e4    100M-Coppe    --      --     --       --    Down   --        --
      r

e5    100M-Coppe    Full    100    Enable   Of    Up     Disable   Auto
      r                            d        f            d
```

```
e6    100M-Coppe   --       --     --       --    Down   --        --
      r

e7    100M-Coppe   --       --     --       --    Down   --        --
      r

e8    100M-Coppe   --       --     --       --    Down   --        --
      r

e9    100M-Coppe   --       --     --       --    Down   --        --
      r

e10   100M-Coppe   --       --     --       --    Down   --        --
      r

e11   100M-Coppe   --       --     --       --    Down   --        --
      r

e12   100M-Coppe   --       --     --       --    Down   --        --
      r

e13   100M-Coppe   --       --     --       --    Down   --        --
      r

e14   100M-Coppe   --       --     --       --    Down   --        --
      r

e15   100M-Coppe   --       --     --       --    Down   --        --
      r

e16   100M-Coppe   --       --     --       --    Down   --        --
      r

e17   100M-Coppe   --       --     --       --    Down   --        --
      r

e18   100M-Coppe   --       --     --       --    Down   --        --
      r

e19   100M-Coppe   --       --     --       --    Down   --        --
      r
```

Related Commands

shutdown

speed

duplex

negotiation

flowcontrol

mdix

back-pressure

show interfaces configuration

show interfaces description

The **show interfaces description** Privileged EXEC mode command displays the description for all configured interfaces.

Syntax

show interfaces description [ethernet *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays descriptions of configured interfaces.

```
Console# show interfaces description


Port        Description
----        -----------
1/e1        lab
1/e2
1/e3
1/e4
1/e5
1/e6
ch1
ch2
```

Related Commands

description

show interfaces counters

The **show interfaces counters** User EXEC mode command displays traffic seen by the physical interface.

Syntax

show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays traffic seen by the physical interface:

```
Console# show interfaces counters


Port     InOctets         InUcastPkts       InMcastPkts      InBcastPkts
----     --------         -----------       -----------      -----------
1/e1     183892           0                 0                0
2/e1     0                0                 0                0
3/e1     123899           0                 0                0

Port     OutOctets        OutUcastPkts      OutMcastPkts     OutBcastPkts
-----    ----------       ------------      ------------     ------------
1/e1     9188             0                 0                0
2/e1     0                0                 0                0
3/e1     8789             0                 0                0

Ch       InOctets         InUcastPkts       InMcastPkts      InBcastPkts
---      --------         ----------        -----------      -----------
1        27889            0                 0                0
```

```
Ch      OutOctets       OutUcastPkts      OutMcastPkts     OutBcastPkts
---     ---------       ------------      ------------     ------------
1       23739           0                 0                0
```

The following example displays counters for Ethernet port 1/e1.

```
Console# show interfaces counters ethernet 1/e1


Port     InOctets       InUcastPkts       InMcastPkts       InBcastPkts
-----    -----------    --------------    -----------       -----------
-
1/e1     183892         0                 0                 0


Port     OutOctets      OutUcastPkts      OutMcastPkts      OutBcastPkts
-----    -----------    --------------    ------------      ------------
-
1/e1     9188           0                 0                 0


FCS Errors: 8
Single Collision Frames: 0
Late Collisions: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display:

Field	Description
InOctets	Counted received octets.
InUcastPkts	Counted received unicast packets.
InMcastPkts	Counted received multicast packets.
InBcastPkts	Counted received broadcast packets.
OutOctets	Counted transmitted octets.
OutUcastPkts	Counted transmitted unicast packets.
OutMcastPkts	Counted transmitted multicast packets.
OutBcastPkts	Counted transmitted broadcast packets.
FCS Errors	Counted received frames that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Counted frames that are involved in a single collision, and are subsequently transmitted successfully.
Late Collisions	Number of times that a collision is detected later than one slotTime into the transmission of a packet.
Oversize Packets	Counted frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Counted frames for which reception fails due to an internal MAC sublayer receive error.
Received Pause Frames	Counted MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

Related Commands

clear counters

port storm-control broadcast enable

The **port storm-control broadcast enable** Interface Configuration (Ethernet) mode command enables broadcast storm control. To disable broadcast storm control, use the **no** form of this command.

Syntax

port storm-control broadcast enable

no port storm-control broadcast enable

Default Setting

Broadcast storm control is disabled.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

Use the **port storm-control broadcast rate** Interface Configuration (Ethernet) mode command, to set the maximum allowable broadcast rate.

Example

The following example enables broadcast storm control on port 1/g1 of a device.

```
Console(config)# interface ethernet 1/g1
Console(config)# port storm-control broadcast enable
```

Related Commands

port storm-control broadcast enable

port storm-control broadcast rate

show ports storm-control

port storm-control broadcast rate

The **port storm-control broadcast rate** Interface Configuration (Ethernet) mode command configures the maximum broadcast rate. To return to the default configuration, use the **no** form of this command.

Syntax

port storm-control broadcast rate *rate*

no port storm-control broadcast rate

Parameters

- *rate* — Maximum kilobits per second of broadcast and multicast traffic on a port.

Default Setting

The default value is 3500 Kbits/Sec.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

Use the **port storm-control broadcast enable** Interface Configuration mode command to enable broadcast storm control.

Example

The following example configures the maximum storm control broadcast rate at 900 Kbits/Sec on Ethernet
port 1/e5 of a device.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# port storm-control broadcast rate 900
```

Related Commands

port storm-control broadcast enable

show ports storm-control

show ports storm-control

The **show ports storm-control** User/Privileged EXEC mode command displays the storm control configuration.

Syntax

show ports storm-control [*interface*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the storm control configuration .

```
Console# show ports storm-control

Port       State       Rate [Kbits/    Included
                       Sec]

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

1/e1       Enabled     70              Broadcast, Multicast, Unknown
                                       Unicast

2/e1       Enabled     100             Broadcast

3/e1       Disabled    100             Broadcast
```

The following example displays the storm control configuration.

```
Console# show ports storm-control

Unknown traffic limited to 1000
Kbits/sec

Port       Broadcast and Multicast Storm Control [Kbits/Sec]

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

1/g1       8000
```

```
2/g1       Disabled

3/g1       Disabled
```

Related Commands

port storm-control broadcast enable

port storm-control broadcast rate

GVRP Commands

Table 4-14. GVRP Commands			
Command	Function	Mode	Page
gvrp enable (Global)	Enables GVRP globally. To disable GVRP on the device, use the **no** form of this command.	GC	4-399
gvrp enable (Interface)	Enables GVRP on an interface. To disable GVRP on an interface, use the **no** form of this command.	IC	4-400
garp timer	Adjusts the values of the join, leave and leaveall timers of GARP applications. To return to the default configuration, use the **no** form of this command.	IC	4-401
gvrp vlan-creation-forbid	Disables dynamic VLAN creation or modification. To enable dynamic VLAN creation or modification, use the **no** form of this command.t	IC	4-402
gvrp registration-forbid	Deregisters all dynamic VLANs on a port and prevents VLAN creation or registration on the port. To allow dynamic registration of VLANs on a port, use the **no** form of this command.	LC	4-402
clear gvrp statistics	Clears all GVRP statistical information.	PE	4-403
show gvrp configuration	Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.	UE	4-404
show gvrp statistics	Displays GVRP statistics.	UE	4-405
show gvrp error-statistics	Displays GVRP error statistics.	LC	4-406

gvrp enable (Global)

GARP VLAN Registration Protocol (GVRP) is an industry-standard protocol designed to propagate VLAN information from device to device. With GVRP, a single device is manually configured with all desired VLANs for the network, and all other devices on the network learn these VLANs dynamically.

The **gvrp enable** Global Configuration mode command enables GVRP globally. To disable GVRP on the device, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Setting

GVRP is globally disabled.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables GVRP globally on the device.

```
Console(config)# gvrp enable
```

Related Commands

gvrp enable (Interface)

gvrp enable (Interface)

The **gvrp enable** Interface Configuration (Ethernet, port-channel) mode command enables GVRP on an interface. To disable GVRP on an interface, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Setting

GVRP is disabled on all interfaces.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

An access port does not dynamically join a VLAN because it is always a member in only one VLAN.

Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID is manually defined as the untagged VLAN VID.

Example

The following example enables GVRP on Ethernet port 1/e6.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# gvrp enable
```

Related Commands

gvrp enable (Global)

garp timer

gvrp vlan-creation-forbid

gvrp registration-forbid

show gvrp configuration

garp timer

The **garp timer** Interface Configuration (Ethernet, Port channel) mode command adjusts the values of the join, leave and leaveall timers of GARP applications. To return to the default configuration, use the **no** form of this command.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*

no garp timer

Parameters

- {**join** | **leave** | **leaveall**} — Indicates the type of timer.
- *timer_value* — Timer values in milliseconds in multiples of 10. (Range: 10-2147483640)

Default Setting

Following are the default timer values:

- Join timer — 200 milliseconds
- Leave timer — 600 milliseconds
- Leavall timer — 10000 milliseconds

Command Mode

Interface configuration (Ethernet, port-channel) mode

Command Usage

The timer_value value must be a multiple of 10. You must maintain the following relationship for the various timer values:

- Leave time must be greater than or equal to three times the join time.
- 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, the GARP application will not operate successfully.

Example

The following example sets the leave timer for Ethernet port 1/e6 to 900 milliseconds.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# garp timer leave 900
```

Related Commands

gvrp enable (Interface)

gvrp vlan-creation-forbid

gvrp registration-forbid

show gvrp configuration

gvrp vlan-creation-forbid

The **gvrp vlan-creation-forbid** Interface Configuration (Ethernet, port-channel) mode command disables dynamic VLAN creation or modification. To enable dynamic VLAN creation or modification, use the **no** form of this command.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Default Setting

Dynamic VLAN creation or modification is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

This command forbids dynamic VLAN creation from the interface. The creation or modification of dynamic VLAN registration entries as a result of the GVRP exchanges on an interface are restricted only to those VLANs for which static VLAN registration exists.

Example

The following example disables dynamic VLAN creation on Ethernet port 1/e6.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# gvrp vlan-creation-forbid
```

Related Commands

gvrp enable (Interface)

garp timer

gvrp registration-forbid

show gvrp configuration

gvrp registration-forbid

The **gvrp registration-forbid** Interface Configuration (Ethernet, port-channel) mode command deregisters all dynamic VLANs on a port and prevents VLAN creation or registration on the port. To allow dynamic registration of VLANs on a port, use the **no** form of this command.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Default Setting

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example forbids dynamic registration of VLANs on Ethernet port 1/e6.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# gvrp registration-forbid
```

Related Commands

gvrp enable (Interface)

garp timer

gvrp vlan-creation-forbid

show gvrp configuration

clear gvrp statistics

The **clear gvrp statistics** Privileged EXEC mode command clears all GVRP statistical information.

Syntax

clear gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example clears all GVRP statistical information on Ethernet port 1/e6.

```
Console# clear gvrp statistics ethernet 1/e6
```

Related Commands

show gvrp statistics

show gvrp error-statistics

show gvrp configuration

The **show gvrp configuration** User EXEC mode command displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

Syntax

show gvrp configuration [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays GVRP configuration information:

```
Console> show gvrp configuration


GVRP Feature is currently enabled on the device.


                                                Timers (milliseconds)

Port(s   Status     Registration   Dynamic      Join   Leave    Leave All
)                                  VLAN
                                   Creation
```

```
------    -------    ------------    ---------    ----    -----    ---------
2/e1      Enabled    Normal          Enabled      200     600      10000
4/e4      Enabled    Normal          Enabled      200     600      10000
```

Related Commands

gvrp enable (Interface)

garp timer

gvrp vlan-creation-forbid

clear gvrp statistics

show gvrp statistics

The **show gvrp statistics** User EXEC mode command displays GVRP statistics.

Syntax

show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example shows GVRP statistical information:

```
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
```

Related Commands

clear gvrp statistics

show gvrp error-statistics

show gvrp error-statistics

The **show gvrp error-statistics** User EXEC mode command displays GVRP error statistics.

Syntax

show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays GVRP statistical information.

```
Console> show gvrp error-statistics

GVRP Error Statistics:

Legend:

INVPROT:    Invalid Protocol Id       INVALEN :     Invalid Attribute
                                                    Length

INVATYP:    Invalid Attribute         INVEVENT:     Invalid Event
            Type

INVAVAL:    Invalid Attribute
            Value

 Port  INVPROT INVATYP INVAVAL INVALEN INVEVENT
```

Related Commands

clear gvrp statistics

show gvrp statistics

IGMP Snooping Commands

Table 4-15. IGMP Snooping Commands

Command	Function	Mode	Page
ip igmp snooping (Global)	Enables Internet Group Management Protocol (IGMP) snooping. To disable IGMP snooping, use the **no** form of this command.	GC	4-408
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN. To disable IGMP snooping on a VLAN interface, use the **no** form of this command.	ICV	4-409
ip igmp snooping host-time-out	Configures the host-time-out. If an IGMP report for a multicast group was not received for a host-time-out period from a specific port, this port is deleted from the member list of that multicast group. To return to the default configuration, use the **no** form of this command.	ICV	4-410
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out. The **ip igmp snooping mrouter-time-out** Interface Configuration (VLAN) mode command is used for setting the aging-out time after multicast device ports are automatically learned. To return to the default configuration, use the **no** form of this command.	ICV	4-410
ip igmp snooping leave-time-out	Configures the leave-time-out. If an IGMP report for a multicast group was not received for a leave-time-out period after an IGMP Leave was received from a specific port, this port is deleted from the member list of that multicast group. To return to the default configuration, use the **no** form of this command.	ICV	4-411
ip igmp snooping multicast-tv	Defines the multicast ip-addresses that are associated with a multicast-tv VLAN	GC	4-412
ip igmp snooping querier enable	Displays information on dynamically learned multicast device interfaces.	UE	4-413
ip igmp snooping querier enable	Use the ip igmp snooping querier enable interface configuration command to enable Internet Group Management Protocol (IGMP) querier on a specific VLAN.	ICV	4-413
ip igmp snooping querier address	Use the ip igmp snooping querier address interface configuration command to define the source IP address that the IGMP Snooping querier would use.	ICV	4-413
ip igmp snooping querier version	Use the ip igmp snooping querier version interface configuration command to configure the IGMP version of an IGMP querier on a specific VLAN.	ICV	4-414
show ip igmp snooping interface	Sets the number of data bits per character that are interpreted and generated by hardware	UE	4-415
show ip igmp snooping groups	Displays multicast groups learned by IGMP snooping.	UE	4-416

ip igmp snooping (Global)

The **ip igmp snooping** Global Configuration mode command enables Internet Group Management Protocol (IGMP) snooping. To disable IGMP snooping, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Setting

IGMP snooping is disabled.

Command Mode

Global Configuration mode

Command Usage

IGMP snooping can only be enabled on static VLANs. It must not be enabled on Private VLANs or their community VLANs.

Example

The following example enables IGMP snooping.

```
Console(config)# ip igmp snooping
```

Related Commands

ip igmp snooping querier enable

ip igmp snooping (Interface)

The **ip igmp snooping** Interface Configuration (VLAN) mode command enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN. To disable IGMP snooping on a VLAN interface, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Setting

IGMP snooping is disabled.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

IGMP snooping can only be enabled on static VLANs. It must not be enabled on Private VLANs or their community VLANs.

Example

The following example enables IGMP snooping on VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping
```

Related Commands

ip igmp snooping querier enable

show ip igmp snooping groups

ip igmp snooping host-time-out

The **ip igmp snooping host-time-out** Interface Configuration (VLAN) mode command configures the host-time-out. If an IGMP report for a multicast group was not received for a host-time-out period from a specific port, this port is deleted from the member list of that multicast group. To return to the default configuration, use the **no** form of this command.

Syntax

ip igmp snooping host-time-out *time-out*

Parameters

- **no ip igmp snooping host-time-out**
- *time-out* — Host timeout in seconds. (Range: 60 - 2147483647)

Default Setting

The default host-time-out is 260 seconds.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

The timeout should be at least greater than 2*query_interval+max_response_time of the IGMP router.

IGMP snooping works on PVE protected ports; however forwarding of query/reports is not limited to the PVE uplink.

Example

The following example configures the host timeout to 300 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping host-time-out 300
```

Related Commands

ip igmp snooping querier enable

ip igmp snooping mrouter-time-out

The **ip igmp snooping mrouter-time-out** Interface Configuration (VLAN) mode command configures the mrouter-time-out. The **ip igmp snooping mrouter-time-out** Interface Configuration (VLAN) mode command is used for setting the aging-out time after multicast device ports are automatically learned. To return to the default configuration, use the **no** form of this command.

Syntax

ip igmp snooping mrouter-time-out *time-out*

no ip igmp snooping mrouter-time-out

Parameters

- *time-out* — Multicast device timeout in seconds (Range: 1 - 2147483647)

Default Setting

The default value is 300 seconds.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the multicast device timeout to 200 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping mrouter-time-out 200
```

Related Commands

ip igmp snooping querier enable

ip igmp snooping leave-time-out

The **ip igmp snooping leave-time-out** Interface Configuration (VLAN) mode command configures the leave-time-out. If an IGMP report for a multicast group was not received for a leave-time-out period after an IGMP Leave was received from a specific port, this port is deleted from the member list of that multicast group. To return to the default configuration, use the **no** form of this command.

Syntax

ip igmp snooping leave-time-out {*time-out* | **immediate-leave**}

no ip igmp snooping leave-time-out

Parameters

- *time-out* — Specifies the leave-time-out in seconds for IGMP queries. (Range: 0-2147483647)
- **immediate-leave** — Indicates that the port should be immediately removed from the members list after receiving IGMP Leave.

Default Setting

The default leave-time-out configuration is 10 seconds.

Command Mode

Interface Configuration (VLAN) mode

Command Usage

The leave timeout should be set greater than the maximum time that a host is allowed to respond to an IGMP query.

Use **immediate leave** only where there is just one host connected to a port.

Example

The following example configures the host leave-time-out to 60 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping leave-time-out 60
```

Related Commands

ip igmp snooping querier enable

ip igmp snooping multicast-tv

The **ip igmp snooping multicast-tv** Global Configuration mode command defines the multicast ip-addresses that are associated with a multicast-tv VLAN. Use the **no** form of this command to remove all associations.

Syntax

ip igmp snooping multicast-tv vlan *vlan-id* {**add** | **remove**} *ip-multicast-address* [**count** *number*]

no ip igmp snooping multicast-tv vlan *vlan-id*

Parameters

- **multicast-tv vlan** *vlan-id* — Specifies the Multicast VLAN ID.
- *ip-multicast-address* — Specifies the multicast IP address.
- *number* — Configure multiple contiguous multicast IP addresses. If unspecified, the default is 1. (Range: 1-256)

Default Configuration

The default configuration has no multicast IP address associated with it.

Command Mode

Global Configuration mode

User Guidelines

Use this command to define the multicast transmissions on a multicast-tv VLAN. The configuration is only relevant for an access port, which is a member in the configured VLAN as a multicast-tv VLAN. If an IGMP message is received on such an access port, it would be associated with the multicast-tv VLAN provided that one of the multicast IP addresses are associated with the multicast-tv VLAN.

Bridge multicast filtering should be enabled prior to configuring this command.

ip igmp snooping querier enable

The **ip igmp snooping querier enable** Interface Configuration (VLAN) mode command enables the Internet Group Management Protocol (IGMP) querier on a specific VLAN. Use the **no** form of this command to disable IGMP querier on a VLAN interface.

Syntax

ip igmp snooping querier enable

no ip igmp snooping querier enable

Default Configuration

The ip igmp snooping querier enable is disabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

IGMP snooping querier can be enabled on a VLAN only if IGMP snooping is enabled for that VLAN.

No more than one switch can be configured as an IGMP Querier for a VLAN.

When IGMP Snooping Querier is enabled, it starts after host-time-out/2 with no IGMP traffic detected from a multicast router.

The IGMP Snooping Querier would disable itself if it detects IGMP traffic from a multicast router. It would restart itself after host-time-out/2.

Following are the IGMP Snooping Querier parameters as function of the IGMP Snooping parameters:

- QueryMaxResponseTime: host-time-out/15.
- QueryInterval: host-time-out/ 3.

ip igmp snooping querier address

The **ip igmp snooping querier address** Interface Configuration (VLAN) mode command defines the source IP address, which the IGMP Snooping querier would use. Use the **no** form of this command to return to default.

Syntax

ip igmp snooping querier address *ip-address*

no ip igmp snooping querier address

Parameters

- *ip-address* — Source IP address

Default Configuration

If an IP address is configured for the VLAN, it would be used as the source address of the IGMP Snooping querier.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If an IP address is not configured by this command, and no IP address is configured for the IGMP querier VLAN interface, the querier would be disabled.

ip igmp snooping querier version

The **ip igmp snooping querier version** Interface Configuration (VLAN) mode command configures the IGMP version of an IGMP querier on a specific VLAN. Use the **no** form of this command to return to default.

Syntax

ip igmp snooping querier version {2 | 3}

no ip igmp snooping querier version

Parameters

- **2** — Specify that the IGMP version would be IGMPv2.
- **3** — Specify that the IGMP version would be IGMPv3.

Default Configuration

The default value is IGMPv3.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If the IGMP querier is configured to IGMPv3, the querier would try to work in IGMPv3. In case the hosts do not support IGMPv3, the querier version would be downgraded.

If the IGMP querier is configured to IGMPv2, the querier would attempt to work in IGMPv2. It can be downgraded automatically to IGMPv1, but cannot be upgraded automatically to IGMPv3.

show ip igmp snooping mrouter

The **show ip igmp snooping mrouter** User EXEC mode command displays information on dynamically learned multicast device interfaces.

Syntax

show ip igmp snooping mrouter [**interface** *vlan-id*]

Parameters

- *vlan-id* — VLAN number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays multicast device interfaces in VLAN 1000.

```
Console> show ip igmp snooping mrouter interface 1000


VLAN            Ports
----            -----
1000            1/e1


Detected multicast devices that are forbidden statically:
VLAN            Ports
----            -----
1000            1/e19
```

Related Commands

ip igmp snooping (Global)

ip igmp snooping (Interface)

ip igmp snooping mrouter-time-out

ip igmp snooping leave-time-out

show ip igmp snooping interface

The **show ip igmp snooping interface** User EXEC mode command displays IGMP snooping configuration.

Syntax

show ip igmp snooping interface *vlan-id*

Parameters

- *vlan-id* — VLAN number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays IGMP snooping information on VLAN 1000.

```
Console> show ip igmp snooping interface

IGMP Snooping is globally enabled

IGMP Snooping admin: Enabled
Hosts and routers IGMP version: 2
IGMP snooping oper mode: Enabled
IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin: default
IGMP snooping querier address oper: 172.16.1.1
IGMP snooping querier version: 3

IGMP host timeout is 300 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 300 sec
Automatic learning of multicast router ports is enabled
```

Related Commands

ip igmp snooping (Global)

ip igmp snooping (Interface)

ip igmp snooping mrouter-time-out

ip igmp snooping leave-time-out

show ip igmp snooping groups

The **show ip igmp snooping groups** User EXEC mode command displays multicast groups learned by IGMP snooping.

Syntax

show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*] [**source** *ip-address*]

Parameters

- *vlan-id* — VLAN number.
- *ip-multicast-address* — IP multicast address.
- *ip-address* — Source IP address.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

To see the full multicast address table (including static addresses) use the **show bridge multicast address-table** Privileged EXEC command.

Example

The following example shows IGMP snooping information on multicast groups.

```
Console> show ip igmp snooping groups

Vlan    Group address              Source        Include     Exlude Ports
                                   address       Ports
----    -----------------          -------       -------
                                                 ---
1       231.2.2.3                  172.16.1.1    1/1
1       231.2.2.3                  172.16.1.2    2/2
19      231.2.2.8                  172.16.1.1    1/9
19      231.2.2.8                  172.16.1.2    1/10-11     1/12
19      231.2.2.8                  172.16.1.3                1/12
IGMP Reporters that are forbidden statically:
---------------------------------------------
Vlan    Group Address              Source        Ports
                                   address
1       231.2.2.3                  172.16.1.1    2/8
19      231.2.2.8                  172.16.1.1    2/8
```

Related Commands

ip igmp snooping (Interface)

IP Addressing Commands

Table 4-16. IP Addressing Commands

Command	Function	Mode	Page
ip address	Sets an IP address. To remove an IP address, use the **no** form of this command.	IC	4-418
ip address dhcp	Acquires an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure an acquired IP address, use the **no** form of this command.	IC	4-419
ip default-gateway	Defines a default gateway (device). To return to the default configuration, use the no form of this command.	GC	4-420
show ip interface	Sets the interval that the system waits for a login attempt	PE	4-421
arp	Adds a permanent entry in the Address Resolution Protocol (ARP) cache. To remove an entry from the ARP cache, use the **no** form of this command.	GC	4-422
arp timeout	Configures how long an entry remains in the ARP cache. To return to the default configuration, use the **no** form of this command.	GC	4-423
clear arp-cache	Deletes all dynamic entries from the ARP cache.	PE	4-424
show arp	Displays entries in the ARP table.	PE	4-424
ip domain-lookup	Enables the IP Domain Naming System (DNS)-based host name-to-address translation. To disable DNS-based host name-to-address translation, use the **no** form of this command.	GC	4-425
ip domain-name	Defines a default domain name used by the software to complete unqualified host names (names without a dotted-decimal domain name). To remove the default domain name, use the **no** form of this command.	GC	4-426
ip name-server	Defines the available name servers. To remove a name server, use the **no** form of this command.	GC	4-426
ip host	Defines static host name-to-address mapping in the host cache. To remove the name-to-address mapping, use the **no** form of this command.	GC	4-427
clear host	Deletes entries from the host name-to-address cache.	PE	4-428
clear host dhcp	Deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).	PE	4-429
show hosts	Displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses.	PE	4-429

ip address

The **ip address** Interface Configuration (Ethernet, VLAN, port-channel) mode command sets an IP address. To remove an IP address, use the **no** form of this command.

Syntax

ip address *ip-address* {*mask* | *prefix-length*}

no ip address [*ip-address*]

Parameters

- *ip-address* —Valid IP address
- *mask* — Valid network mask of the IP address.
- *prefix-length* — Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8 -30)

Default Setting

No IP address is defined for interfaces.

Command Mode

Interface Configuration (Ethernet, VLAN, port-channel) mode

Command Usage

An IP address cannot be configured for a range of interfaces (range context).

Example

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27 255.255.255.0
```

Related Commands

ip default-gateway

ip address dhcp

ip address dhcp

The **ip address dhcp** Interface Configuration (Ethernet, VLAN, port-channel) mode command acquires an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure an acquired IP address, use the **no** form of this command.

Syntax

ip address dhcp [**hostname** *host-name*]

no ip address dhcp

Parameters

- *host-name* — Specifies the name of the host to be placed in the DHCP option 12 field. This name does not have to be the same as the host name specified in the **hostname** Global Configuration mode command. (Range: 1-20 characters)

Default Setting

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, VLAN, port-channel) mode

Command Usage

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.

Some DHCP servers require that the DHCPDISCOVER message have a specific host name. The **ip address dhcp hostname** *host-name* command is most typically used when the host name is provided by the system administrator.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If the **ip address dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the specified DHCP host name is the globally configured host name of the device. However, the **ip address dhcp hostname** *host-name* command can be used to place a different host name in the DHCP option 12 field.

The **no ip address dhcp** command deconfigures any IP address that was acquired, thus sending a DHCPRELEASE message.

Example

The following example acquires an IP address for Ethernet port 1/e16 from DHCP.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# ip address dhcp
```

Related Commands

ip address

ip default-gateway

ip default-gateway

The **ip default-gateway** Global Configuration mode command defines a default gateway (device). To return to the default configuration, use the no form of this command.

Syntax

ip default-gateway *ip-address*

no ip default-gateway

Parameters

- *ip-address* — Valid IP address of the default gateway.

Default Setting

No default gateway is defined.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example defines default gateway 192.168.1.1.

```
Console(config)# ip default-gateway 192.168.1.1
```

Related Commands

ip address

ip address dhcp

show ip interface

The **show ip interface** Privileged EXEC mode command displays the usability status of configured IP interfaces.

Syntax

show ip interface [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel number*]

Parameters

- *interface-number* — Valid Ethernet port.
- *vlan-id* — Valid VLAN number.
- *port-channel number* — Valid Port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example the displays the configured IP interfaces and their types.

```
Console# show ip interface
```

```
Gateway IP Address      Type                Activity status
------------------      ------              ---------------
10.7.1.1                Static              Active



IP address              Interface           Type
-------------           ---------           -------
10.7.1.192/24           VLAN 1              Static
10.7.2.192/24           VLAN 2              DHCP
```

Related Commands

ip address

ip address dhcp

arp

The **arp** Global Configuration mode command adds a permanent entry in the Address Resolution Protocol (ARP) cache. To remove an entry from the ARP cache, use the **no** form of this command.

Syntax

arp *ip_addr hw_addr* {**ethernet** i*nterface-number* | **vlan** *vlan-id* | **port-channel** *port-channel number*}

no arp *ip_addr* {**ethernet** i*nterface-number* | **vlan** *vlan-id* | **port-channel** *port-channel number*}

Parameters

- *ip_addr* — Valid IP address or IP alias to map to the specified MAC address.
- *hw_addr* — Valid MAC address to map to the specified IP address or IP alias.
- *interface-number* — Valid Ethernet port.
- *vlan-id* — Valid VLAN number**.**
- *port-channel number.* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, static ARP cache entries do not generally have to be specified.

Example

The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
Console(config)# arp 198.133.219.232 00:00:0c:40:0f:bc ethernet 1/e6
```

Related Commands

arp timeout

show arp

arp timeout

The **arp timeout** Global Configuration mode command configures how long an entry remains in the ARP cache. To return to the default configuration, use the **no** form of this command.

Syntax

arp timeout *seconds*

no arp timeout

Parameters

- *seconds* — Time (in seconds) that an entry remains in the ARP cache. (Range: 1 - 40000000)

Default Setting

The default timeout is 60000 seconds.

Command Mode

Global Configuration mode

Command Usage

It is recommended not to set the timeout value to less than 3600.

Example

The following example configures the ARP timeout to 12000 seconds.

```
Console(config)# arp timeout 12000
```

Related Commands

arp

show arp

clear arp-cache

The **clear arp-cache** Privileged EXEC mode command deletes all dynamic entries from the ARP cache.

Syntax

clear arp-cache

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

Related Commands

arp

arp timeout

show arp

The **show arp** Privileged EXEC mode command displays entries in the ARP table.

Syntax

show arp [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**ethernet** *interface* **| port-channel** *port-channel-number*]

Parameters

- *ip-address* — Displays the ARP entry of a specific IP address.
- *mac-address* — Displays the ARP entry of a specific MAC address.
- *interface* — Displays the ARP entry of a specific Ethernet port interface.
- *port-channel-number* — Displays the ARP entry of a specific Port-channel number interface.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays entries in the ARP table.

```
Console# show arp

ARP timeout: 80000 Seconds


Interface      IP address       HW address          Status

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

1/e1           10.7.1.102       00:10:B5:04:DB:4B   Dynamic

2/e2           10.7.1.135       00:50:22:00:2A:A4   Static
```

Related Commands

arp

arp timeout

ip domain-lookup

The **ip domain-lookup** Global Configuration mode command enables the IP Domain Naming System (DNS)-based host name-to-address translation. To disable DNS-based host name-to-address translation, use the **no** form of this command.

Syntax

ip domain-lookup

no ip domain-lookup

Default Setting

IP Domain Naming System (DNS)-based host name-to-address translation is enabled.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables IP Domain Naming System (DNS)-based host name-to-address translation.

```
Console(config)# ip domain-lookup
```

Related Commands

ip domain-name

ip name-server

ip host

show hosts

ip domain-name

The **ip domain-name** Global Configuration mode command defines a default domain name used by the software to complete unqualified host names (names without a dotted-decimal domain name). To remove the default domain name, use the **no** form of this command.

Syntax

ip domain-name *name*

no ip domain-name

Parameters

- *name* — Specifies the default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1-158 characters)

Default Setting

A default domain name is not defined.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example defines default domain name www.Alcatel.com.

```
Console(config)# ip domain-name www.Alcatel.com
```

Related Commands

ip domain-lookup

ip name-server

ip host

show hosts

ip name-server

The **ip name-server** Global Configuration mode command defines the available name servers. To remove a name server, use the **no** form of this command.

Syntax

ip name-server *server-address* [*server-address2 … server-address8*]

no ip name-server [*server-address1 … server-address8*]

Parameters

- *server-address* — Specifies IP addresses of the name server.

Default Setting

No name server addresses are specified.

Command Mode

Global Configuration mode

Command Usage

The preference of the servers is determined by the order in which they were entered.

Up to 8 servers can be defined using one command or using multiple commands.

Example

The following example sets the available name server.

```
Console(config)# ip name-server 176.16.1.18
```

Related Commands

ip domain-lookup

ip domain-name

ip host

show hosts

ip host

The **ip host** Global Configuration mode command defines static host name-to-address mapping in the host cache. To remove the name-to-address mapping, use the **no** form of this command.

Syntax

ip host *name address*

no ip host *name*

Parameters

- *name* — Name of the host (Range: 1-158 characters)
- *address* — Associated IP address.

Default Setting

No host is defined.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example defines a static host name-to-address mapping in the host cache.

```
Console(config)# ip host accounting.Alcatel.com 176.10.23.1
```

Related Commands

ip domain-lookup

ip domain-name

ip name-server

clear host

show hosts

clear host

The **clear host** Privileged EXEC mode command deletes entries from the host name-to-address cache.

Syntax

clear host {*name* | *****}

Parameters

- *name* — Specifies the host entry to be removed.
  (Range: 1-158 characters)
- ***** — Removes all entries.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example deletes all entries from the host name-to-address cache.

```
Console# clear host *
```

Related Commands

ip host

clear host dhcp

The **clear host dhcp** Privileged EXEC mode command deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).

Syntax

clear host dhcp {*name* | *****}

Parameters

- *name* — Specifies the host entry to be removed.
  (Range: 1-158 characters)
- ***** — Removes all entries.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

This command deletes the host name-to-address mapping temporarily until the next renewal of the IP address.

Example

The following example deletes all entries from the host name-to-address mapping.

```
Console# clear host dhcp *
```

Related Commands

ip host

show hosts

The **show hosts** Privileged EXEC mode command displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses.

Syntax

show hosts [*name*]

Parameters

- *name* — Specifies the host name. (Range: 1-158 characters)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays host information.

```
Console# show hosts
Host name: Device
Default domain is gm.com, sales.gm.com, usa.sales.gm.com(DHCP)
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19

Configured host name-to-address mapping:
Host                                      Addresses
----                                      ---------
accounting.gm.com                         176.16.8.8 176.16.8.9 (DHCP)

Cache:               TTL(Hours)
Host                 Total    Elapsed     Type    Addresses
----                 -----    -------     -----   ---------
                                          -
www.stanford.edu     72       3           IP      171.64.14.203
```

Related Commands

ip domain-lookup

ip domain-name

ip name-server

ip host

LACP Commands

Table 4-17. LACP Commands

Command	Function	Mode	Page
lacp system-priority	Configures the system priority. To return to the default configuration, use the **no** form of this command.	GC	4-431
lacp port-priority	Configures physical port priority. To return to the default configuration, use the **no** form of this command.	ICE	4-432
lacp timeout	Assigns an administrative LACP timeout. To return to the default configuration, use the **no** form of this command.	ICE	4-432
show lacp ethernet	Displays LACP information for Ethernet ports.	PE	4-433
show lacp port-channel	Displays LACP information for a port-channel.	PE	4-435

lacp system-priority

The **lacp system-priority** Global Configuration mode command configures the system priority. To return to the default configuration, use the **no** form of this command.

Syntax

lacp system-priority *value*

no lacp system-priority

Parameters

- *value* — Specifies system priority value. (Range: 1 - 65535)

Default Setting

The default system priority is 1.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the system priority to 120.

```
Console(config)# lacp system-priority 120
```

Related Commands

show lacp port-channel

lacp port-priority

The **lacp port-priority** Interface Configuration (Ethernet) mode command configures physical port priority. To return to the default configuration, use the **no** form of this command.

Syntax

lacp port-priority *value*

no lacp port-priority

Parameters

- *value* — Specifies port priority. (Range: 1 - 65535)

Default Setting

The default port priority is 1.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following example defines the priority of Ethernet port 1/e6 as 247.

```
Console(config)# interface ethernet 1/e6
Console(config-if)# lacp port-priority 247
```

Related Commands

lacp timeout

show lacp ethernet

show lacp port-channel

lacp timeout

The **lacp timeout** Interface Configuration (Ethernet) mode command assigns an administrative LACP timeout. To return to the default configuration, use the **no** form of this command.

Syntax

lacp timeout {**long | short**}

no lacp timeout

Parameters

- **long** — Specifies the long timeout value.
- **short** — Specifies the short timeout value.

Default Setting

The default port timeout value is **long**.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following example assigns a long administrative LACP timeout to Ethernet port 1/e6 .

```
Console(config)# interface ethernet 1/e6
Console(config-if)# lacp timeout long
```

Related Commands

lacp port-priority

show lacp ethernet

show lacp port-channel

show lacp ethernet

The **show lacp ethernet** Privileged EXEC mode command displays LACP information for Ethernet ports.

Syntax

show lacp ethernet *interface* [**parameters** | **statistics** | **protocol-state**]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- **parameters** — Link aggregation parameter information.
- **statistics** — Link aggregation statistics information.
- **protocol-state** — Link aggregation protocol-state information.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example display LACP information for Ethernet port 1/e1.

```
Console# show lacp ethernet 1/e1


Port 1/e1 LACP parameters:

       Actor
```

```
                     system priority:            1
                     system mac addr:            00:00:12:34:56:78
                     port Admin key:             30
                     port Oper key:              30
                     port Oper number:           21
                     port Admin priority:        1
                     port Oper priority:         1
                     port Admin timeout:         LONG
                     port Oper timeout:          LONG
                     LACP Activity:              ACTIVE
                     Aggregation:                AGGREGATABLE
                     synchronization:            FALSE
                     collecting:                 FALSE
                     distributing:               FALSE
                     expired:                    FALSE
       Partner
                     system priority:            0
                     system mac addr:            00:00:00:00:00:00
                     port Admin key:             0
                     port Oper key:              0
                     port Oper number:           0
                     port Admin priority:        0
                     port Oper priority:         0
                     port Oper timeout:          LONG
                     LACP Activity:              PASSIVE
                     Aggregation:                AGGREGATABLE
                     synchronization:            FALSE
                     collecting:                 FALSE
                     distributing:               FALSE
                     expired:                    FALSE

Port 1/e1 LACP Statistics:
LACP PDUs sent:                                  2
LACP PDUs received:                              2

Port 1/e1 LACP Protocol State:
    LACP State Machines:
              Receive FSM:               Port Disabled State
              Mux FSM:                   Detached State
              Periodic Tx FSM:           No Periodic State
    Control Variables:
              BEGIN:                     FALSE
              LACP_Enabled:              TRUE
              Ready_N:                   FALSE
              Selected:                  UNSELECTED
              Port_moved:                FALSE
              NNT:                       FALSE
              Port_enabled:              FALSE
    Timer counters:
              periodic tx timer:         0
              current while timer:       0
              wait while timer:          0
```

Related Commands

lacp port-priority

lacp timeout

show lacp port-channel

show lacp port-channel

The **show lacp port-channel** Privileged EXEC mode command displays LACP information for a port-channel.

Syntax

show lacp port-channel [*port_channel_number*]

Parameters

- *port_channel_number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays LACP information about port-channel 1.

```
Console# show lacp port-channel 1
Port-Channel 1: Port Type 1000 Ethernet
        Actor
                   System Priority:            1
                   MAC Address:                 00:02:85:0E:1C:00
                   Admin Key:                   29
                   Oper Key:                    29

         Partner
                   System Priority:            0
                   MAC Address:                 00:00:00:00:00:00
                   Oper Key:                    14
```

Related Commands

lacp system-priority

lacp port-priority

lacp timeout

show lacp ethernet

Line Commands

Table 4-18. Line Commands

Command	Function	Mode	Page
line	Identifies a specific line for configuration and enters the Line Configuration command mode.	GC	4-437
speed	Sets the line baud rate. To return to the default configuration, use the **no** form of the command.	LC	4-438
autobaud	Sets the line for automatic baud rate detection (autobaud). To disable automatic baud rate detection, use the **no** form of the command.	LC	4-439
exec-timeout	Sets the interval that the system waits until user input is detected. To return to the default configuration, use the **no** form of this command.	LC	4-439
history	Enables the command history function. To disable the command history function, use the **no** form of this command.	LC	4-440
history size	Configures the command history buffer size for a particular line. To reset the command history buffer size to the default configuration, use the **no** form of this command.	LC	4-440
terminal history	Enables the command history function for the current terminal session. To disable the command history function, use the **no** form of this command.	UE	4-441
terminal history size	Configures the command history buffer size for the current terminal session. To reset the command history buffer size to the default setting, use the **no** form of this command.	UE	4-442
show line	Displays line parameters.	UE	4-443

line

The **line** Global Configuration mode command identifies a specific line for configuration and enters the Line Configuration command mode.

Syntax

line {**console** | **telnet** | **ssh**}

Parameters

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the device as a virtual terminal for remote console access.

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

Related Commands

show line

speed

The **speed** Line Configuration mode command sets the line baud rate. To return to the default configuration, use the **no** form of the command.

Syntax

speed *bps*

no speed

Parameters

- *bps*—Baud rate in bits per second (bps). Possible values are 2400, 9600, 19200, 38400, 57600 and 115200.

Default Setting

The default speed is 9600 bps.

Command Mode

Line Configuration (console) mode

Command Usage

This command is available only on the line console.

The configured speed is applied when Autobaud is disabled. This configuration applies only to the current session.

Examples

The following example configures the line baud rate to 115200.

```
Console(config)# line console
Console(config-line)# speed 115200
```

Related Commands

show line

autobaud

The **autobaud** Line Configuration mode command sets the line for automatic baud rate detection (autobaud). To disable automatic baud rate detection, use the **no** form of the command.

Syntax

autobaud

no autobaud

Default Setting

Autobaud is disabled.

Command Mode

Line Configuration (console) mode

Command Usage

This command is available only on the line console.

To start communication using Autobaud , press **<Enter>** twice. This configuration applies only to the current session.

Example

The following example enables autobaud.

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

Related Commands

show line

exec-timeout

The **exec-timeout** Line Configuration mode command sets the interval that the system waits until user input is detected. To return to the default configuration, use the **no** form of this command.

Syntax

exec-timeout *minutes* [*seconds*]

no exec-timeout

Parameters

- *minutes* — Specifies the number of minutes. (Range: 0 - 65535)
- *seconds* — Specifies additional time intervals in seconds. (Range: 0 - 59)

Default Setting

The default configuration is 10 minutes.

Command Mode

Line Configuration mode

Command Usage

To specify no timeout, enter the **exec-timeout** 0 command.

Example

The following example configures the interval that the system waits until user input is detected to 20 minutes.

```
Console(config)# line console
Console(config-line)# exec-timeout 20
```

Related Commands

show line

history

The **history** Line Configuration mode command enables the command history function. To disable the command history function, use the **no** form of this command.

Syntax

history

no history

Default Setting

The command history function is enabled.

Command Mode

Line Configuration mode

Command Usage

This command enables the command history function for a specified line. To enable or disable the command history function for the current terminal session, use the **terminal history** user EXEC mode command.

Example

The following example enables the command history function for telnet.

```
Console(config)# line telnet
Console(config-line)# history
```

Related Commands

history size

show history

show line

history size

The **history size** Line Configuration mode command configures the command history buffer size for a particular line. To reset the command history buffer size to the default configuration, use the **no** form of this command.

Syntax

history size *number-of-commands*

no history size

Parameters

- *number-of-commands*—Number of commands that the system records in its history buffer. (Range: 10 - 147)

Default Setting

The default history buffer size is 10.

Command Mode

Line Configuration mode

Command Usage

This command configures the command history buffer size for a particular line. To configure the command history buffer size for the current terminal session, use the **terminal history size** User EXEC mode command.

Example

The following example changes the command history buffer size to 100 entries for a particular line.

```
Console(config-line)# history size 100
```

Related Commands

history

show history

show line

terminal history

The **terminal history** user EXEC command enables the command history function for the current terminal session. To disable the command history function, use the **no** form of this command.

Syntax

terminal history

terminal no history

Default Setting

The default configuration for all terminal sessions is defined by the **history** line configuration command.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example disables the command history function for the current terminal session.

```
Console# terminal no history
```

Related Commands

terminal history size

show line

terminal history size

The **terminal history size** user EXEC command configures the command history buffer size for the current terminal session. To reset the command history buffer size to the default setting, use the **no** form of this command..

Syntax

terminal history size *number-of-commands*

terminal no history size

Parameters

- *number-of-commands* — Specifies the number of commands the system may record in its command history buffer. The buffer size is dependent on device resources.

Default Setting

The command history buffer size has no default.

Command Mode

User EXEC mode

Command Usage

The **terminal history size** user EXEC command configures the size of the command history buffer for the current terminal session. To change the default size of the command history buffer, use the **history** line configuration command.

Example

The following example configures the command history buffer size to 20 commands for the current terminal session.

```
Console# terminal history size 20
```

Related Commands

show line

show line

The **show line** User EXEC mode command displays line parameters.

Syntax

show line [console | **telnet** | **ssh**]

Parameters

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Setting

If the line is not specified, the default value is console.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the line configuration.

```
Console> show line


Console configuration:

               Interactive timeout: Disabled

               History: 10

               Baudrate: 9600

               Databits: 8

               Parity: none

               Stopbits: 1


Telnet configuration:

               Interactive timeout: 10 minutes 10 seconds

               History: 10


SSH configuration:

               Interactive timeout: 10 minutes 10 seconds

               History: 10
```

Related Commands

line

speed

autobaud

exec-timeout

history

history size

terminal historyterminal history size

Management ACL Commands

Table 4-19. Management ACL Commands

Command	Function	Mode	Page
management access-list	Configures a management access list and enters the Management Access-list Configuration command mode. To delete an access list, use the **no** form of this command.	GC	4-445
permit (Management)	Defines a permit rule.	ACL	4-446
deny (Management)	Defines a deny rule.	ACL	4-447
management access-class	Restricts management connections by defining the active management access list. To disable this restriction, use the **no** form of this command.	GC	4-448
show management access-list	Sets the interval that the command interpreter waits until user input is detected	PE	4-449
show management access-class	Sets the password intrusion threshold, which limits the number of failed logon attempts	PE	4-450

management access-list

The **management access-list** Global Configuration mode command configures a management access list and enters the Management Access-list Configuration command mode. To delete an access list, use the **no** form of this command.

Syntax

management access-list *name*

no management access-list *name*

Parameters

- *name* — Access list name. (Range: 1-32 characters)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Use this command to configure a management access list. The command enters the Access-list Configuration mode, where permit and deny access rules are defined using the **permit (Management)** and **deny (Management)** commands.

If no match criteria are defined, the default is deny.

If you reenter an access list context, the new rules are entered at the end of the access list.

Use the **management access-class** command to select the active access list.

The active management list cannot be updated or removed.

Management ACL requires a valid management interface, which is a port, VLAN, or port-channnel with an IP address or console interface. Management ACL only restricts access to the device for management configuration or viewing.

Example

The following example creates a management access list called mlist, configures management Ethernet interfaces 1/e1 and 2/e9 and makes the new access list the active list.

```
Console(config)# management access-list mlist
Console(config-macl)# permit ethernet 1/e1
Console(config-macl)# permit ethernet 2/e9
Console(config-macl)# exit
Console(config)# management access-class mlist
```

The following example creates a management access list called mlist, configures all interfaces to be management interfaces except Ethernet interfaces 1/e1 and 2/e9 and makes the new access list the active list.

```
Console(config)# management access-list mlist
Console(config-macl)# deny ethernet 1/e1
Console(config-macl)# deny ethernet 2/e9
Console(config-macl)# permit
Console(config-macl)# exit
Console(config)# management access-class mlist
```

Related Commands

permit (Management)

deny (Management)

show management access-list

show management access-class

management access-class

permit (Management)

The **permit** Management Access-List Configuration mode command defines a permit rule.

Syntax

permit [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel-number*] [**service** *service*]

permit ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel-number* |] [**service** *service*]

Parameters

- *interface-number* — A valid Ethernet port number.
- *vlan-id* — A valid VLAN number.
- *port-channel-number* — A valid port channel index.
- *ip-address* — A valid source IP address.
- *mask* — A valid network mask of the source IP address.
- *prefix-length* — Number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0 - 32)
- *service* — Service type. Possible values: **telnet**, **ssh**, **http, https** and **snmp**.

Default Setting

If no permit rule is defined, the default is set to deny**.**

Command Mode

Management Access-list Configuration mode

Command Usage

Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

The system supports up to 128 management access rules.

Example

The following example permits all ports in the mlist access list.

```
Console(config)# management access-list mlist
Console(config-macl)# permit
```

Related Commands

management access-list

deny (Management)

show management access-list

deny (Management)

The **deny** Management Access-List Configuration mode command defines a deny rule.

Syntax

deny [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel-number*] [**service** *service*]

deny ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *port-channel-number* |] [**service** *service*]

Parameters

- *interface-number* — A valid Ethernet port number.
- *vlan-id* — A valid VLAN number.
- *port-channel-number* — A valid port-channel number.
- *ip-address* — A valid source IP address.
- *mask* — A valid network mask of the source IP address.
- **mask** *prefix-length* — Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)
- *service* — Service type. Possible values: **telnet**, **ssh**, **http, https** and **snmp**.

Default Setting

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

Command Usage

Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

The system supports up to 128 management access rules.

Example

The following example denies all ports in the access list called mlist.

```
Console(config)# management access-list mlist
Console(config-macl)# deny
```

Related Commands

management access-list

permit (Management)

show management access-list

management access-class

The **management access-class** Global Configuration mode command restricts management connections by defining the active management access list. To disable this restriction, use the **no** form of this command.

Syntax

management access-class {**console-only** | *name*}

no management access-class

Parameters

- **console-only** — Indicates that the device can be managed only from the console.
- *name* — Specifies the name of the access list to be used.

(Range: 1-32 characters)

If no access list is specified, an empty access list is used.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures an access list called mlist as the management access list.

```
Console(config)# management access-class mlist
```

Related Commands

management access-list

show management access-class

show management access-list

The **show management access-list** Privileged EXEC mode command displays management access-lists.

Syntax

show management access-list [*name*]

Parameters

- *name* — Specifies the name of a management access list. (Range: 1 - 32 characters)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the mlist management access list.

```
Console# show management access-list mlist

mlist

-----

        permit ethernet 1/e1
        permit ethernet 2/e2

! (Note: all other access implicitly denied)
```

Related Commands

management access-list

permit (Management)

deny (Management)

show management access-class

The **show management access-class** Privileged EXEC mode command displays the active management access list.

Syntax

show management access-class

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays information about the active management access list.

```
Console# show management access-class
Management access-class is enabled, using access list mlist
```

Related Commands

management access-class

management access-list

PHY Diagnostics Commands

Table 4-20. PHY Diagnostics Commands

Command	Function	Mode	Page
test copper-port tdr	Uses Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.	PE	4-376
show copper-ports tdr	Displays information on the last Time Domain Reflectometry (TDR) test performed on copper ports.	UE	4-452
show copper-ports cable-length	Displays the estimated copper cable length attached to a port.	UE	4-452
show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics.	PE	4-453

test copper-port tdr

The **test copper-port tdr** Privileged EXEC mode command uses Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.

Syntax

test copper-port tdr *interface*

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

The port to be tested should be shut down during the test, unless it is a combination port with fiber port active.

The maximum length of the cable for the TDR test is 120 meter.

Example

The following example results in a report on the cable attached to port 1/e3.

```
Console# test copper-port tdr 1/e3
Cable is open at 64 meters
Console# test copper-port tdr 2/e3
Can’t perform this test on fiber ports
```

Related Commands

show copper-ports tdr

show copper-ports cable-length

show copper-ports tdr

The **show copper-ports tdr** User EXEC mode command displays information on the last Time Domain Reflectometry (TDR) test performed on copper ports.

Syntax

show copper-ports tdr [*interface*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

The maximum length of the cable for the TDR test is 120 meter.

Example

The following example displays information on the last TDR test performed on all copper ports.

```
Console> show copper-ports tdr


Port     Result     Length [meters]     Date
----     ------     ---------------     ----
1/e1     OK
1/e2     Short      50                  13:32:00 23 July 2005
1/e3     Test has not been performed
1/e4     Open       64                  13:32:00 23 July 2005
1/e5     Fiber      -                   -
```

Related Commands

test copper-port tdr

show copper-ports cable-length

show copper-ports cable-length

The **show copper-ports cable-length** User EXEC mode command displays the estimated copper cable length attached to a port.

Syntax

show copper-ports cable-length [*interface*]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

The port must be active and working in 100M or 1000M mode.

Example

The following example displays the estimated copper cable length attached to all ports.

```
Console> show copper-ports cable-length


Port         Length [meters]

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

1/e1         < 50

1/e2         Copper not active

1/e3         110-140

1/g1         Fiber
```

Related Commands

test copper-port tdr

show copper-ports tdr

show fiber-ports optical-transceiver

The **show fiber-ports optical-transceiver** Privileged EXEC command displays the optical transceiver diagnostics.

Syntax

show fiber-ports optical-transceiver [*interface*] [**detailed**]

Parameters

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- **detailed** — Detailed diagnostics.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

To test optical transceivers, ensure a fiber link is present.

Examples

The following examples display the optical transceiver diagnostics.

```
Console# show fiber-ports optical-transceiver


                                           Power

Port    Temp      Voltage    Current    Output   Input    TX Fault    LOS

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

1/g1    W         OK         E          OK       OK       OK          OK

1/g2    OK        OK         OK         OK       OK       E           OK

1/g3    Copper


Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power.
Input Power – Measured RX  received power.
Tx Fault – Transmitter fault
LOS – Loss of signal
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

```
Console# show fiber-ports optical-transceiver detailed
                                        Power
Port    Temp      Voltag   Current   Output    Input     TX Fault    LOS
                  e
        [C]       [Volt]   [mA]      [mWatt]   [mWatt]

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

1/g1    48        5.15     50        1.789     1.789     No          No

1/g2    43        5.15     10        1.789     1.789     No          No

1/g3    Copper


Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power.
Input Power – Measured RX  received power.
Tx Fault – Transmitter fault
LOS – Loss of signal
```

Port Channel Commands

Table 4-21. Port Channel Commands

Command	Function	Mode	Page
interface port-channel	Enters the interface configuration mode to configure a specific port-channel.	GC	4-455
interface range port-channel	Enters the interface configuration mode to configure multiple port-channels.	GC	4-455
channel-group	Associates a port with a port-channel. To remove a port from a port-channel, use the **no** form of this command.	ICE	4-456
show interfaces port-channel	Displays port-channel information.	PE	4-457

interface port-channel

The **interface port-channel** Global Configuration mode command enters the interface configuration mode to configure a specific port-channel.

Syntax

interface port-channel *port-channel-number*

Parameters

- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Eight aggregated links can be defined with up to eight member ports per port-channel. The aggregated links' valid IDs are 1-8.

Example

The following example enters the context of port-channel number 1.

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

Related Commands

show interfaces port-channel

interface range port-channel

The **interface range port-channel** Global Configuration mode command enters the interface configuration mode to configure multiple port-channels.

Syntax

interface range port-channel {*port-channel-range* | **all**}

Parameters

- *port-channel-range* — List of valid port-channels to add. Separate nonconsecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels.
- **all** — All valid port-channels.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Commands under the interface range context are executed independently on each interface in the range.

Example

The following example groups port-channels 1, 2 and 6 to receive the same command.

```
Console(config)# interface range port-channel 1-2,6
```

Related Commands

show interfaces port-channel

channel-group

The **channel-group** Interface Configuration (Ethernet) mode command associates a port with a port-channel. To remove a port from a port-channel, use the **no** form of this command.

Syntax

channel-group *port-channel-number* **mode** {**on** | **auto**}

no channel-group

Parameters

- *port-channel_number* — Specifies the number of the valid port-channel for the current port to join.
- **on** — Forces the port to join a channel without an LACP operation.
- **auto** — Allows the port to join a channel as a result of an LACP operation.

Default Setting

The port is not assigned to a port-channel.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following example forces port 1/e1 to join port-channel 1 without an LACP operation.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# channel-group 1 mode on
```

Related Commands

show interfaces port-channel

show interfaces port-channel

The **show interfaces port-channel** Privileged EXEC mode command displays port-channel information.

Syntax

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

Parameters

- *port-channel-number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays information on all port-channels.

```
Console# show interfaces port-channel


Channel                    Ports

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

1                          Active: 1/e1, 2/e2

2                          Active: 2/e2, 2/e7 Inactive: 3/e1

3                          Active: 3/e3, 3/e8
```

Related Commands

channel-group

Port Monitor Commands

Table 4-22. Port Monitor Commands

Command	Function	Mode	Page
port monitor	Starts a port monitoring session. To stop a port monitoring session, use the **no** form of this command.	ICE	4-458
show ports monitor	Displays the port monitoring status.	UE	4-459

port monitor

The **port monitor** Interface Configuration mode command starts a port monitoring session. To stop a port monitoring session, use the **no** form of this command.

Syntax

port monitor *src-interface* **[rx | tx]**

no port monitor *src-interface*

Parameters

- *src-interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- **rx —** Monitors received packets only.
- **tx —** Monitors transmitted packets only.

Default Setting

Monitors both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

This command enables traffic on one port to be copied to another port, or between the source port (src-interface) and a destination port (port being configured).

The following restrictions apply to ports configured as destination ports:

- The port cannot be already configured as a source port.
- The port cannot be a member in a port-channel.
- An IP interface is not configured on the port.
- GVRP is not enabled on the port.
- The port is not a member of a VLAN, except for the default VLAN (will automatically be removed from the default VLAN).
- The following restrictions apply to ports configured to be source ports:
- The port cannot be already configured as a destination port.

Example

The following example copies traffic on port 1/e8 (source port) to port 1/e1 (destination port).

```
Console(config)# interface ethernet 1/e1
Console(config-if)# port monitor 1/e8
```

Related Commands

show ports monitor

show ports monitor

show ports monitor

The **show ports monitor** User EXEC mode command displays the port monitoring status.

Syntax

show ports monitor

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example shows how the port monitoring status is displayed.

```
Console# show ports monitor

Source Port      Destination Port     Type     Status     VLAN Tagging

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

1/e1             1/e8                 RX,TX    Active     No

1/e2             1/e8                 RX,TX    Active     No

1/e18            1/e8                 RX       Active     No
```

Related Commands

port monitor

show ports monitor

Power over Ethernet Commands

Table 4-23. Power over Ethernet Commands

Command	Function	Mode	Page
power inline	Configures the administrative mode of inline power on an interface.	ICE	4-376
power inline powered-device	Adds a comment or description of the powered device type to enable the user to remember what is attached to the interface. To remove the description, use the **no** form of this command.	ICE	4-459
power inline priority	Configures the inline power management priority of the interface. To return to the default configuration, use the **no** form of this command.	ICE	4-462
power inline usage-threshold	Configures the threshold for initiating inline power usage alarms. To return to the default configuration, use the **no** form of this command.	GC	4-462
power inline traps enable	Enables inline power traps. To disable inline power traps, use the **no** form of this command.	GC	4-463
show power inline	Displays the information about inline power.	UE	4-464

.

power inline

The **port inline** Interface Configuration (Ethernet) mode command configures the administrative mode of inline power on an interface.

Syntax

power inline {auto | never}

Parameters

- **auto —** Enables the device discovery protocol and, if found, supplies power to the device.
- **never —** Disables the device discovery protocol and stops supplying power to the device.

Default Setting

The device discovery protocol is enabled.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables powered device discovery protocol on port 1/e1, so that power will be supplied to a discovered device.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# power inline auto
```

Related Commands

power inline powered-device

power inline priority

power inline usage-threshold

show power inline

power inline powered-device

The **power inline powered-device** Interface Configuration (Ethernet) mode command adds a comment or description of the powered device type to enable the user to remember what is attached to the interface. To remove the description, use the **no** form of this command.

Syntax

power inline powered-device *pd-type*

no power inline powered-device

Parameters

- *pd-type* **—** Specifies the type of powered device attached to the interface (Range: 1-24 characters).

Default Setting

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures a description to an IP-phone to a powered device connected to Ethernet interface 1/e1.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# power inline powered-device IP-phone
```

Related Commands

power inline

power inline priority

power inline usage-threshold

show power inline

power inline priority

The **power inline priority** Interface Configuration (Ethernet) mode command configures the inline power management priority of the interface. To return to the default configuration, use the **no** form of this command.

Syntax

power inline priority {critical | high | low}

no power inline priority

Parameters

- **critical —** Indicates that operating the powered device is critical.
- **high —** Indicates that operating the powered device has high priority.
- **low —** Indicates that operating the powered device has low priority.

Default Setting

The default setting is low priority.

Command Mode

Interface Configuration (Ethernet) mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the device connected to Ethernet interface 1/e1 as a high-priority powered device.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# power inline priority high
```

Related Commands

power inline

power inline powered-device

power inline usage-threshold

show power inline

power inline usage-threshold

The **power inline usage-threshold** Global Configuration mode command configures the threshold for initiating inline power usage alarms. To return to the default configuration, use the **no** form of this command.

Syntax

power inline usage-threshold *percentage*

no power inline usage-threshold

Parameters

- *percentage* **—** Specifies the threshold as a percentage to compare measured power (Range: 1-99).

Default Setting

The default threshold is 95 percent.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the power usage threshold for which alarms are sent to 80%.

```
Console(config)# power inline usage-threshold 80
```

Related Commands

power inline

power inline powered-device

power inline priority

show power inline

power inline traps enable

The **power inline traps enable** Global Configuration mode command enables inline power traps. To disable inline power traps, use the **no** form of this command.

Syntax

power inline traps enable

no power inline traps

Default Setting

Inline power traps are disabled.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables inline power traps to be sent when a power usage threshold is exceeded.

```
Console(config)# power inline traps enable
```

Related Commands

show power inline

show power inline

The **show power inline** User EXEC mode command displays the information about inline power.

Syntax

show power inline [ethernet *interface*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays information about inline power.

```
Console# show power inline


Power: On

Nominal Power: 150 Watt

Consumed Power: 120 Watts (80%)

Usage Threshold: 95%

Traps: Enabled


Port      Powered Device   State     Priority    Status     Classification [w]

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

1/e1      IP Phone Model   Auto      High        On         0.44 - 12.95
          A

2/e1      Wireless AP      Auto      Low         On         0.44 - 3.84
          Model

3/e1                       Auto      Low         Off        N/A


Console# show power inline ethernet 1/e1
```

```
Port     Powered Device   State    Priority    Status    Classification [w]
----     -------------    -----    --------    ------    -----------------
         ---
1/e1     IP Phone Model   Auto     High        On        0.44 - 12.95
         A

Overload Counter: 1
Short Counter: 0
Denied Counter: 0
Absent Counter: 0
Invalid Signature Counter: 0
```

The following table describes the significant fields shown in the example:

Field	Description
Power	The operational status of the inline power sourcing equipment.
Nominal Power	The nominal power of the inline power sourcing equipment in Watts.
Consumed Power	Measured usage power in Watts.
Usage Threshold	The usage threshold expressed in percents for comparing the measured power and initiating an alarm if threshold is exceeded.
Traps	Indicates if inline power traps are enabled.
Port	The Ethernet port number.
Powered Device	Description of the powered device type.
State	Indicates if the port is enabled to provide power. Can be: Auto or Never.
Priority	The priority of the port from the point of view of inline power management. Can be: Critical, High or Low.
Status	Describes the inline power operational status of the port. Can be: On, Off, Test-Fail, Testing, Searching or Fault.
Classification	The power consumption range of the powered device. Can be: 0.44 – 12.95, 0.44 – 3.84, 3.84 – 6.49 or 6.49 – 12.95.
Overload Counter	Counts the number of overload conditions that has been detected.
Short Counter	Counts the number of short conditions that has been detected.
Denied Counter	Counts the number of times power has been denied.

Absent Counter	Counts the number of times power has been removed because powered device dropout was detected.
Invalid Signature Counter	Counts the number of times an invalid signature of a powered device was detected.

Related Commands

power inline

power inline powered-device

power inline priority

power inline usage-threshold

power inline traps enable

QoS Commands

Table 4-24. QoS Commands

Command	Function	Mode	Page
qos	Enables quality of service (QoS) on the device. To disable QoS on the device, use the **no** form of this command.	GC	4-468
show qos	Displays the quality of service (QoS) mode for the device.	UE	4-469
class-map	Creates or modifies a class map and enters the Class-map Configuration mode. To delete a class map, use the **no** form of this command.	GC	4-469
show class-map	Displays all class maps.	UE	4-470
match	Defines the match criteria for classifying traffic. To delete the match criteria, use the **no** form of this command.	CMC	4-471
policy-map	Creates a policy map and enters the Policy-map Configuration mode. To delete a policy map, use the **no** form of this command.	GC	4-472
class	Defines a traffic classification and enters the Policy-map Class Configuration mode. To remove a class map from the policy map, use the **no** form of this command.	PMC	4-472
rate-limit	Limits the rate of the incoming traffic.	UE	4-473
show policy-map	Displays the policy maps.	UE	4-474
trust cos-dscp	Configures the trust state. The trust state determines the source of the internal DSCP value used by Quality of Service (QoS). To return to the default configuration, use the **no** form of this command.	PCC	4-475
set	Sets new values in the IP packet.	PCC	4-476
police	Defines the policer for classified traffic. To remove a policer, use the **no** form of this command.	PCC	4-477
qos aggregate-policer	Defines the policer parameters that can be applied to multiple traffic classes within the same policy map. To remove an existing aggregate policer, use the **no** form of this command.	GC	4-478
show qos aggregate-policer	Displays the aggregate policer parameter.	UE	4-480
police aggregate	Applies an aggregate policer to multiple classes within the same policy map. To remove an existing aggregate policer from a policy map, use the **no** form of this command.	PCC	4-481
wrr-queue cos-map	Maps Class of Service (CoS) values to a specific egress queue. To return to the default configuration, use the **no** form of this command.	GC	4-481
priority-queue out num-of-queues	Configures the number of expedite queues. To return to the default configuration, use the **no** form of this command.	GC	4-482
traffic-shape	Configures the shaper of the egress port/queue. To disable the shaper, use the **no** form of this command.	IC	4-483
show qos interface	Displays Quality of Service (QoS) information on the interface.	UE	4-484

Table 4-24. QoS Commands

Command	Function	Mode	Page
qos wrr-queue threshold	Assigns queue thresholds globally. To return to the default configuration, use the **no** form of this command.	GC	4-486
qos map dscp-dp	Use the **qos map dscp-dp** Global Configuration mode command to map DSCP to Drop Precedence. To return to the default setting, use the **no** form of this command.	GC	4-487
qos map policed-dscp	Modifies the policed-DSCP map for remarking purposes. To return to the default map, use the **no** form of this command.	GC	4-487
qos map dscp-queue	Modifies the DSCP to CoS map. To return to the default map, use the **no** form of this command.	GC	4-488
qos trust (Global)	Configures the system to the basic mode and trust state. To return to the untrusted state, use the **no** form of this command.	GC	4-489
qos cos	Defines the default CoS value of a port. To return to the default configuration, use the **no** form of this command.	IC	4-490
qos dscp-mutation	Applies the DSCP Mutation map to a system DSCP trusted port. To return to the trust state with no DSCP mutation, use the **no** form of this command.	GC	4-491
qos map dscp-mutation	Modifies the DSCP to DSCP mutation map. To return to the default DSCP to DSCP mutation map, use the **no** form of this command.	GC	4-492
show qos map	Displays the QoS mapping information.	GC	4-493

qos

The **qos** Global Configuration mode command enables quality of service (QoS) on the device. To disable QoS on the device, use the **no** form of this command.

Syntax

qos [basic | advanced]

no qos

Parameters

- **basic** — QoS basic mode.
- **advanced** — QoS advanced mode, which enables the full range of QoS configuration.

Default Setting

The QoS basic mode is enabled.

Command Mode

Global Configuration mode

Command Usage

If QoS Mode is set to Advanced, the command **qos trust** is applied only to packets that egress from the GE ports.

Example

The following example enables QoS on the device.

```
Console(config)# qos
```

Related Commands

show qos

show qos

The **show qos** User EXEC mode command displays the quality of service (QoS) mode for the device.

Syntax

show qos

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

Trust mode is displayed if QoS is enabled in basic mode.

Example

The following example displays QoS attributes when QoS is enabled in basic mode on the device.

```
Console> show qos
Qos: basic
Basic tust: dscp
```

Related Commands

qos

class-map

The **create-map** Global Configuration mode command creates or modifies a class map and enters the Class-map Configuration mode. To delete a class map, use the **no** form of this command.

Syntax

class-map *class-map-name* [**match-all** | **match-any**]

no class-map *class-map-name*

Parameters

- *class-map-name* — Specifies the name of the class map.
- **match-all** — Checks that the packet matches all classification criteria in the class map match statement.

- **match-any** — Checks that the packet matches one or more classification criteria in the class map match statement.

Default Setting

By default, the **match-all** parameter is selected.

Command Mode

Global Configuration mode

Command Usage

The **class-map** Global Configuration mode command is used to define packet classification, marking and aggregate policing as part of a globally named service policy applied on a per-interface basis.

The Class-Map Configuration mode enables entering up to two **match** Class-map Configuration mode commands to configure the classification criteria for the specified class. If two **match** Class-map Configuration mode commands are entered, each should point to a different type of ACL (e.g., one to an IP ACL and one to a MAC ACL). Since packet classification is based on the order of the classification criteria, the order in which the **match** Class-Map Configuration mode commands are entered is important.

If there is more than one match statement in a **match-all** class map and the same classification field appears in the participating ACLs, an error message is generated.

Note: A class map in match-all mode cannot be configured if it contains both an IP ACL and a MAC ACL with an ether type that is not 0x0800.

Example

The following example creates a class map called class1 and configures it to check that packets match all classification criteria in the class map match statement.

```
Console(config)# class-map class1 match-all
Console(config-cmap)#
```

Related Commands

show class-map

show class-map

The **show class-map** User EXEC mode command displays all class maps.

Syntax

show class-map [*class-map-name*]

Parameters

- *class-map-name* — Specifies the name of the class map to be displayed.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example shows the class map for class1.

```
Console> show class-map class1
Class Map match-any class1 (id4)
Match Ip dscp 11 21
```

Related Commands

class-map

match

The **match** Class-map Configuration mode command defines the match criteria for classifying traffic. To delete the match criteria, use the **no** form of this command.

Syntax

match access-group *acl-name*

no match access-group *acl-name*

Parameters

- *acl-name* — Specifies the name of an IP or MAC ACL.

Default Setting

No match criterion is supported.

Command Mode

Class-map Configuration mode.

Command Usage

There are no user guidelines for this command.

Example

The following example defines the match criterion for classifying traffic as an access group called Alcatel in a class map called class1..

```
Console (config)# class-map class1
Console (config-cmap)# match access-group alcatel
```

Related Commands

ip-access-list

mac access-list

policy-map

The **policy-map** Global Configuration mode command creates a policy map and enters the Policy-map Configuration mode. To delete a policy map, use the **no** form of this command.

Syntax

policy-map *policy-map-name*

no policy-map *policy-map-name*

Parameters

- *policy-map-name* — Specifies the name of the policy map.

Default Setting

If the packet is an IP packet, the DCSP value of the policy map is 0.

If the packet is tagged, the CoS value is 0.

Command Mode

Global Configuration mode

Command Usage

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** Global Configuration mode command to specify the name of the policy map to be created or modified.

Class policies in a policy map can only be defined if match criteria has already been defined for the classes. Use the **class-map** Global Configuration and **match** Class-map Configuration commands to define the match criteria of a class.

Only one policy map per interface per direction is supported. A policy map can be applied to multiple interfaces and directions.

Example

The following example creates a policy map called policy1 and enters the Policy-map Configuration mode.

```
Console (config)# policy-map policy1
Console (config-pmap)#
```

Related Commands

show policy-map

service-policy

class

The **class** Policy-map Configuration mode command defines a traffic classification and enters the Policy-map Class Configuration mode. To remove a class map from the policy map, use the **no** form of this command.

Syntax

class *class-map-name* [**access-group** *acl-name*]

no class *class-map-name*

Parameters

- *class-map-name* — Specifies the name of an existing class map. If the class map does not exist, a new class map will be created under the specified name.
- *acl-name* — Specifies the name of an IP or MAC ACL.

Default Setting

No policy map is defined.

Command Mode

Policy-map Configuration mode

Command Usage

Before modifying a policy for an existing class or creating a policy for a new class, use the **policy-map** Global Configuration mode command to specify the name of the policy map to which the policy belongs and to enter the Policy-map Configuration mode.

Example

The following example defines a traffic classification called class1 with an access-group called Alcatel. The class is in a policy map called policy1.

```
Console(config)# policy-map policy1
Console (config-pmap)# class class1 access-group Alcatel
```

rate-limit

The **rate-limit** interface configuration command limits the rate of the incoming traffic. The **no** form of this command is used to disable rate limit.

Syntax

rate-limit *rate*

no rate-limit

Parameters

- *rate* — Maximum of kilobits per second of ingress traffic on a port. (Range: 62K - 100M)

Default Setting

1000 Kbits/Sec

Command Mode

Interface configuration (Ethernet)

Command Usage

The command can be enabled on a specific port only if port storm-control brodcast enable interface configuration command is not enabled on that port.

Example

The following example limits the rate of the incoming traffic to 62.

```
Console(config-ip)# rate-limit 62
```

rate-limit (VLAN)

The **rate-limit** VLAN global configuration command limits the rate of the incoming traffic for a VLAN. Use the **no** form to disable rate limit.

Syntax

rate-limit *vlan committed-rate-kbps committed-burst-byte*

no rate-limit *vlan*

Parameters

- *vlan* — Specifies the VLAN ID*.*
- *committed-rate-kbps* — The average traffic rate (CIR) in kbits per second(bps).
- *committed-burst-byte* — The maximum burst size (CBS) in bytes.

Default Setting

Disabled.

Command Mode

Global configuration

Command Usage

Rate limit is calculated separately for each unit in a stack, and for each packet processor in a unit. Traffic policing in a policy map have precedence over VLAN rate limiting. I.e. if a packet is subject to traffic policing in a policy map and is associated with a VLAN that is rate limited, the packet would be counted only in the traffic policing of the policy map.

Example

The following example limits the rate of the incoming traffic for a VLAN.

```
Console(config)# rate-limit CIR CBS
```

show policy-map

The **show policy-map** User EXEC command displays the policy maps.

Syntax

show policy-map [*policy-map-name* [**class** *class-name*]]

Parameters

- *policy-map-name* — Specifies the name of the policy map to be displayed.
- *class-name* — Specifies the name of the class whose QoS policies are to be displayed.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays all policy maps.

```
Console> show policy-map
Policy Map policy1
  class class1
    set Ip dscp 7

Policy Map policy2
  class class 2
    police 96000 4800 exceed-action drop
  class class3
    police 124000 96000 exceed-action policed-dscp-transmit
```

Related Commands

policy-map

service-policy

trust cos-dscp

The **trust cos-dscp** Policy-map Class Configuration mode command configures the trust state. The trust state determines the source of the internal DSCP value used by Quality of Service (QoS). To return to the default configuration, use the **no** form of this command.

Syntax

trust cos-dscp

no trust cos-dscp

Default Setting

The port is not in the trust mode.

If the port is in trust mode, the internal DSCP value is derived from the ingress packet.

Command Mode

Policy-map Class Configuration mode

Command Usage

Action serviced to a class, so that if an IP packet arrives, the queue is assigned per DSCP. If a non-IP packet arrives, the queue is assigned per CoS (VPT).

Example

The following example configures the trust state for a class called class1 in a policy map called policy1.

```
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# trust cos-dscp
```

Related Commands

set

set

The **set** Policy-map Class Configuration mode command sets new values in the IP packet.

Syntax

set {**dscp** *new-dscp* | **queue** *queue-id* | **cos** *new-cos*}

no set

Parameters

- *new-dscp* — Specifies a new DSCP value for the classified traffic (Range: 0-63).
- *queue-id* — Specifies an explicit queue ID for setting the egress queue.
- *new-cos* — Specifies a new user priority for marking the packet (Range: 0-7).

Default Setting

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

Command Usage

This command is mutually exclusive with the **trust** Policy-map Class Configuration command within the same policy map.

Policy maps that contain **set** or **trust** Policy-map Class Configuration commands or that have ACL classifications cannot be attached to an egress interface by using the **service-policy** (Ethernet, Port-channel) Interface Configuration mode command.

To return to the Policy-map Configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

If QoS Mode is set to Advanced, the command **qos trust** is applied only to packets that egress from the GE ports.

The command does not function an FE port.

Example

The following example sets the dscp value in the packet to 56 for classes in in policy map called policy1.

```
Console (config)# policy-map policy1
Console (config-pmap)# set dscp 56
Console (config-if)# service-policy input policy1
```

Related Commands

trust cos-dscp

police

The **police** Policy-map Class Configuration mode command defines the policer for classified traffic. To remove a policer, use the **no** form of this command.

Syntax

police *committed-rate-bps committed-burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit** }]

no police

Parameters

- *committed-rate-bps* — Specifies the average traffic rate (CIR) in Kbps. (Range: 64-1000000)
- *committed-burst-byte* — Specifies normal burst size (CBS) in bytes (Range: 4096-16769020). The FE maximum rate is 62500.
- **drop** — Indicates that when the rate is exceeded, the packet is dropped.
- **policed-dscp-transmit** — Indicates that when the rate is exceeded, the DSCP of the packet is remarked according to the policed-DSCP map as configured by the **qos map policed-dscp** Global Configuration mode command.

Default Setting

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

Command Usage

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 bps or the normal burst size exceeds 96000 bps, the packet is dropped. The class is called class1 and is in a policy map called policy1..

```
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# police 124000 9600 exceed-action drop
```

Related Commands

qos aggregate-policer

show qos aggregate-policer

police aggregate

service-policy

The service-policy command applies a policy map to the input of a particular interface. Use no form in order to detach policy map from interface.

Syntax

service-policy input *policy-map-name*

no service-policy input

no police

Parameters

- *policy-map-name* — Applies the specified policy-map to the input interface.

Default Setting

This command has no default configuration.

Command Mode

Interface configuration (Ethernet, VLAN, Port-Channel).

Command Usage

One policy map per interface per direction is supported.

Example

The following command applies a policy map to the input of a particular interface.

```
Console(config)# interface ethernet 1/1
Console(config-if) service-policy input
```

qos aggregate-policer

The **qos aggregate-policer** Global Configuration mode command defines the policer parameters that can be applied to multiple traffic classes within the same policy map. To remove an existing aggregate policer, use the **no** form of this command.

Syntax

qos aggregate-policer *aggregate-policer-name committed-rate-bps excess-burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**} [**dscp** *dscp*]

no qos aggregate-policer

Parameters

- *aggregate-policer-name* — Specifies the name of the aggregate policer.
- *committed-rate-bps* — Specifies the average traffic rate (CIR) in Kbps (Range: 64-1000000).
- *excess-burst-byte* — Specifies the excess burst size (CBS) in bytes (Range: 4096-16769020). The FE maximum rate is 62500.
- **drop** — Indicates that when the rate is exceeded, the packet is dropped.
- **policed-dscp-transmit** — Indicates that when the rate is exceeded, the DSCP of the packet is remarked.
- *dscp* — Specifies the value that the DSCP would be remarked. If unspecified, the DSCP would be remarked according to the policed-DSCP map as configured by the **qos map policed-dscp** Global Configuration mode command.

Default Setting

No aggregate policer is define.

Command Mode

Global Configuration mode

Command Usage

Policers that contain **set** or **trust** Policy-map Class Configuration commands or that have ACL classifications cannot be attached to an output interface.

Define an aggregate policer if the policer is shared with multiple classes.

Policers in one port cannot be shared with other policers in another device; traffic from two different ports can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps.

This policer can also be used in Cascade police to make a cascade policer.

An aggregate policer cannot be deleted if it is being used in a policy map. The **no police aggregate** Policy-map Class Configuration command must first be used to delete the aggregate policer from all policy maps.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following example defines the parameters of a policer called policer1 that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 bps or the normal burst size exceeds 96000 bps, the packet is dropped..

```
Console (config)# qos aggregate-policer policer1 124000 96000
exceed-action drop
```

Related Commands

police

show qos aggregate-policer

police aggregate

show qos aggregate-policer

The **show qos aggregate-policer** User EXEC mode command displays the aggregate policer parameter.

Syntax

show qos aggregate-policer [*aggregate-policer-name*]

Parameters

- *aggregate-policer-name* — Specifies the name of the aggregate policer to be displayed.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines.

Example

The following example displays the parameters of the aggregate policer called policer1.

```
Console> show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
not used by any policy map
```

Related Commands

police

qos aggregate-policer

police aggregate

police aggregate

The **police aggregate** Policy-map Class Configuration mode command applies an aggregate policer to multiple classes within the same policy map. To remove an existing aggregate policer from a policy map, use the **no** form of this command.

Syntax

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

Parameters

- *aggregate-policer-name* — Specifies the name of the aggregate policer.

Default Setting

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

Command Usage

An aggregate policer can be applied to multiple classes in the same policy map; An aggregate policer cannot be applied across multiple policy maps or interfaces.

To return to the Policy-map Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

Example

The following example applies the aggregate policer called policer1 to a calass called class1 in policy map called policy1.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1
Console(config-pmap-c)# police aggregate policer1
```

Related Commands

police

qos aggregate-policer

show qos aggregate-policer

wrr-queue cos-map

The **wrr-queue cos-map** Global Configuration mode command maps Class of Service (CoS) values to a specific egress queue. To return to the default configuration, use the **no** form of this command.

Syntax

wrr-queue cos-map *queue-id cos1...cos8*

no wrr-queue cos-map [*queue-id*]

Parameters

- *queue-id* — Specifies the queue number to which the CoS values are mapped.
- *cos1...cos8* — Specifies CoS values to be mapped to a specific queue (Range: 0-7).

Default Setting

There is no default configuration for this command.

Command Mode

Global Configuration mode

Command Usage

This command can be used to distribute traffic into different queues, where each queue is configured with different Weighted Round Robin (WRR) and Weighted Random Early Detection (WRED) parameters.

It is recommended to specifically map a single VPT to a queue, rather than mapping multiple VPTs to a single queue. Use the **priority-queue out** Interface Configuration (Ethernet, Port-channel) mode command to enable expedite queues.

Example

The following example maps CoS 7 to queue 2.

```
Console(config)# wrr-queue cos-map 2 7
```

Related Commands

priority-queue out num-of-queues

priority-queue out num-of-queues

The **priority-queue out num-of-queues** Global Configuration mode command configures the number of expedite queues. To return to the default configuration, use the **no** form of this command.

Syntax

priority-queue out num-of-queues *number-of-queues*

no priority-queue out num-of-queues

Parameters

- *number-of-queues* — Specifies the number of expedite queues. Expedite queues have higher indexes (Range: 0-4).

Default Setting

All queues are expedite queues.

Command Mode

Global Configuration mode

Command Usage

Configuring the number of expedite queues affects the Weighted Round Robin (WRR) weight ratio because fewer queues participate in the WRR.

Example

The following example configures the number of expedite queues as 0.

```
Console(config)# priority-queue out num-of-queues 0
```

Related Commands

wrr-queue cos-map

traffic-shape

The **traffic-shape** Interface Configuration (Ethernet, port-channel) mode command configures the shaper of the egress port. To disable the shaper, use the **no** form of this command.

Syntax

traffic-shape { *committed-rate committed-burst* }

no traffic-shape

Parameters

- *committed-rate* — Specifies the average traffic rate (CIR) in Kbps. (Range: 64-1000000)
- *excess-burst* — Specifies the excess burst size (CBS) in bytes. (Range: 4096-16769020). The FE maximum rate is 62500.

Default Setting

No shape is defined.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

This command activates the shaper on a specified egress port.

To activate the shaper on an egress port, enter the Interface Configuration mode and specify the port number. Then run this command without the **queue-id** parameter. The CIR and the CBS will be applied to the specified port.

Example

The following example sets a shaper on Ethernet port 1/g1 when the average traffic rate exceeds 124000 bps or the normal burst size exceeds 96000 bps.

```
Console(config)# interface ethernet 1/g1
Console(config-if) traffic-shape 124000 96000
```

Related Commands

qos map policed-dscp

qos map dscp-queue

show qos interface

The **show qos interface** User EXEC mode command displays Quality of Service (QoS) information on the interface.

Syntax

show qos interface [buffers | **queueing** | **policers** | **shapers** | *rate-limit*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]

Parameters

- **buffers** — Display quality of service (QoS) buffers information at the interface level.
- **queuing** — Display quality of service (QoS) queuing information at the interface level.
- **policers** — Display quality of service (QoS) policers information at the interface level.
- **shapers** — Display quality of service (QoS) shapers information at the interface leve.
- **rate limit** — Display quality of service (QoS) rate-limit information at the interface leve.
- ***ethernet*** *interface-number* — Specify port for which QoS information will be displayed.
- **vlan** *vlan-id* — Vlan number.
- **port-channel** *number* — Specify port channel to which QoS information is directed.

Default Setting

There is no default configuration for this command.

Command Mode

User EXEC mode

Command Usage

If no keyword is specified, port QoS QoS mode (for example, DSCP trusted, CoS trusted, untrusted), default CoS value, DSCP-to-DSCP-mutation map attached to the port, and policy map attached to the interface are displayed.

If no interface is specified, QoS information about all interfaces is displayed.

Example

The following example displays the buffer settings for queues on Ethernet port 1/e1.

```
Console# show qos interface ethernet 1/e1 buffers

Ethernet 1/e1
```

```
Notify Q depth


qid    Size

1      125

2      125

3      125

4      125

5      125

6      125

7      125

8      125


qid                                                   Threshold

1                                                     100

2                                                     100

3                                                     100

4                                                     100

5                                                     N/A

6                                                     N/A

7                                                     N/A

8                                                     N/A


qid    Min    Max    Prob   Min    Max    Prob   Min    Max    Prob   Weight
       DP0    DP0    DP0    DP1    DP1    DP1    DP2    DP2    DP2

1      N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

2      N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

3      N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

4      N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

5      50     60     13     65     80     6      85     95     4      2

6      50     60     13     65     80     6      85     95     4      2

7      50     60     13     65     80     6      85     95     4      2

8      50     60     13     65     80     6      85     95     4      2
```

Related Commands

qos map policed-dscp

qos map dscp-queue

qos wrr-queue threshold

The **wrr-queue threshold** Global Configuration mode command assigns queue thresholds globally. To return to the default configuration, use the **no** form of this command.

Syntax

qos wrr-queue threshold *queue-id threshold-percentage0 threshold-percentage1, threshold-percentage2*

no qos wrr-queue threshold *queue-id*

qos wrr-queue threshold gigabitethernet *queue-id threshold-percentage0 threshold-percentage1, threshold-percentage2*

no qos wrr-queue threshold gigabitethernet *queue-id*

no qos wrr-queue threshold *queue-id*

Parameters

- **gigabitethernet** — Indicates that the thresholds are to be applied to Gigabit Ethernet ports.
- *queue-id* — Specifies the queue number to which the threshold is assigned.
- *threshold-percentage 0,1,2* — Specifies the queue threshold percentage value. Each value is separated by a space. (Range: 0-100)

Default Setting

80 percent for all thresholds.

Command Mode

Global Configuration mode.

Command Usage

The packet refers to a certain threshold by the conformance level. If threshold 0 is exceeded, packets with the corresponding DP are dropped until the threshold is no longer exceeded. However, packets assigned to threshold 1 or 2 continue to be queued and sent as long as the second or third threshold is not exceeded.

Example

The following example assigns a threshold of 80 percent to WRR queue 1.

```
Console (config)# qos wrr-queue threshold gigabitethernet 1 80
```

Related Commands

show qos interface

qos map dscp-dp

Use the **qos map dscp-dp** Global Configuration mode command to map DSCP to Drop Precedence. To return to the default setting, use the **no** form of this command.

Syntax

qos map dscp-dp *dscp-list* **to** *dp*

no qos map dscp-dp

Parameters

- *dscp-list* — Specifies up to 8 DSCP values separated by a space.
- *dp* — Enter the Drop Precedence value to which the DSCP value corresponds. (Possible values are 0 - 2 where 2 is the highest Drop Precedence)
- *dp* — Enter the Drop Precedence value to which the DSCP value corresponds. (Possible values are 0 - 1 where 1 is the highest Drop Precedence)
- Parameters Range
  - *dscp-list* 0 -63
  - *dp* 0 -2
  - *dp* 0 -1

Default Setting

All the DSCPs are mapped to Drop Precedence 0.

Command Mode

Global Configuration mode.

Command Usage

There are no user guidelines for this command.

·Example

The following example maps DSCP value 123 to Drop Precedence 1.

```
Console (config)# qos map dscp-dp 123 to 1
```

Related Commands

show qos interface

qos map policed-dscp

The **qos map policed-dscp** Global Configuration mode command modifies the policed-DSCP map for remarking purposes. To return to the default map, use the **no** form of this command.

Syntax

qos map policed-dscp *dscp-list* **to** *dscp-mark-down*

no qos map policed-dscp

Parameters

- *dscp- list* — Specifies up to 8 DSCP values separated by a space. (Range: 0-63)
- *dscp-mark-down* — Specifies the DSCP value to mark down. (Range: 0-63)

Default Setting

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

Command Usage

DSCP values 3,11,19… cannot be remapped to other values.

·Example

The following example marks down incoming DSCP value 3 as DSCP value 43 on the policed-DSCP map.

```
Console(config)# qos map policed-dscp 3 to 43
Reserved DSCP. DSCP 3  was not configured.
```

Related Commands

show qos interface

qos map dscp-queue

qos map dscp-queue

The **qos map dscp-queue** Global Configuration mode command modifies the DSCP to CoS map. To return to the default map, use the **no** form of this command.

Syntax

qos map dscp-queue *dscp-list* **to** *queue-id*

no qos map dscp-queue

Parameters

- *dscp-list* — Specifies up to 4 DSCP values separated by a space. (Range: 0 - 63)
- *queue-id* — Specifies the queue number to which the DSCP values are mapped.

Default Setting

The following table describes the default map.

DSCP value	0-15	16-31	32-47	48-63
Queue-ID	1	2	3	4

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
Console(config)# qos map dscp-queue 33 40 41 to 1
```

Related Commands

show qos interface

qos map policed-dscp

qos trust (Global)

The **qos trust** Global Configuration mode command configures the system to the basic mode and trust state. To return to the untrusted state, use the **no** form of this command.

Syntax

qos trust {**cos** | **dscp**}

no qos trust

Parameters

- **cos** — Indicates that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- **dscp** — Indicates that ingress packets are classified with packet DSCP values.

Default Setting

CoS is the default trust mode.

Command Mode

Global Configuration mode

Command Usage

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every device in the domain.

A switch port on an inter-QoS domain boundary can be configured to the DSCP trust state, and, if the DSCP values are different between the QoS domains, the DSCP to DSCP mutation map can be applied.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured as trust DSCP, traffic is mapped to a queue according to the DSCP-queue map.

If QoS Mode is set to Advanced, the command **qos trust** is applied only to packets that egress from the GE ports.

Example

The following example configures the system to the DSCP trust state.

```
Console(config)# qos trust dscp
```

Related Commands

qos cos

qos trust (Interface)

The qos trust (Interface) command enables each port trust state while the system is in basic mode. Use no for to disable trust state on each port.

qos trust

no qos trust

Default Setting

Each port is enabled while system is in basic mode.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

No Command Usage for this command.

Example.

The following example enables each port trust state while the system is in basic mode

```
Console(config)# interface ethernet 1/e15
Console(config-if) qos trust 3
```

qos cos

The **qos cos** Interface Configuration (Ethernet, port-channel) mode command defines the default CoS value of a port. To return to the default configuration, use the **no** form of this command.

Syntax

qos cos *default-cos*

Parameters

- *default-cos* — Specifies the default CoS value of the port. (Range: 0 - 7)

Default Setting

Default CoS value of a port is 0.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

If the port is trusted, the default CoS value of the port is used to assign a CoS value to all untagged packets entering the port.

Example

The following example configures port 1/e15 default CoS value to 3.

```
Console(config)# interface ethernet 1/e15
Console(config-if) qos cos 3
```

Related Commands

qos trust (Global)

qos cos

qos dscp-mutation

The **qos dscp-mutation** Global Configuration mode command applies the DSCP Mutation map to a system DSCP trusted port. To return to the trust state with no DSCP mutation, use the **no** form of this command.

Syntax

qos dscp-mutation

no qos dscp-mutation

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode.

Command Usage

The DSCP to DSCP mutation map is applied to a port at the boundary of a Quality of Service (QoS) administrative domain.

If two QoS domains have different DSCP definitions, use the DSCP to DSCP mutation map to match one set of DSCP values with the DSCP values of another domain.

Apply the DSCP to DSCP mutation map only to ingress and to DSCP-trusted ports. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports.

If the DSCP to DSCP mutation map is applied to an untrusted port, class of service (CoS) or IP-precedence trusted port, this command has no immediate effect until the port becomes DSCP-trusted.

Example

The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
Console(config)# qos dscp-mutation
```

Related Commands

qos trust (Global)

qos cos

qos map dscp-mutation

The **qos map dscp-mutation** Global Configuration mode command modifies the DSCP to DSCP mutation map. To return to the default DSCP to DSCP mutation map, use the **no** form of this command.

Syntax

qos map dscp-mutation *in-dscp* **to** *out-dscp*

n**o qos map dscp-mutation**

Parameters

- *in-dscp* — Specifies up to 8 DSCP values separated by spaces. (Range: 0-63)
- *out-dscp* — Specifies up to 8 DSCP values separated by spaces. (Range: 0-63)

Default Setting

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

Command Usage

This is the only map that is not globally configured. it is possible to have several maps and assign each one to different ports.

Example

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP mutation map value 63.

```
Console (config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

The following table describes the significant fields shown in the example:

Field	Description
Power	The operational status of the inline power sourcing equipment.
Nominal Power	The nominal power of the inline power sourcing equipment in Watts.
Consumed Power	Measured usage power in Watts.
Usage Threshold	The usage threshold expressed in percents for comparing the measured power and initiating an alarm if threshold is exceeded.
Traps	Indicates if inline power traps are enabled.
Port	The Ethernet port number.
Powered Device	Description of the powered device type.
State	Indicates if the port is enabled to provide power. Can be: Auto or Never.
Priority	The priority of the port from the point of view of inline power management. Can be: Critical, High or Low.
Status	Describes the inline power operational status of the port. Can be: On, Off, Test-Fail, Testing, Searching or Fault.
Classification	The power consumption range of the powered device. Can be: 0.44 – 12.95, 0.44 – 3.84, 3.84 – 6.49 or 6.49 – 12.95.
Overload Counter	Counts the number of overload conditions that has been detected.
Short Counter	Counts the number of short conditions that has been detected.
Denied Counter	Counts the number of times power has been denied.
Absent Counter	Counts the number of times power has been removed because powered device dropout was detected.
Invalid Signature Counter	Counts the number of times an invalid signature of a powered device was detected.

Related Commands

qos dscp-mutation

show qos map

The **show qos map** Global Configuration mode command displays the QoS mapping information.

Syntax

```
show qos map [dscp-queue  | dscp-dp | tcp-port-queue |  udp-port-queue  |
policed-dscp | dscp-mutation | service-type-cos | service-type-dscp]
```

Parameters

- **dscp-queue** — Displays the DSCP to queue map.
- **dscp-dp** — Displays the DSCP to Drop Precedence map.

- **tcp-port-queue** — Displays the TCP Port to queue map.
- **udp-port-queue** — Displays the UDP Port to queue map.
- **policed-dscp** — Displays the DSCP to DSCP remark table.
- **dscp-mutation** — Displays the DSCP-DSCP mutation table.
- **service-type-cos** — Displays the Service type to CoS map (Service mode only).
- **service-type-dscp** — Displays the Service type to DSCP map (Service mode only).

Default Configuration

The default configuration is set to disabled.

Command Mode

EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the QoS mapping information.

```
Console> show qos map
```

RADIUS Commands

Table 4-25. RADIUS Commands

Command	Function	Mode	Page
radius-server host	Specifies a RADIUS server host. To delete the specified RADIUS host, use the **no** form of this command.	GC	4-495
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. To return to the default configuration, use the **no** form of this command.	GC	4-497
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts. To reset the default configuration, use the **no** form of this command.	GC	4-497
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers. To return to the default configuration, use the **no** form of this comman.	GC	4-498
radius-server timeout	Sets the interval during which the device waits for a server host to reply. To return to the default configuration, use the **no** form of this command.	GC	4-499
radius-server deadtime	Improves RADIUS response time when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To return to the default configuration, use the **no** form of this command.	GC	4-500
show radius-servers	Displays the RADIUS server settings.	GC	4-501

radius-server host

The **radius-server host** Global Configuration mode command specifies a RADIUS server host. To delete the specified RADIUS host, use the **no** form of this command.

Syntax

radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**source** *source*] [**priority** *priority*] [**usage** *type*]

no radius-server host {*ip-address* | *hostname*}

Parameters

- *ip-address* — IP address of the RADIUS server host.
- *hostname* — Hostname of the RADIUS server host. (Range: 1-158 characters)
- *auth-port-number* — Port number for authentication requests. The host is not used for authentication if the port number is set to 0. (Range: 0-65535)
- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)
- *retries* — Specifies the retransmit value. (Range: 1-10)
- *deadtime* — Length of time in minutes during which a RADIUS server is

skipped over by transaction requests. (Range: 0-2000)

- *key-string* — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Range: 0-128 characters)
- *source* — Specifies the source IP address to use for communication. 0.0.0.0 is interpreted as request to use the IP address of the outgoing IP interface.
- *priority* — Determines the order in which servers are used, where 0 has the highest priority. (Range: 0-65535)
- *type* — Specifies the usage type of the server. Possible values: **login**, **dot.1x** or **all**.

Default Setting

No RADIUS server host is specified.

The port number for authentication requests is 1812.

The usage type is **all**.

Command Mode

Global Configuration mode

Command Usage

To specify multiple hosts, multiple **radius-server host** commands can be used.

If no host-specific timeout, retries, deadtime or key-string values are specified, global values apply to each RADIUS server host.

The address type of the source parameter must be the same as the **ip-address** parameter.

To define a RADIUS server on the out-of-band port, use the out-of-band IP address format - oob/ip-address.

Example

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20 and a 20-second timeout period.

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

Related Commands

radius-server key

radius-server retransmit

radius-server source-ip

radius-server timeout

radius-server deadtime

show radius-servers

radius-server key

The **radius-server key** Global Configuration mode command sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. To return to the default configuration, use the **no** form of this command.

Syntax

radius-server key [*key-string*]

no radius-server key

Parameters

- *key-string* — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0-128 characters)

Default Setting

The key-string is an empty string.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
Console(config)# radius-server key alcatel-server
```

Related Commands

radius-server host

radius-server retransmit

radius-server source-ip

radius-server timeout

radius-server deadtime

show radius-servers

radius-server retransmit

The **radius-server retransmit** Global Configuration mode command specifies the number of times the software searches the list of RADIUS server hosts. To reset the default configuration, use the **no** form of this command.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

Parameters

- *retries* — Specifies the retransmit value. (Range: 1 - 10)

Default Setting

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the number of times the software searches the list of RADIUS server hosts to 5 times.

```
console(config)# radius-server retransmit 5
```

Related Commands

radius-server host

radius-server key

radius-server source-ip

radius-server timeout

radius-server deadtime

show radius-servers

radius-server source-ip

The **radius-server source-ip** Global Configuration mode command specifies the source IP address used for communication with RADIUS servers. To return to the default configuration, use the **no** form of this command.

Syntax

radius-server source-ip *source*

no radius-source-ip *source*

Parameters

- *source* — Specifies a valid source IP address.

Default Setting

The source IP address is the IP address of the outgoing IP interface.

Command Mode

Global Configuration mode

Command Usage

To define source-ip on the out-of-band port, use the out-of-band IP address format - oob/ip-address.

Example

The following example configures the source IP address used for communication with RADIUS servers to 10.1.1.1.

```
console(config)# radius-server source-ip 10.1.1.1
```

Related Commands

radius-server host

radius-server key

radius-server retransmit

radius-server timeout

radius-server deadtime

show radius-servers

radius-server timeout

The **radius-server timeout** Global Configuration mode command sets the interval during which the device waits for a server host to reply. To return to the default configuration, use the **no** form of this command.

Syntax

radius-server timeout *timeout*

no radius-server timeout

Parameters

- *timeout* — Specifies the timeout value in seconds. (Range: 1 - 30)

Default Setting

The timeout value is 3 seconds.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the timeout interval to 5 seconds.

```
Console(config)# radius-server timeout 5
```

Related Commands

radius-server host

radius-server key

radius-server retransmit

radius-server source-ip

radius-server deadtime

show radius-servers

radius-server deadtime

The **radius-server deadtime** Global Configuration mode command improves RADIUS response time when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To return to the default configuration, use the **no** form of this command.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

Parameters

- *deadtime* — Length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0 - 2000)

Default Setting

The deadtime setting is 0.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example sets the deadtime to 10 minutes.

```
Console(config)# radius-server deadtime 10
```

Related Commands

radius-server host

radius-server key

radius-server retransmit

radius-server source-ip

radius-server timeout

show radius-servers

show radius-servers

The **show radius-servers** Privileged EXEC mode command displays the RADIUS server settings.

Syntax

show radius-servers

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays RADIUS server settings.

```
Console# show radius-servers



IP         Por    TimeOu   Retransm    DeadTim    Source    Priori    Usag
address    t      t        it          e          IP        ty        e
           Aut
           h

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

172.16.1   164    Global   Global      Global     -         1         All
.1         5

172.16.1   164    11       8           Global     Global    2         All
.2         5


Global values

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

TimeOut: 3

Retransmit: 3

Deadtime: 0

Source IP: 172.16.8.1
```

Related Commands

radius-server host

radius-server key

radius-server retransmit

radius-server source-ip

radius-server timeout

radius-server deadtime

RMON Commands

Table 4-26. RMON Commands

Command	Function	Mode	Page
show interfaces status	Displays RMON Ethernet statistics.	UE	4-390
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the **no** form of this command.	IC	4-505
show rmon collection history	Displays the requested RMON history group statistics.	UE	4-506
show rmon history	Displays RMON Ethernet history statistics.	UE	4-507
rmon alarm	Configures alarm conditions. To remove an alarm, use the **no** form of this command.	GC	4-510
show rmon alarm-table	Displays the alarms table.	UE	4-511
show rmon alarm	Displays alarm configuration.	UE	4-512
rmon event	Configures an event. To remove an event, use the **no** form of this command.	GC	4-514
show rmon events	Displays the RMON event table.	UE	4-514
show rmon log	Displays the RMON log table.	UE	4-515
rmon table-size	Configures the maximum size of RMON tables. To return to the default configuration, use the **no** form of this command.	GC	4-517

show rmon statistics

The **show rmon statistics** User EXEC mode command displays RMON Ethernet statistics.

Syntax

show rmon statistics {**ethernet** *interface number* | **port-channel** *port-channel-number*}

Parameters

- *interface number* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays RMON Ethernet statistics for Ethernet port 1/e1.

```
Console> show rmon statistics ethernet 1/e1
Port: 1/e1
Octets: 878128                         Packets: 978
Broadcast: 7                           Multicast: 1
CRC Align Errors: 0                    Collisions: 0
Undersize Pkts: 0                      Oversize Pkts: 0
Fragments: 0                           Jabbers: 0
64 Octets: 98                          65 to 127 Octets: 0
128 to 255 Octets: 0                   256 to 511 Octets: 0
512 to 1023 Octets: 491                1024 to max Octets: 389
```

The following table describes significant fields shown above:

Field	Description
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received and directed to the broadcast address. This does not include multicast packets.
Multicast	The total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1632 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).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Undersize Pkts	The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	The total number of packets received longer than 1632 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and 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	The total number of packets received longer than 1632 octets (excluding framing bits, but including FCS octets), and 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).
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to 1518 Octets	The total number of packets (including bad packets) received that are between 1024 and 1632 octets in length inclusive (excluding framing bits but including FCS octets).

Related Commands

show rmon collection history

rmon collection history

The **rmon collection history** Interface Configuration (Ethernet, port-channel) mode command enables a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the **no** form of this command.

Syntax

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

Parameters

- *index* — Specifies the statistics group index . (Range: 1-65535)
- *ownername* — Specifies the RMON statistics group owner name.
- *bucket-number* — Number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range:1-65535)
- *seconds* — Number of seconds in each polling cycle. (Range: 1-3600)

Default Setting

RMON statistics group owner name is an empty string.

Number of buckets specified for the RMON collection history statistics group is 50.

Number of seconds in each polling cycle is 1800.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

Cannot be configured for a range of interfaces (range context).

Example

The following example enables a Remote Monitoring (RMON) MIB history statistics group on Ethernet port 1/e1 with index number 1 and a polling interval period of 2400 seconds.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# rmon collection history 1 interval 2400
```

Related Commands

show rmon collection history

show rmon history

show rmon collection history

The **show rmon collection history** User EXEC mode command displays the requested RMON history group statistics.

Syntax

show rmon collection history [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — Valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays all RMON history group statistics.

```
Console> show rmon collection history


Index      Interface    Interval    Requested   Granted    Owner
                                    Samples     Samples

-----      ---------    --------    ---------   -------    -------
```

```
1           1/e1          30           50           50          CLI
2           1/e1          1800         50           50          Manager
```

The following table describes significant fields shown above:

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

Related Commands

rmon collection history

show rmon history

show rmon history

The **show rmon history** User EXEC mode command displays RMON Ethernet history statistics.

Syntax

show rmon history *index* {**throughput** | **errors | other**} [**period** *seconds*]

Parameters

- *index* — Specifies the requested set of samples. (Range: 1 - 65535)
- **throughput** — Indicates throughput counters.
- **errors** — Indicates error counters.
- **other** — Indicates drop and collision counters.
- *seconds* — Specifies the period of time in seconds.
  (Range: 1-4294967295)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Examples

The following examples displays RMON Ethernet history statistics for index 1.

```
Console> show rmon history 1 throughput

Sample Set: 1                          Owner: CLI

Interface: 1/e1                        Interval: 1800

Requested samples: 50                  Granted samples: 50


Maximum table size: 500


Time                     Octets       Packet    Broadca     Multica     Util
                                      s         st          st

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

Jan 18 2002 21:57:00     303595962    357568    3289        7287        19%

Jan 18 2002 21:57:30     287696304    275686    2789        5878        20%


Console> show rmon history 1 errors

Sample Set: 1                          Owner: Me

Interface: 1/e1                        Interval: 1800

Requested samples: 50                  Granted samples: 50


Maximum table size: 500 (800 after reset)


Time                     CRC Align    Unders    Oversiz     Fragmen     Jabbe
                                      ize       e           ts          rs

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

Jan 18 2002 21:57:00     1            1         0           49          0

Jan 18 2002 21:57:30     1            1         0           27          0


Console> show rmon history 1 other

Sample Set: 1                          Owner: Me

Interface: 1/e1                        Interval: 1800

Requested samples: 50                  Granted samples: 50
```

```
Maximum table size: 500


Time                                Droppe    Collisi
                                    d         ons

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

Jan 18 2002 21:57:00                3         0

Jan 18 2002 21:57:30                3         0
```

The following table describes significant fields shown above:

Field	Description
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.
Util	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1632 octets, inclusive, but had 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	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	The number of packets received during this sampling interval that were longer than 1632 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had 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 (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.

Jabbers	The number of packets received during this sampling interval that were longer than 1632 octets (excluding framing bits but including FCS octets), and had 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).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

Related Commands

rmon collection history

show rmon collection history

rmon alarm

The **rmon alarm** Global Configuration mode command configures alarm conditions. To remove an alarm, use the **no** form of this command.

Syntax

rmon alarm *index MIB_OBJECT_ID interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]

no rmon alarm *index*

Parameters

- *index* — Specifies the alarm index. (Range: 1-65535)
- MIB_OBJECT_ID — Specifies the object identifier (MIB Number) of the variable to be sampled.
- *interval* — Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1-4294967295)
- *rthreshold* — Specifies the rising threshold. (Range: 0-4294967295)
- *fthreshold* — Specifies the falling threshold. (Range: 0-4294967295)
- *revent* — Specifies the event index used when a rising threshold is crossed. (Range: 1-65535)
- *fevent* — Specifies the event index used when a falling threshold is crossed. (Range: 1-65535)
- *type* — Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. Possible values are **absolute** and **delta**.
- If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- *direction* — Specifies the alarm that may be sent when this entry is first set to valid. Possible values are **rising**, **rising-falling** and **falling**.

  - If the first sample (after this entry becomes valid) is greater than or equal to *rthreshold* and *direction* is equal to **rising** or **rising-falling**, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to *fthreshold* and *direction* is equal to **falling** or **rising-falling**, a single falling alarm is generated.
- *name* — Specifies the name of the person who configured this alarm. If unspecified, the name is an empty string.

Default Setting

The type is **absolute**.

The startup direction is **rising-falling**.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the following alarm conditions:

- Alarm index — 1000
- MIB_OBJECT_ID — MIB Number
- Sample interval — 360000 seconds
- Rising threshold — 1000000
- Falling threshold — 1000000
- Rising threshold event index — 10
- Falling threshold event index — 20

```
Console(config)# rmon alarm 1000 Alcatel 360000 1000000 1000000 10 20
```

Related Commands

show rmon alarm-table

show rmon alarm

show rmon alarm-table

The **show rmon alarm-table** User EXEC mode command displays the alarms table.

Syntax

show rmon alarm-table

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the alarms table.

```
Console> show rmon alarm-table


Index          OID                                     Owner
-----          ----------------------                  -------
1              1.3.6.1.2.1.2.2.1.10.1                  CLI
2              1.3.6.1.2.1.2.2.1.10.1                  Manager
3              1.3.6.1.2.1.2.2.1.10.9                  CLI
```

The following table describes significant fields shown above:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

Related Commands

rmon alarm

show rmon alarm

show rmon alarm

The **show rmon alarm** User EXEC mode command displays alarm configuration.

Syntax

show rmon alarm *number*

Parameters

- *number* — Specifies the alarm index. (Range: 1 - 65535)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays RMON 1 alarms.

```
Console> show rmon alarm 1
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	The statistic value during the last sampling period. For example, if the sample type is **delta**, this value is the difference between the samples at the beginning and end of the period. If the sample type is **absolute**, this value is the sampled value at the end of the period.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is **absolute**, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is **delta**, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.
Owner	The entity that configured this entry.

Related Commands

rmon alarm

show rmon alarm-table

rmon event

The **rmon event** Global Configuration mode command configures an event. To remove an event, use the **no** form of this command.

Syntax

rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]

no rmon event *index*

Parameters

- *index* — Specifies the event index. (Range: 1 - 65535)
- *type* — Specifies the type of notification generated by the device about this event. Possible values: **none**, **log**, **trap**, **log-trap**.
- **community** *text* — If the specified notification type is **trap**, an SNMP trap is sent to the SNMP community specified by this octet string.
(Range: 0-127 characters)
- **description** *text* — Specifies a comment describing this event.
(Range: 0-127 characters)
- *name* — Specifies the name of the person who configured this event. If unspecified, the name is an empty string.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

If **log** is specified as the notification type, an entry is made in the log table for each event. If **trap** is specified, an SNMP trap is sent to one or more management stations.

Example

The following example configures an event identified as index 10 and for which the device generates a notification in the log table.

```
Console(config)# rmon event 10 log
```

Related Commands

show rmon events

show rmon events

The **show rmon events** User EXEC mode command displays the RMON event table.

Syntax

show rmon events

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the RMON event table.

```
Console> show rmon events


Inde    Description      Type        Community    Owner     Last time sent
x

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

1       Errors           Log                      CLI       Jan 18 2002 23:58:17

2       High             Log-Trap    device       Manage    Jan 18 2002 23:59:48
        Broadcast                                 r
```

The following table describes significant fields shown above:

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

Related Commands

rmon event

show rmon log

The **show rmon log** User EXEC mode command displays the RMON log table.

Syntax

show rmon log [*event*]

Parameters

- *event* — Specifies the event index. (Range: 0 - 65535)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the RMON log table.

```
Console> show rmon log

Maximum table size: 500

Event     Description        Time

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

1         Errors             Jan 18 2002 23:48:19

1         Errors             Jan 18 2002 23:58:17

2         High Broadcast     Jan 18 2002 23:59:48


Console> show rmon log

Maximum table size: 500 (800 after reset)

Event     Description        Time

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

1         Errors             Jan 18 2002 23:48:19

1         Errors             Jan 18 2002 23:58:17

2         High Broadcast     Jan 18 2002 23:59:48
```

The following table describes the significant fields shown in the display:

Field	Description
Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry was created.

Related Commands

rmon alarm

rmon table-size

The **rmon table-size** Global Configuration mode command configures the maximum size of RMON tables. To return to the default configuration, use the **no** form of this command.

Syntax

rmon table-size {**history** *entries* | **log** *entries*}

no rmon table-size {**history** | **log**}

Parameters

- **history** *entries* — Maximum number of history table entries.
  (Range: 20-32767)
- **log** *entries* — Maximum number of log table entries. (Range: 20-32767)

Default Setting

History table size is 270.

Log table size is 200.

Command Mode

Global Configuration mode

Command Usage

The configured table size taskes effect after the device is rebooted.

Example

The following example configures the maximum RMON history table sizes to 100 entries.

```
Console(config)# rmon table-size history 100
```

Related Commands

rmon alarm

SNMP Commands

.

Table 4-27. SNMP Commands

Command	Function	Mode	Page
snmp-server community	Configures the community access string to permit access to the SNMP protocol. To remove the specified community string, use the **no** form of this command.	GC	4-519
snmp-server view	Creates or updates a Simple Network Management Protocol (SNMP) server view entry. To remove a specified SNMP server view entry, use the **no** form of this command.	GC	4-520
snmp-server group	Configures a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. To remove a specified SNMP group, use the **no** form of this command.	GC	4-521
snmp-server userr	Configures a new SNMP Version 3 user. To remove a user, use the **no** form of this command.	GC	4-522
snmp-server engineID locall	Specifies the Simple Network Management Protocol (SNMP) engineID on the local device. To remove the configured engine ID, use the **no** form of this command.	GC	4-523
snmp-server enable traps	Enables the device to send SNMP traps. To disable SNMP traps, use the no form of the command.	GC	4-525
snmp-server filter	Creates or updates a Simple Network Management Protocol (SNMP) server filter entry. To remove the specified SNMP server filter entry, use the **no** form of this command.	GC	4-525
snmp-server host	Specifies the recipient of Simple Network Management Protocol Version 1 or Version 2 notifications. To remove the specified host, use the **no** form of this command.	GC	4-526
snmp-server v3-hostt	Specifies the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the **no** form of this command.	GC	4-528
snmp-server trap authentication	Enables the device to send SNMP traps when authentication fails. To disable SNMP failed authentication traps, use the **no** form of this command.	GC	4-529
snmp-server contact	Configures the system contact (sysContact) string. To remove system contact information, use the **no** form of the command.	GC	4-529
snmp-server location	Configures the system location string. To remove the location string, use the **no** form of this command.	GC	4-530
snmp-server sett	Defines the SNMP MIB value.	GC	4-531
show snmp	Displays the SNMP status.	PE	4-531
show snmp engineid	Displays the ID of the local Simple Network Management Protocol (SNMP) engine.	PE	4-533
show snmp views	Displays the configuration of views.	PE	4-534
show snmp groups	Displays the configuration of groups.	PE	4-535
show snmp filters	Displays the configuration of filters.	PE	4-536
show snmp users	Displays the configuration of users.	PE	4-536

.

snmp-server community

The **snmp-server community** Global Configuration mode command configures the community access string to permit access to the SNMP protocol. To remove the specified community string, use the **no** form of this command.

Syntax

snmp-server community *community* [**ro** | **rw** | **su**] [*ip-address*][**view** *view-name*]

snmp-server community-group *community group-name* [*ip-address*]

no snmp-server community *community* [*ip-address*]

Parameters

- *community* — Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 characters)
- **ro** — Indicates read-only access (default).
- **rw** —Indicates read-write access.
- **su** —Indicates SNMP administrator access.
- *ip-address* — Specifies the IP address of the management station.
- *group-name* — Specifies the name of a previously defined group. A group defines the objects available to the community. (Range: 1-30 characters)
- *view-name* — Specifies the name of a previously defined view. The view defines the objects available to the community. (Range: 1-30 characters)

Default Setting

No communities are defined.

Command Mode

Global Configuration mode

Command Usage

The **view-name** parameter cannot be specified for **su**, which has access to the whole MIB.

The **view-name** parameter can be used to restrict the access rights of a community string. When it is specified:

An internal security name is generated.

The internal security name for SNMPv1 and SNMPv2 security models is mapped to an internal group name.

The internal group name for SNMPv1 and SNMPv2 security models is mapped to a view-name (read-view and notify-view always, and for **rw** for write-view also)

The **group-name** parameter can also be used to restrict the access rights of a community string. When it is specified:

An internal security name is generated.

The internal security name for SNMPv1 and SNMPv2 security models is mapped to the group name.

Example

The following example defines community access string **public** to permit administrative access to SNMP protocol at an administrative station with IP address 192.168.1.20.

```
Console(config)# snmp-server community public su 192.168.1.20
```

Related Commands

show snmp

snmp-server view

The **snmp-server view** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server view entry. To remove a specified SNMP server view entry, use the **no** form of this command.

Syntax

snmp-server view *view-name oid-tree* **{included | excluded}**

no snmp-server view *view-name* [*oid-tree*]

Parameters

- *view-name* — Specifies the label for the view record that is being created or updated. The name is used to reference the record.
  (Range: 1-30 characters)
- *oid-tree* — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- **included** — Indicates that the view type is included.
- **excluded** — Indicates that the view type is excluded.

Default Setting

No view entry exists.

Command Mode

Global Configuration mode

Command Usage

This command can be entered multiple times for the same view record.

The number of views is limited to 64.

No check is made to determine that a MIB node corresponds to the "starting portion" of the OID until the first wildcard.

Example

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group.

```
Console(config)# snmp-server view user-view system included
Console(config)# snmp-server view user-view system.7 excluded
Console(config)# snmp-server view user-view ifEntry.*.1 included
```

Related Commands

show snmp

show snmp views

snmp-server group

The **snmp-server group** Global Configuration mode command configures a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. To remove a specified SNMP group, use the **no** form of this command.

Syntax

snmp-server group *groupname* **{v1 | v2 | v3 {noauth | auth | priv} [notify** *notifyview* **] } [read** *readview***] [write** *writeview***]**

no snmp-server group *groupname* **{v1 | v2 | v3 [noauth | auth | priv]}**

Parameters

- *groupname* — Specifies the name of the group.
- **v1** — Indicates the SNMP Version 1 security model.
- **v2** — Indicates the SNMP Version 2 security model.
- **v3** — Indicates the SNMP Version 3 security model.
- **noauth** — Indicates no authentication of a packet. Applicable only to the SNMP Version 3 security model.
- **auth** — Indicates authentication of a packet without encrypting it. Applicable only to the SNMP Version 3 security model.
- **priv** — Indicates authentication of a packet with encryption. Applicable only to the SNMP Version 3 security model.
- *readview* — Specifies a string that is the name of the view that enables only viewing the contents of the agent. If unspecified, all objects except for the community-table and SNMPv3 user and access tables are available.
- *writeview* — Specifies a string that is the name of the view that enables entering data and configuring the contents of the agent. If unspecified, nothing is defined for the write view.
- *notifyview* — Specifies a string that is the name of the view that enables specifying an inform or a trap. If unspecified, nothing is defined for the notify view. Applicable only to the SNMP Version 3 security model.

Default Setting

No group entry exists.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example attaches a group called user-group to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called user-view.

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

Related Commands

show snmp

show snmp groups

snmp-server user

The **snmp-server user** Global Configuration mode command configures a new SNMP Version 3 user. To remove a user, use the **no** form of this command.

Syntax

snmp-server user *username groupname* **[remote** *engineid-string***] [auth-md5** *password* **| auth-sha** *password* **| auth-md5-key** *md5-des-keys* **| auth-sha-key** *sha-des-keys* **]**

no snmp-server user *username* **[remote** *engineid-string***]**

Parameters

- *username* — Specifies the name of the user on the host that connects to the agent. (Range: 1-30 characters)
- *groupname* — Specifies the name of the group to which the user belongs. (Range: 1-30 characters)
- *engineid-string* — Specifies the engine ID of the remote SNMP entity to which the user belongs. The engine ID is a concatenated hexadecimal string. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon.
  (Range: 5-32 characters)
- **auth-md5** *password* — Indicates the HMAC-MD5-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- **auth-sha** *password* — Indicates the HMAC-SHA-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- **auth-md5-key** *md5-des-keys* — Indicates the HMAC-MD5-96 authentication level. The user should enter a concatenated hexadecimal string of the MD5 key (MSB) and the privacy key (LSB). If authentication is

only required, 16 bytes should be entered; if authentication and privacy are required, 32 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (16 or 32 bytes)

- **auth-sha-key** *sha-des-keys* — Indicates the HMAC-SHA-96 authentication level. The user should enter a concatenated hexadecimal string of the SHA key (MSB) and the privacy key (LSB). If authentication is only required, 20 bytes should be entered; if authentication and privacy are required, 36 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (20 or 36 bytes)

Default Setting

No group entry exists.

Command Mode

Global Configuration mode

Command Usage

If auth-md5 or auth-sha is specified, both authentication and privacy are enabled for the user.

When a **show running-config** Privileged EXEC mode command is entered, a line for this user will not be displayed. To see if this user has been added to the configuration, type the **show snmp users** Privileged EXEC mode command.

An SNMP EngineID has to be defined to add SNMP users to the device. Changing or removing the SNMP EngineID value deletes SNMPv3 users from the device's database.

The remote engineid designates the remote management station and should be defined to enable the device to receive informs.

Example

The following example configures an SNMPv3 user **John** in group **user-group**.

```
Console(config)# snmp-server user John user-group
```

Related Commands

show snmp users

snmp-server engineID local

The **snmp-server engineID local** Global Configuration mode command specifies the Simple Network Management Protocol (SNMP) engineID on the local device. To remove the configured engine ID, use the **no** form of this command.

Syntax

snmp-server engineID local {*engineid-string* | **default**}

no snmp-server engineID local

Parameters

- *engineid-string* — Specifies a character string that identifies the engine ID. (Range: 5-32 characters)
- **default** — The engine ID is created automatically based on the device MAC address.

Default Setting

The engine ID is not configured.

If SNMPv3 is enabled using this command, and the default is specified, the default engine ID 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.

Command Mode

Global Configuration mode

Command Usage

To use SNMPv3, you have to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device.

If the SNMPv3 engine ID is deleted or the configuration file is erased, SNMPv3 cannot be used. By default, SNMPv1/v2 are enabled on the device. SNMPv3 is enabled only by defining the Local Engine ID.

If you want to specify your own ID, you do not have to specify the entire 32-character engine ID if it contains trailing zeros. Specify only the portion of the engine ID up to the point where just zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify snmp-server engineID local 1234.

Since the engine ID should be unique within an administrative domain, the following is recommended:

For a standalone device, use the default keyword to configure the engine ID.

For a stackable system, configure the engine ID and verify its uniqueness.

Changing the value of the engine ID has the following important side-effect. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The user’s command line password is then destroyed, as required by RFC 2274. As a result, the security digests of SNMPv3 users become invalid if the local value of the engine ID change, and the users will have to be reconfigured.

You cannot specify an engine ID that consists of all 0x0, all 0xF or 0x000000001.

The **show running-config** Privileged EXEC mode command does not display the SNMP engine ID configuration. To see the SNMP engine ID configuration, enter the **snmp-server engineID local** GlobalConfiguration mode command.

Example

The following example enables SNMPv3 on the device and sets the local engine ID of the device to the default value.

```
Console(config) # snmp-server engineID local default
```

Related Commands

show snmp engineid

snmp-server enable traps

The **snmp-server enable traps** Global Configuration mode command enables the device to send SNMP traps. To disable SNMP traps, use the **no** form of the command.

Syntax

snmp-server enable traps

no snmp-server enable traps

Default Setting

SNMP traps are enabled.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables SNMP traps.

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

Related Commands

show snmp

snmp-server filter

The **snmp-server filter** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server filter entry. To remove the specified SNMP server filter entry, use the **no** form of this command.

Syntax

snmp-server filter *filter-name oid-tree* {**included | excluded**}

no snmp-server filter *filter-name* [*oid-tree*]

Parameters

- *filter-name* — Specifies the label for the filter record that is being updated or created. The name is used to reference the record.
  (Range: 1-30 characters)
- *oid-tree* — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included** — Indicates that the filter type is included.
- **excluded** — Indicates that the filter type is excluded.

Default Setting

No filter entry exists.

Command Mode

Global Configuration mode

Command Usage

This command can be entered multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

Example

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
Console(config)# snmp-server filter filter-name system included
Console(config)# snmp-server filter filter-name system.7 excluded
Console(config)# snmp-server filter filter-name ifEntry.*.1 included
```

Related Commands

show snmp filters

snmp-server host

The **snmp-server host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 1 or Version 2 notifications. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server host {*ip-address* **|** *hostname***}** *community-string* **[traps | informs] [1 | 2] [udp-port** *port***] [filter** *filtername***] [timeout** *seconds***] [retries** *retries***]**

no snmp-server host {*ip-address* **|** *hostname***} [traps | informs]**

Parameters

- *ip-address* — Specifies the IP address of the host (targeted recipient).
- *hostname* — Specifies the name of the host. (Range:1-158 characters)
- *community-string* — Specifies a password-like community string sent with the notification operation. (Range: 1-20)
- **traps** — Indicates that SNMP traps are sent to this host. If unspecified, SNMPv2 traps are sent to the host.
- **informs** — Indicates that SNMP informs are sent to this host. Not applicable to SNMPv1.
- **1** — Indicates that SNMPv1 traps will be used.
- **2** — Indicates that SNMPv2 traps will be used. If
- *port* — Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range:1-65535)
- *filtername* — Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- *seconds* — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is 15 seconds. (Range: 1-300)
- retries — Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is 3. (Range: 1-255)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

When configuring an SNMPv1 or SNMPv2 notification recipient, a notification view for that recipient is automatically generated for all the MIB.

When configuring an SNMPv1 notification recipient, the **Inform** option cannot be selected.

If a trap and inform are defined on the same target, and an inform was sent, the trap is not sent.

Example

The following example enables SNMP traps for host 10.1.1.1 with community string "management" using SNMPv2.

```
Console(config)# snmp-server host 10.1.1.1 management 2
```

Related Commands

show snmp

snmp-server v3-host

The **snmp-server v3-host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server v3-host {*ip-address* **|** *hostname***}** *username* **[traps | informs] {noauth | auth | priv} [udp-port** *port***] [filter** *filtername***] [timeout** *seconds***] [retries** *retries***]**

no snmp-server v3-host {*ip-address* **|** *hostname***}** *username* **[traps | informs]**

Parameters

- *ip-address* — Specifies the IP address of the host (targeted recipient).
- *hostname* — Specifies the name of the host. (Range:1-158 characters)
- *username* — Specifies the name of the user to use to generate the notification. (Range: 1-25)
- **traps** — Indicates that SNMP traps are sent to this host.
- **informs** — Indicates that SNMP informs are sent to this host.
- **noauth** — Indicates no authentication of a packet.
- **auth** — Indicates authentication of a packet without encrypting it.
- **priv** — Indicates authentication of a packet with encryption.
- *port* — Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range: 1-65535)
- *filtername* — Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- *seconds* — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is 15 seconds. (Range: 1-300)
- *retries* — Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is 3. (Range: 1-255)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

A user and notification view are not automatically created. Use the **snmp-server user**, **snmp-server group** and **snmp-server view** Global Configuration mode commands to generate a user, group and notify group, respectively.

Example

The following example configures an SNMPv3 host.

```
Console(config)# snmp-server v3-host 192.168.0.20 john noauth
```

Related Commands

show snmp

snmp-server trap authentication

The **snmp-server trap authentication** Global Configuration mode command enables the device to send SNMP traps when authentication fails. To disable SNMP failed authentication traps, use the **no** form of this command.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Default Setting

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables SNMP failed authentication traps.

```
Console(config)# snmp-server trap authentication
```

Related Commands

show snmp

snmp-server contact

The **snmp-server contact** Global Configuration mode command configures the system contact (sysContact) string. To remove system contact information, use the **no** form of the command.

Syntax

snmp-server contact *text*

no snmp-server contact

Parameters

- *text* — Specifies the string that describes system contact information. (Range: 0-160 characters)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Do not include spaces in the text string or place text that includes spaces inside quotation marks.

Example

The following example configures the system contact point called **Alcatel_Technical_Support**.

```
console(config)# snmp-server contact Alcatel_Technical_Support
```

Related Commands

show snmp

snmp-server location

The **snmp-server location** Global Configuration mode command configures the system location string. To remove the location string, use the **no** form of this command.

Syntax

snmp-server location *text*

no snmp-server location

Parameters

- *text* — Specifies a string that describes system location information. (Range: 0-160 characters)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Do not include spaces in the text string or place text that includes spaces inside quotation marks.

Example

The following example defines the device location as **New_York**.

```
Console(config)# snmp-server location New_York
```

Related Commands

show snmp

snmp-server set

The **snmp-server set** Global Configuration mode command defines the SNMP MIB value.

Syntax

snmp-server set *variable-name name1 value1* [*name2 value2 …*]

Parameters

- *variable-name* — MIB variable name.
- *name value* — List of name and value pairs. In the case of scalar MIBs, only a single pair of name values. In the case of an entry in a table, at least one pair of name and value followed by one or more fields.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Although the CLI can set any required configuration, there might be a situation where a SNMP user sets a MIB variable that does not have an equivalent command. In order to generate configuration files that support those situations, the **snmp-server set** command is used.

This command is case-sensitive.

Example

The following example configures the scalar MIB sysName with the value **Alcatel**.

```
Console(config)# snmp-server set sysName sysname Alcatel
```

Related Commands

show snmp

show snmp

The **show snmp** Privileged EXEC mode command displays the SNMP status.

Syntax

show snmp

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the SNMP communications status.

```
Console# show snmp


Communit    Community-Ac    View name   IP
y-String    cess                        address

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

public      read only       user-view   All

private     read write      Default     172.16.1.1

private     su              DefaultSu   172.17.1.1
                            per


Community-stri              Group       IP address
ng                          name

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

public                      user-grou   all
                            p


Traps are enabled.

Authentication trap is enabled.


Version 1,2 notifications

Target Address    Type     Community   Version    UDP     Filter   TO     Retri
                                                  Port    Name     Sec    es

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

192.122.173.42    Trap     public      2          162              15     3

192.122.173.42    Inform   public      2          162              15     3


Version 3 notifications

Target Address    Type     Username    Security   UDP     Filter   TO     Retri
                                       Level      Port    Name     Sec    es

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

192.122.173.42    Inform   Bob         Priv       162              15     3
```

```
System Contact: Robert

System Location: Marketing
```

The following table describes significant fields shown above.

Field	Description
Community-string	Community access string to permit access to the SNMP protocol.
Community-access	Type of access - read-only, read-write, super access
IP Address	Management station IP Address.
Trap-Rec-Address	Targeted Recipient
Trap-Rec-Community	Statistics sent with the notification operation.
Version	SNMP version for the sent trap 1 or 2.

Related Commands

snmp-server user

snmp-server engineID local

snmp-server enable traps

snmp-server filter

snmp-server host

snmp-server v3-host

snmp-server trap authentication

snmp-server contact

snmp-server location

snmp-server set

show snmp engineid

The **show snmp engineID** Privileged EXEC mode command displays the ID of the local Simple Network Management Protocol (SNMP) engine.

Syntax

show snmp engineID

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the SNMP engine ID.

```
Console# show snmp engineID

Local SNMP engineID: 08009009020C0B099C075878
```

Related Commands

snmp-server engineID local

show snmp views

The **show snmp views** Privileged EXEC mode command displays the configuration of views.

Syntax

show snmp views [*viewname***]**

Parameters

- *viewname* — Specifies the name of the view. (Range: 1-30)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the configuration of views.

```
Console# show snmp views


Name                 OID Tree                                 Type

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

user-view            iso                                      Included

user-view            snmpNotificationMIB                      Excluded

user-view            usmUser                                  Included
```

Related Commands

snmp-server view

show snmp groups

The **show snmp groups** Privileged EXEC mode command displays the configuration of groups.

Syntax

show snmp groups [*groupname*]

Parameters

- *groupname*—Specifies the name of the group. (Range: 1-30)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the configuration of views.

```
Console# show snmp groups


Name              Security               Views
                  Model      Level       Read      Write     Notify
--------------    -----      -----       -------   -------   -------
user-group        V3         priv        Default   ""        ""
managers-group    V3         priv        Default   Default   ""
managers-group    V3         priv        Default   ""        ""
```

The following table describes significant fields shown above.

Field	Description
Name	Name of the group.
Security Model	SNMP model in use (v1, v2 or v3).
Security Level	Authentication of a packet with encryption. Applicable only to the SNMP v3 security model.
Views Read	Name of the view that enables only viewing the contents of the agent. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.

Write	Name of the view that enables entering data and managing the contents of the agent.
Notify	Name of the view that enables specifying an inform or a trap.

Related Commands

snmp-server group

show snmp filters

The **show snmp filters** Privileged EXEC mode command displays the configuration of filters.

Syntax

show snmp filters [*filtername***]**

Parameters

- *filtername*—Specifies the name of the filter. (Range: 1-30)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the configuration of filters.

```
Console# show snmp filters


Name                OID Tree                   Type

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

user-filter         1.3.6.1.2.1.1              Included

user-filter         1.3.6.1.2.1.1.7            Excluded

user-filter         1.3.6.1.2.1.2.2.1.*.1      Included
```

Related Commands

snmp-server filter

show snmp users

The **show snmp users** Privileged EXEC mode command displays the configuration of users.

Syntax

show snmp users [*username*]

Parameters

- *username*—Specifies the name of the user. (Range: 1-30)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the configuration of users.

```
Console# show snmp users

Name      Group name      Auth Method     Remote
------    ------------    ---------       -------------------------
John      user-group      md5
John      user-group      md5             08009009020C0B099C075879
```

Related Commands

snmp-server user

Spanning-Tree Commands

Table 4-28. Spanning-Tree Commands

Command	Function	Mode	Page
spanning-tree	Enables spanning-tree functionality. To disable spanning-tree functionality, use the **no** form of this command.	GC	4-539
spanning-tree mode	Configures the spanning-tree protocol. To return to the default configuration, use the **no** form of this command.	GC	4-540
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. To return to the default configuration, use the **no** form of this command.	GC	4-541
spanning-tree hello-time	Configures the spanning tree bridge hello time, which is how often the device broadcasts hello messages to other devices.To return to the default configuration, use the **no** form of this command.t	GC	4-542
spanning-tree max-age	Configures the spanning tree bridge maximum age. To return to the default configuration, use the **no** form of this command.	GC	4-543
spanning-tree priority	Configures the spanning tree priority of the device. The priority value is used to determine which bridge is elected as the root bridge. To return to the default configuration, use the **no** form of this command.	GC	4-544
spanning-tree disable	Disables spanning tree on a specific port. To enable spanning tree on a port, use the **no** form of this command.	IC	4-544
spanning-tree costt	Configures the spanning tree path cost for a port. To return to the default configuration, use the **no** form of this command.	IC	4-545
spanning-tree port-priority	Configures port priority. To return to the default configuration, use the **no** form of this command.	IC	4-546
spanning-tree portfast	Enables PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup without waiting for the standard forward time delay. To disable PortFast mode, use the **no** form of this command.	IC	4-547
spanning-tree link-type	Overrides the default link-type setting determined by the duplex mode of the port and enables Rapid Spanning Tree Protocol (RSTP) transitions to the forwarding state. To return to the default configuration, use the **no** form of this command.	IC	4-548
spanning-tree pathcost method	Sets the default path cost method. To return to the default configuration, use the **no** form of this command.	GC	4-549
spanning-tree bpdu	Defines BPDU handling when the spanning tree is disabled globally or on a single interface. To return to the default configuration, use the **no** form of this command.	GC	4-550
clear spanning-tree detected-protocols	Restarts the protocol migration process (forces renegotiation with neighboring devices) on all interfaces or on a specified interface.	PE	4-551
spanning-tree mst priority	Configures the device priority for the specified spanning-tree instance. To return to the default configuration, use the **no** form of this command.	GC	4-551

Table 4-28. Spanning-Tree Commands

Command	Function	Mode	Page
spanning-tree mst max-hops	Configures the number of hops in an MST region before the BPDU is discarded and the port information is aged out. To return to the default configuration, use the **no** form of this command.	GC	4-552
spanning-tree mst port-priority	Configures port priority for the specified MST instance. To return to the default configuration, use the **no** form of this command.	IC	4-553
spanning-tree mst cost	Configures the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To return to the default configuration, use the **no** form of this command.	IC	4-554
spanning-tree mst configuration	Enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.	GC	4-556
instance (mst)	Maps VLANS to an MST instance.	MST	4-556
name (mst)	Defines the configuration name. To return to the default setting, use the no form of this command.	MST	4-558
revision (mst)	Defines the configuration revision number. To return to the default configuration, use the **no** form of this command.	MST	4-558
show (mst)	Displays the current or pending MST region configuration.	MST	4-559
exit (mst)	Exits the MST configuration mode and applies all configuration changes.	MST	4-561
abort (mst)	Exits the MST configuration mode without applying the configuration changes.	MST	4-561
spanning-tree guard root	Enables root guard on all spanning tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. To disable root guard on the interface, use the **no** form of this command.	IC	4-562
spanning-tree bpduguard	Use the spanning-tree bpduguard interface configuration command to shutdown an interface when it receives a bridge protocol data unit (BPDU).	IC	4-563
dot1x bpdu	Use the dot1x bpdu global configuration command to define 802.1x BPDU handling when 802.1x is globally disabled.	GC	4-563
show dot1x bpdu	Use the show dot1x bpdu EXEC command to display the 802.1x BPDU handling when 802.1x is globally disabled.	UE	4-564
show spanning-tree	Displays spanning-tree configuration.	PE	4-564

spanning-tree

The **spanning-tree** Global Configuration mode command enables spanning-tree functionality. To disable spanning-tree functionality, use the **no** form of this command.

Syntax

spanning-tree

no spanning-tree

Default Setting

Spanning-tree is enabled.

Command Modes

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables spanning-tree functionality.

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

Related Commands

spanning-tree mode

show spanning-tree

spanning-tree mode

The **spanning-tree mode** Global Configuration mode command configures the spanning-tree protocol. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mode {**stp** | **rstp**| **mstp**}

no spanning-tree mode

Parameters

- **stp** — Indicates that the Spanning Tree Protocol (STP) is enabled.
- **rstp** — Indicates that the Rapid Spanning Tree Protocol (RSTP) is enabled.
- **mstp** — Indicates that the Multiple Spanning Tree Protocol (RSTP) is enabled.

Default Setting

STP is enabled.

Command Modes

Global Configuration mode

Command Usage

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP and uses STP when the neighbor device uses STP.

Example

The following example configures the spanning-tree protocol to RSTP.

```
console(config)# spanning-tree mode rstp
```

Related Commands

spanning-tree

show spanning-tree

spanning-tree forward-time

The **spanning-tree forward-time** Global Configuration mode command 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. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

Parameters

- *seconds* — Time in seconds. (Range: 4 - 30)

Default Setting

The default forwarding time for the IEEE Spanning Tree Protocol (STP) is 15 seconds.

Command Modes

Global Configuration mode

Command Usage

When configuring the forwarding time, the following relationship should be kept:

2*(Forward-Time - 1) >= Max-Age

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
Console(config)# spanning-tree forward-time 25
```

Related Commands

spanning-tree hello-time

spanning-tree max-age

spanning-tree priority

spanning-tree disable

spanning-tree cost

spanning-tree port-priority

spanning-tree portfast

spanning-tree link-type

show spanning-tree

spanning-tree hello-time

The **spanning-tree hello-time** Global Configuration mode command configures the spanning tree bridge hello time, which is how often the device broadcasts hello messages to other devices.To return to the default configuration, use the **no** form of this command.

Syntax

s**panning-tree hello-time** *seconds*

no spanning-tree hello-time

Parameters

- *seconds* — Time in seconds. (Range: 1 - 10)

Default Setting

The default hello time for IEEE Spanning Tree Protocol (STP) is 2 seconds.

Command Modes

Global Configuration mode

Command Usage

When configuring the hello time, the following relationship should be kept:

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures spanning tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```

Related Commands

spanning-tree forward-time

spanning-tree max-age

spanning-tree priority

spanning-tree disable

spanning-tree cost

spanning-tree port-priority

spanning-tree portfast

spanning-tree link-type

show spanning-tree

spanning-tree max-age

The **spanning-tree max-age** Global Configuration mode command configures the spanning tree bridge maximum age. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

Parameters

- *seconds* — Time in seconds. (Range: 6 - 40)

Default Setting

The default maximum age for IEEE Spanning Tree Protocol (STP) is 20 seconds.

Command Modes

Global Configuration mode

Command Usage

When configuring the maximum age, the following relationships should be kept:

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures the spanning tree bridge maximum-age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```

Related Commands

spanning-tree forward-time

spanning-tree hello-time

spanning-tree priority

spanning-tree disable

spanning-tree cost

spanning-tree port-priority

spanning-tree portfast

spanning-tree link-type

show spanning-tree

spanning-tree priority

The **spanning-tree priority** Global Configuration mode command configures the spanning tree priority of the device. The priority value is used to determine which bridge is elected as the root bridge. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

Parameters

- *priority* — Priority of the bridge. (Range: 0 - 61440 in steps of 4096)

Default Setting

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

Command Modes

Global Configuration mode

Command Usage

The bridge with the lowest priority is elected as the root bridge.

Example

The following example configures spanning tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```

Related Commands

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-age

spanning-tree disable

spanning-tree cost

spanning-tree port-priority

spanning-tree portfast

spanning-tree link-type

show spanning-tree

spanning-tree disable

The **spanning-tree disable** Interface Configuration mode command disables spanning tree on a specific port. To enable spanning tree on a port, use the **no** form of this command.

Syntax

spanning-tree disable

no spanning-tree disable

Default Setting

Spanning tree is enabled on all ports.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example disables spanning-tree on Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# spanning-tree disable
```

Related Commands

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-age

spanning-tree priority

spanning-tree cost

spanning-tree port-priority

spanning-tree portfast

spanning-tree link-type

show spanning-tree

spanning-tree cost

The **spanning-tree cost** Interface Configuration mode command configures the spanning tree path cost for a port. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

Parameters

- *cost* — Path cost of the port (Range: 1 - 200,000,000)

Default Setting

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Command Usage

The path cost method is configured using the **spanning-tree pathcost method** Global Configuration mode command.

Example

The following example configures the spanning-tree cost on Ethernet port 1/e15 to 35000.

```
Console(config)# interface ethernet 1/e15
Console(config-if)# spanning-tree cost 35000
```

Related Commands

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-age

spanning-tree priority

spanning-tree disable

spanning-tree port-priority

spanning-tree portfast

spanning-tree link-type

show spanning-tree

spanning-tree port-priority

The **spanning-tree port-priority** Interface Configuration mode command configures port priority. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

Parameters

- *priority* — The priority of the port. (Range: 0 - 240 in multiples of 16)

Default Setting

The default port priority for IEEE Spanning TreeProtocol (STP) is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the spanning priority on Ethernet port 1/e15 to 96.

```
Console(config)# interface ethernet 1/e15
Console(config-if)# spanning-tree port-priority 96
```

Related Commands

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-age

spanning-tree priority

spanning-tree disable

spanning-tree cost

spanning-tree portfast

spanning-tree link-type

show spanning-tree

spanning-tree portfast

The **spanning-tree portfast** Interface Configuration mode command enables PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup without waiting for the standard forward time delay. To disable PortFast mode, use the **no** form of this command.

Syntax

spanning-tree portfast [auto]

no spanning-tree portfast

Parameters

- **auto** — Specifies that the software waits for 3 seconds (with no BPDUs received on the interface) before putting the interface into PortFast mode.

Default Setting

PortFast mode is disabled.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Command Usage

This feature should be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt device and network operations.

An interface with PortFast mode enabled is moved directly to the spanning tree forwarding state when linkup occurs without waiting the standard forward-time delay.

Example

The following example enables PortFast on Ethernet port 1/e15**.**

```
Console(config)# interface ethernet 1/e15
Console(config-if)# spanning-tree portfast
```

Related Commands

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-age

spanning-tree priority

spanning-tree disable

spanning-tree cost

spanning-tree port-priority

spanning-tree link-type

show spanning-tree

spanning-tree link-type

The **spanning-tree link-type** Interface Configuration mode command overrides the default link-type setting determined by the duplex mode of the port and enables Rapid Spanning Tree Protocol (RSTP) transitions to the forwarding state. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree spanning-tree link-type

Parameters

- **point-to-point** — Indicates that the port link type is point-to-point.

- **shared** — Indicates that the port link type is shared.

Default Setting

The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables shared spanning-tree on Ethernet port 1/e5**.**

```
Console(config)# interface ethernet 1/e15
Console(config-if)# spanning-tree link-type shared
```

Related Commands

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-age

spanning-tree priority

spanning-tree disable

spanning-tree cost

spanning-tree port-priority

spanning-tree portfast

show spanning-tree

spanning-tree pathcost method

The **spanning-tree pathcost method** Global Configuration mode command sets the default path cost method. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

Parameters

- *long* — Specifies port path costs with a range of 1-200,000,000 .
- *short* — Specifies port path costs with a range of 1-65,535.

Default Setting

Short path cost method.

Command Mode

Global Configuration mode

Command Usage

This command applies to all spanning tree instances on the device.

The cost is set using the **spanning-tree cost** command.

Example

The following example sets the default path cost method to **long**.

```
Console(config)# spanning-tree pathcost method long
```

Related Commands

show spanning-tree

spanning-tree bpdu

The **spanning-tree bpdu** Global Configuration mode command defines BPDU handling when the spanning tree is disabled globally or on a single interface. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree bpdu {**filtering** | **flooding** | **bridging**}

no spanning-tree bpdu

Parameters

- *filtering* — When Spanning Tree is disabled on an interface, BPDU packets are filtered.
- *flooding* — When Spanning Tree is disabled on an interface, untagged BPDU packets are flooded unconditionally (Without applying VLAN rules), to all ports which have Spanning Tree disabled.
- *bridging* — When Spanning Tree is globally disabled, untagged or tagged BPDU packets are flooded, and are subject to ingress and egress VLAN rules. This mode is not relevant if Spanning Tree is disabled only on a group of ports.

Default Setting

The default setting is flooding.

Command Modes

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example defines BPDU packet flooding when the spanning-tree is disabled on an interface.

```
Console(config)# spanning-tree bpdu flooding
```

Related Commands

show spanning-tree

clear spanning-tree detected-protocols

The **clear spanning-tree detected-protocols** Privileged EXEC mode command restarts the protocol migration process (forces renegotiation with neighboring devices) on all interfaces or on a specified interface.

Syntax

clear spanning-tree detected-protocols [**ethernet** *interface* **|** **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Modes

Privileged EXEC mode

Command Usage

This feature should be used only when working in RSTP or MSTP mode.

Example

The following example restarts the protocol migration process on Ethernet port 1/e11.

```
Console# clear spanning-tree detected-protocols ethernet 1/e11
```

Related Commands

show spanning-tree

spanning-tree mst priority

The **spanning-tree mst priority** Global Configuration mode command configures the device priority for the specified spanning-tree instance. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree ***mst*** *instance-id* **priority**

Parameters

- *instance-id* — ID of the spanning -tree instance. (Range: 1-Product Specific upper limit)
- *priority* — Device priority for the specified spanning-tree instance. (Range: 0-61440 in multiples of 4096)

Default Setting

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

Command Mode

Global Configuration mode

Command Usage

The device with the lowest priority is selected as the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
Console (config) # spanning-tree mst 1 priority 4096
```

Related Commands

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

name (mst)

revision (mst)

show (mst)

exit (mst)

abort (mst)

show spanning-tree

spanning-tree mst max-hops

The **spanning-tree mst priority** Global Configuration mode command configures the number of hops in an MST region before the BPDU is discarded and the port information is aged out. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Parameters

- *hop-count* — Number of hops in an MST region before the BPDU is discarded. (Range: 1-40)

Default Setting

The default number of hops is 20.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
Console (config) # spanning-tree mst max-hops 10
```

Related Commands

spanning-tree mst priority

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

name (mst)

revision (mst)

show (mst)

exit (mst)

abort (mst)

show spanning-tree

spanning-tree mst port-priority

The **spanning-tree mst port-priority** Interface Configuration mode command configures port priority for the specified MST instance. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Parameters

- *instance-ID* — ID of the spanning tree instance.

(Range: 1-Product Specific upper limit)

- *priority* — The port priority. (Range: 0 - 240 in multiples of 16)

Default Setting

The default port priority for IEEE Multiple Spanning Tree Protocol (MSTP) is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the port priority of port g1 to 142.

```
Console(config)# interface ethernet g1
Console(config-if)# spanning-tree mst 1 port-priority 142
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

name (mst)

revision (mst)

show (mst)

exit (mst)

abort (mst)

show spanning-tree

spanning-tree mst cost

The **spanning-tree mst cost** Interface Configuration mode command configures the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Parameters

- *instance-ID* — ID of the spanning -tree instance (Range: 1-16).
- *cost* — The port path cost. (Range: 1 - 200,000,000)

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Modes

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the MSTP instance 1 path cost for Ethernet port 1/e9 to 4.

```
Console(config) # interface ethernet 1/e9
Console(config-if) # spanning-tree mst 1 cost 4
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst configuration

instance (mst)

name (mst)

revision (mst)

show (mst)

exit (mst)

abort (mst)

show spanning-tree

spanning-tree mst configuration

The **spanning-tree mst configuration** Global Configuration mode command enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.

Syntax

spanning-tree mst configuration

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

All devices in an MST region must have the same VLAN mapping, configuration revision number and name.

Example

The following example configures an MST region.

```
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
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

instance (mst)

name (mst)

revision (mst)

show (mst)

exit (mst)

abort (mst)

show spanning-tree

instance (mst)

The **instance** MST Configuration mode command maps VLANS to an MST instance.

Syntax

instance *instance-id* **{add | remove} vlan** *vlan-range*

Parameters

- *instance-ID* — ID of the MST instance.
  (Range: 1-Product Specific upper limit)
- *vlan-range* — VLANs to be added to or removed from the specified MST instance. To specify a range of VLANs, use a hyphen. To specify a series of VLANs, use a comma. (Range: 1-4094)

Default Setting

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Modes

MST Configuration mode

Command Usage

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 add vlan 10-20
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

name (mst)

revision (mst)

show (mst)

exit (mst)

abort (mst)

show spanning-tree

name (mst)

The **name** MST Configuration mode command defines the configuration name. To return to the default setting, use the **no** form of this command.

Syntax

name *string*

no name

Parameters

- *string* — MST configuration name. Case-sensitive (Range: 1-32 characters).

Default Setting

The default name is a bridge ID.

Command Mode

MST Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example defines the configuration name as region1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # name region 1
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

revision (mst)

show (mst)

exit (mst)

abort (mst)

show spanning-tree

revision (mst)

The **revision** MST configuration command defines the configuration revision number. To return to the default configuration, use the **no** form of this command.

Syntax

revision *value*

no revision

Parameters

- *value* — Configuration revision number (Range: 0-65535).

Default Setting

The default configuration revision number is 0.

Command Mode

MST Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example sets the configuration revision to 1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # revision 1
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

name (mst)

show (mst)

exit (mst)

abort (mst)

show spanning-tree

show (mst)

The **show** MST Configuration mode command displays the current or pending MST region configuration.

Syntax

show {current | pending}

Parameters

- **current** — Indicates the current region configuration.
- **pending** — Indicates the pending region configuration.

Default Setting

This command has no default configuration.

Command Mode

MST Configuration mode

Command Usage

The pending MST region configuration takes effect only after exiting the MST configuration mode.

Example

The following example displays a pending MST region configuration.

```
Console(config-mst)# show pending

Pending MST configuration

Name: Region1

Revision: 1

Instance          Vlans Mapped                State

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

0                 1-9,21-4094                 Enabled

1                 10-20                       Enabled
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

name (mst)

revision (mst)

exit (mst)

abort (mst)

show spanning-tree

exit (mst)

The **exit** MST Configuration mode command exits the MST configuration mode and applies all configuration changes.

Syntax

exit

Default Setting

This command has no default configuration.

Command Mode

MST Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example exits the MST configuration mode and saves changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # exit
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

name (mst)

revision (mst)

show (mst)

abort (mst)

show spanning-tree

abort (mst)

The **abort** MST Configuration mode command exits the MST configuration mode without applying the configuration changes.

Syntax

abort

Default Setting

This command has no default configuration.

Command Mode

MST Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example exits the MST configuration mode without saving changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # abort
```

Related Commands

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

name (mst)

revision (mst)

show (mst)

exit (mst)

show spanning-tree

spanning-tree guard root

The **spanning-tree guard root** Interface Configuration (Ethernet, port-channel) mode command enables root guard on all spanning tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. To disable root guard on the interface, use the **no** form of this command.

Syntax

spanning-tree guard root

no spanning-tree guard root

Default Setting

Root guard is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

Root guard can be enabled when the device operates in STP, RSTP and MSTP.

When root guard is enabled, the port changes to the alternate state if spanning-tree calculations selects the port as the root port.

Examples

The following example prevents Ethernet port 1/g1 from being the root port of the device.

```
Console(config) # interface ethernet 1/g1
Console(config-mst) # spanning-tree guard root
```

Related Commands

show spanning-tree

spanning-tree bpduguard

The **spanning-tree bpduguard** Interface Configuration (Ethernet, port-channel) mode command shutdowns an interface when it receives a bridge protocol data unit (BPDU). To restore the default configuration, use the **no** form of this command.

Syntax

spanning-tree bpduguard

no spanning-tree bpduguard

Default Configuration

The default configuration is set to disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

You can enable the command when the spanning tree is enabled (useful when the port is in the PortFast mode) or disabled.

dot1x bpdu

Use the dot1x bpdu global configuration command to define 802.1x BPDU handling when 802.1x is globally disabled. Use the no form of this command to return to default.

Syntax

dot1x bpdu {filtering | bridging}

no dot1x bpdu

Parameters

- **filtering** — Specify that when 802.1x is globally disabled, 802.1x BPDU packets would be filtered.

- **bridging** — Specify that when 802.1x is globally disabled, 802.1x BPDU packets would be bridged.

Default

Filtering

Command Modes

Global configuration

Usage Guidelines

According to IEEE802.1 standards the 802.1X BPDUs should never be forwarded - The 802.1X BPDUs should be handled by the software in case 802.1X is enabled on the ingress port, or discarded in all other cases.

This feature enables to bridge 802.1X BPDUs packets as data packets.

The feature can be enabled only when 802.1X is globally disabled (by the no dot1x system-auth-control global configuration command). If the port is disabled for 802.1X but 802.1X is enabled globally, 802.1X BPDUs would always be discarded.

show dot1x bpdu

Use the show dot1x bpdu EXEC command to display the 802.1x BPDU handling when 802.1x is globally disabled.

Syntax

```
show dot1x bpdu
```

Command Modes

EXEC

Usage Guidelines

There are no usage guidelines for this command

Examples

```
Switch# show dot1x bpdu
802.1X BPDU packets are trapped for the 802.1X protocol.

Switch# show dot1x bpdu
802.1X BPDU packets are filtered.

Switch# show dot1x bpdu
802.1X BPDU packets are bridged.
```

show spanning-tree

The **show spanning-tree** Privileged EXEC mode command displays spanning-tree configuration.

Syntax

show spanning-tree [ethernet *interface -number*| **port-channel** *port-channel-number*] [**instance** instance-id]

show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** instance-id]

show spanning-tree mst-configuration

Parameters

- *interface-number* — A valid Ethernet port.
- *port-channel-number* — A valid port channel number.
- **detail** — Indicates detailed information.
- **active** — Indicates active ports only.
- **blockedports** — Indicates blocked ports only.
- **mst-configuration** — Indicates the MST configuration identifier.
- *instance-id* — Specifies the ID of the spanning tree instance (The range lower limit is 0. The upper limit is product-specific).

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays spanning-tree information.

```
Console# show spanning-tree



Spanning tree enabled mode RSTP

Default port cost method: long



Root    Priority                32768
ID

        Address                 00:01:42:97:e0:00

        Path                    20000
        Cost

        Root                    1 (1/
        Port                    e1)

        Hello Time 2 sec        Max Age 20     Forward Delay 15 sec
                                sec
```

```
Brid   Priority               36864
ge
ID

       Address                00:02:4b:29:7a:00

       Hello Time 2 sec       Max Age 20     Forward Delay 15 sec
                              sec


Interfaces

Name   State      Prio.Nbr   Cost    Sts   Role   PortFast   Type

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

1/e1   Enabled    128.1      20000   FWD   Root   No         P2p (RSTP)

1/e2   Enabled    128.2      20000   FWD   Desg   No         Shared (STP)

1/e3   Disabled   128.3      20000   -     -      -          -

1/e4   Enabled    128.4      20000   BLK   ALTN   No         Shared (STP)

1/e5   Enabled    128.5      20000   DIS   -      -          -


Console# show spanning-tree


Spanning tree enabled mode RSTP

Default port cost method: long


Root   Priority               36864
ID

       Address                00:02:4b:29:7a:00

       This switch is the root.

       Hello Time 2 sec       Max Age 20     Forward Delay 15 sec
                              sec


Interfaces

Name   State      Prio.Nbr   Cost    Sts   Role   PortFast   Type

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

1/e1   Enabled    128.1      20000   FWD   Desg   No         P2p (RSTP)

1/e2   Enabled    128.2      20000   FWD   Desg   No         Shared (STP)

1/e3   Disabled   128.3      20000   -     -      -          -

1/e4   Enabled    128.4      20000   FWD   Desg   No         Shared (STP)
```

```
1/e5   Enabled     128.5       20000   DIS    -       -          -


Console# show spanning-tree


Spanning tree disabled (BPDU filtering) mode RSTP

Default port cost method: long


Root   Priority               N/A
ID

       Address                N/A

       Path                   N/A
       Cost

       Root                   N/A
       Port

       Hello Time N/A         Max Age N/A    Forward Delay N/A


Brid   Priority               36864
ge
ID

       Address                00:02:4b:29:7a:00

       Hello Time 2 sec       Max Age 20     Forward Delay 15 sec
                              sec


Interfaces

Name   State       Prio.Nbr    Cost    Sts    Role    PortFast   Type

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

1/e1   Enabled     128.1       20000   -      -       -          -

1/e2   Enabled     128.2       20000   -      -       -          -

1/e3   Disabled    128.3       20000   -      -       -          -

1/e4   Enabled     128.4       20000   -      -       -          -

1/e5   Enabled     128.5       20000   -      -       -          -
```

```
Console# show spanning-tree active


Spanning tree enabled mode RSTP

Default port cost method: long


Root    Priority                32768
ID

        Address                 00:01:42:97:e0:00

        Path                    20000
        Cost

        Root                    1 (1/
        Port                    e1)

        Hello Time 2 sec        Max Age 20     Forward Delay 15 sec
                                sec


Brid    Priority                36864
ge
ID

        Address                 00:02:4b:29:7a:00

        Hello Time 2 sec        Max Age 20     Forward Delay 15 sec
                                sec


Interfaces

Name    State       Prio.Nbr    Cost     Sts    Role    PortFast    Type

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

1/e1    Enabled     128.1       20000    FWD    Root    No          P2p (RSTP)

1/e2    Enabled     128.2       20000    FWD    Desg    No          Shared (STP)

1/e4    Enabled     128.4       20000    BLK    ALTN    No          Shared (STP)
```

```
Console# show spanning-tree blockedports


Spanning tree enabled mode RSTP

Default port cost method: long


Root     Priority               32768
ID

         Address                00:01:42:97:e0:00

         Path                   20000
         Cost

         Root                   1 (1/
         Port                   1)

         Hello Time 2 sec       Max Age 20     Forward Delay 15 sec
                                sec


Brid     Priority               36864
ge
ID

         Address                00:02:4b:29:7a:00

         Hello Time 2 sec       Max Age 20     Forward Delay 15 sec
                                sec


Interfaces

Name     State       Prio.Nbr    Cost     Sts    Role    PortFast    Type

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

1/e4     Enabled     128.4       20000    BLK    ALTN    No          Shared (STP)
```

```
Console# show spanning-tree detail


Spanning tree enabled mode RSTP

Default port cost method: long


Root   Priority              32768
ID

       Address               00:01:42:97:e0:00

       Path                  20000
       Cost

       Root                  1 (1/
       Port                  e1)

       Hello Time 2 sec      Max Age 20    Forward Delay 15 sec
                             sec


Brid   Priority   36864
ge
ID

       Address               00:02:4b:29:7a:00

       Hello Time 2 sec      Max Age 20    Forward Delay 15 sec
                             sec


Number of topology changes 2 last change occurred 2d18h ago

Time   hold 1, topology change 35, notification 2
s:

       hello 2, max age 20, forward delay 15


Port 1 (1/e1) enabled

State: Forwarding                     Role: Root

Port id: 128.1                        Port cost: 20000

Type: P2p (configured: auto) RSTP     Port Fast: No (configured:no)

Designated bridge Priority: 32768     Address: 00:01:42:97:e0:00

Designated port id: 128.25            Designated path cost: 0

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638
```

```
Port 2 (1/e2) enabled
State: Forwarding                     Role: Designated
Port id: 128.2                        Port cost: 20000
Type: Shared (configured: auto) STP   Port Fast: No (configured:no)
Designated bridge Priority: 32768     Address: 00:02:4b:29:7a:00
Designated port id: 128.2             Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (1/e3) disabled
State: N/A                            Role: N/A
Port id: 128.3                        Port cost: 20000
Type: N/A (configured: auto)          Port Fast: N/A (configured:no)
Designated bridge Priority: N/A       Address: N/A
Designated port id: N/A               Designated path cost: N/A
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

Port 4 (1/e4) enabled
State: Blocking                       Role: Alternate
Port id: 128.4                        Port cost: 20000
Type: Shared (configured:auto) STP    Port Fast: No (configured:no)
Designated bridge Priority: 28672     Address: 00:30:94:41:62:c8
Designated port id: 128.25            Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 5 (1/e5) enabled
State: Disabled                       Role: N/A
Port id: 128.5                        Port cost: 20000
Type: N/A (configured: auto)          Port Fast: N/A (configured:no)
Designated bridge Priority: N/A       Address: N/A
Designated port id: N/A               Designated path cost: N/A
```

```
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

Console# show spanning-tree ethernet 1/e1
Port 1 (1/e1) enabled
State: Forwarding                     Role: Root
Port id: 128.1                        Port cost: 20000
Type: P2p (configured: auto) RSTP     Port Fast: No (configured:no)
Designated bridge Priority: 32768     Address: 00:01:42:97:e0:00
Designated port id: 128.25            Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Console# show spanning-tree mst-configuration


Name: Region1
Revision: 1
Instance           Vlans mapped       State
--------           ------------       ---
                                      ---
                                      -
0                  1-9, 21-4094       Ena
                                      ble
                                      d
1                  10-20              Ena
                                      ble
                                      d

Console# show spanning-tree


Spanning tree enabled mode MSTP
Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root ID        Priority   32768
```

```
                   Address     00:01:42:97:e0:00

                   Path        20000
                   Cost

                   Root        1 (1/
                   Port        e1)

                   Hello Time 2 sec    Max Age 20    Forward Delay 15 sec
                                       sec


IST Master ID      Priority    32768

                   Address     00:02:4b:29
                               :7a:00

                   This switch is the IST master.

                   Hello Time 2 sec    Max Age 20    Forward Delay 15 sec
                                       sec

                   Max hops    20


Interfaces

Name    State      Prio.Nbr    Cost     Sts    Role    PortFast    Type

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

1/e1    Enabled    128.1       20000    FWD    Root    No          P2p Bound
                                                                   (RSTP)

1/e2    Enabled    128.2       20000    FWD    Desg    No          Shared Bound
                                                                   (STP)

1/e3    Enabled    128.3       20000    FWD    Desg    No          P2p

1/e4    Enabled    128.4       20000    FWD    Desg    No          P2p


###### MST 1 Vlans Mapped: 10-20

CST Root ID        Priority    24576

                   Address     00:02:4b:29:89:76

                   Path        20000
                   Cost

                   Root        4 (1/
                   Port        e4)

                   Rem hops    19


Bridge ID          Priority    32768
```

```
                    Address     00:02:4b:29
                                :7a:00


Interfaces

Name    State        Prio.Nbr    Cost     Sts    Role    PortFast    Type

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

1/e1    Enabled      128.1       20000    FWD    Boun    No          P2p Bound
                                                                     (RSTP)

1/e2    Enabled      128.2       20000    FWD    Boun    No          Shared Bound
                                                                     (STP)

1/e3    Enabled      128.3       20000    BLK    Altn    No          P2p

1/e4    Enabled      128.4       20000    FWD    Desg    No          P2p


Console# show spanning-tree detail


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID         Priority    32768

                    Address     00:01:42:97:e0:00

                    Path        20000
                    Cost

                    Root        1 (1/
                    Port        e1)

                    Hello Time 2 sec    Max Age 20    Forward Delay 15 sec
                                        sec


IST Master ID       Priority    32768

                    Address     00:02:4b:29
                                :7a:00

                    This switch is the IST master.

                    Hello Time 2 sec    Max Age 20    Forward Delay 15 sec
                                        sec

                    Max hops    20

                    Number of topology changes 2 last change occurred 2d18h
                    ago
```

```
                   Times:  hold 1, topology change 35, notification 2
                   hello 2, max age 20, forward delay 15


Port 1 (1/e1) enabled

State: Forwarding                            Role: Root

Port id: 128.1                               Port cost: 20000

Type: P2p (configured: auto) Boundary RSTP   Port Fast: No (configured:no)

Designated bridge Priority: 32768            Address: 00:01:42:97:e0:00

Designated port id: 128.25                   Designated path cost: 0

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638


Port 2 (1/e2) enabled

State: Forwarding                            Role: Designated

Port id: 128.2                               Port cost: 20000

Type: Shared (configured: auto) Boundary     Port Fast: No (configured:no)
STP

Designated bridge Priority: 32768            Address: 00:02:4b:29:7a:00

Designated port id: 128.2                    Designated path cost: 20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 3 (1/e3) enabled

State: Forwarding                            Role: Designated

Port id: 128.3                               Port cost: 20000

Type: Shared (configured: auto) Internal     Port Fast: No (configured:no)

Designated bridge Priority: 32768            Address: 00:02:4b:29:7a:00

Designated port id: 128.3                    Designated path cost: 20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


Port 4 (1/e4) enabled

State: Forwarding                            Role: Designated
```

```
Port id: 128.4                              Port cost: 20000

Type: Shared (configured: auto) Internal    Port Fast: No (configured:no)

Designated bridge Priority: 32768           Address: 00:02:4b:29:7a:00

Designated port id: 128.2                   Designated path cost: 20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 170638


###### MST 1 Vlans Mapped: 10-20

Root ID            Priority    24576

                   Address     00:02:4b:29:89:76

                   Path        20000
                   Cost

                   Port        4 (1/
                   Cost        e4)

                   Rem hops    19


Bridge ID          Priority    32768

                   Address     00:02:4b:29:7a:00

                   Number of topology changes 2 last change occurred 1d9h ago

                   Times:  hold 1, topology change 2, notification 2
                   hello 2, max age 20, forward delay 15


Port 1 (1/e1) enabled

State: Forwarding                           Role: Boundary

Port id: 128.1                              Port cost: 20000

Type: P2p (configured: auto) Boundary RSTP  Port Fast: No (configured:no)

Designated bridge Priority: 32768           Address: 00:02:4b:29:7a:00

Designated port id: 128.1                   Designated path cost: 20000

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638
```

```
Port 2 (1/e2) enabled
State: Forwarding                            Role: Designated
Port id: 128.2                               Port cost: 20000
Type: Shared (configured: auto) Boundary     Port Fast: No (configured:no)
STP
Designated bridge Priority: 32768            Address: 00:02:4b:29:7a:00
Designated port id: 128.2                    Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (1/e3) disabled
State: Blocking                              Role: Alternate
Port id: 128.3                               Port cost: 20000
Type: Shared (configured: auto) Internal     Port Fast: No (configured:no)
Designated bridge Priority: 32768            Address: 00:02:4b:29:1a:19
Designated port id: 128.78                   Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 4 (1/e4) enabled
State: Forwarding                            Role: Designated
Port id: 128.4                               Port cost: 20000
Type: Shared (configured: auto) Internal     Port Fast: No (configured:no)
Designated bridge Priority: 32768            Address: 00:02:4b:29:7a:00
Designated port id: 128.2                    Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long
```

```
###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID        Priority   32768

                   Address    00:01:42:97:e0:00

                   Path       20000
                   Cost

                   Root       1 (1/
                   Port       e1)

                   Hello Time 2 sec    Max Age 20    Forward Delay 15 sec
                                       sec


IST Master ID      Priority   32768

                   Address    00:02:4b:19
                              :7a:00

                   Path       10000
                   Cost

                   Rem hops   19


Brid               Priority   32768
ge
ID

                   Address    00:02:4b:29
                              :7a:00

                   Hello Time 2 sec    Max Age 20    Forward Delay 15 sec
                                       sec

                   Max hops   20


Console# show spanning-tree


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID        Priority   32768

                   Address    00:01:42:97:e0:00

                   This switch is root for CST and IST master.

                   Root       1 (1/
                   Port       e1)
```

```
                    Hello Time 2 sec    Max Age 20   Forward Delay 15 sec
                                        sec

                    Max hops   20
```

Related Commands

spanning-tree

spanning-tree mode

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-age

spanning-tree priority

spanning-tree disable

spanning-tree cost

spanning-tree port-priority

spanning-tree portfast

spanning-tree link-type

spanning-tree pathcost method

spanning-tree bpdu

clear spanning-tree detected-protocols

spanning-tree mst priority

spanning-tree mst max-hops

spanning-tree mst port-priority

spanning-tree mst cost

spanning-tree mst configuration

instance (mst)

name (mst)

revision (mst)

show (mst)

exit (mst)

abort (mst)

spanning-tree guard root

SSH Commands

Table 4-29. SSH Commands

Command	Function	Mode	Page
ip ssh port	Specifies the port to be used by the SSH server. To return to the default configuration, use the **no** form of this command.	GC	4-580
ip ssh server	Enables the device to be configured from a SSH server. To disable this function, use the **no** form of this command.	GC	4-581
crypto key generate dsa	Generates DSA key pairs.	GC	4-581
crypto key generate rsa	Generates RSA key pairs.	GC	4-582
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions. To disable this function, use the **no** form of this command.	GC	4-583
crypto key pubkey-chain ssh	Enters the SSH Public Key-chain Configuration mode. The mode is used to manually specify other device public keys such as SSH client public keys.	GC	4-584
user-key	Specifies which SSH public key is manually configured. To remove an SSH public key, use the **no** form of this command.	SPK	4-585
key-string	Manually specifies an SSH public key.	SPK	4-586
show ip ssh	Displays the SSH server configuration.	PE	4-587
show crypto key mypubkey	Displays the SSH public keys on the device.	PE	4-588
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the device.	PE	4-589

ip ssh port

The **ip ssh port** Global Configuration mode command specifies the port to be used by the SSH server. To return to the default configuration, use the **no** form of this command.

Syntax

ip ssh port *port-number*

no ip ssh port

Parameters

- *port-number* — Port number for use by the SSH server (Range: 1 - 65535).

Default Setting

The default port number is 22.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example specifies the port to be used by the SSH server as 8080.

```
Console(config)# ip ssh port 8080
```

Related Commands

ip ssh server

show ip ssh

ip ssh server

The **ip ssh server** Global Configuration mode command enables the device to be configured from a SSH server. To disable this function, use the **no** form of this command.

Syntax

ip ssh server

no ip ssh server

Default Setting

Device configuration from a SSH server is enabled.

Command Mode

Global Configuration mode

Command Usage

If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the **crypto key generate dsa**, and **crypto key generate rsa** Global Configuration mode commands.

Example

The following example enables configuring the device from a SSH server.

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

Related Commands

ip ssh port

show ip ssh

crypto key generate dsa

The **crypto key generate dsa** Global Configuration mode command generates DSA key pairs.

Syntax

crypto key generate dsa

Default Setting

DSA key pairs do not exist.

Command Mode

Global Configuration mode

Command Usage

DSA keys are generated in pairs: one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys are displayed.

This command is not saved in the device configuration; however, the keys generated by this command are saved in the private configuration, which is never displayed to the user or backed up on another device.

DSA keys are saved to the backup master.

This command may take a considerable period of time to execute.

Example

The following example generates DSA key pairs.

```
Console(config)# crypto key generate dsa
```

Related Commands

crypto key generate rsa

ip ssh pubkey-auth

crypto key pubkey-chain ssh

user-key

key-string

show crypto key mypubkey

show crypto key pubkey-chain ssh

crypto key generate rsa

The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs.

Syntax

crypto key generate rsa

Default Setting

RSA key pairs do not exist.

Command Mode

Global Configuration mode

Command Usage

RSA keys are generated in pairs: one public RSA key and one private RSA key. If the device already has RSA keys, a warning and prompt to replace the existing keys with new keys are displayed.

This command is not saved in the device configuration; however, the keys generated by this command are saved in the private configuration which is never displayed to the user or backed up on another device.

RSA keys are saved to the backup master.

This command may take a considerable period of time to execute.

Example

The following example generates RSA key pairs.

```
Console(config)# crypto key generate rsa
```

Related Commands

crypto key generate dsa

ip ssh pubkey-auth

crypto key pubkey-chain ssh

user-key

key-string

show crypto key mypubkey

show crypto key pubkey-chain ssh

ip ssh pubkey-auth

The **ip ssh pubkey-auth** Global Configuration mode command enables public key authentication for incoming SSH sessions. To disable this function, use the **no** form of this command.

Syntax

ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Setting

Public Key authentication fo incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

Command Usage

AAA authentication is independent

Example

The following example enables public key authentication for incoming SSH sessions.

```
Console(config)# ip ssh pubkey-auth
```

Related Commands

crypto key generate dsa

crypto key generate rsa

crypto key pubkey-chain ssh

user-key

key-string

show crypto key mypubkey

show crypto key pubkey-chain ssh

crypto key pubkey-chain ssh

The **crypto key pubkey-chain ssh** Global Configuration mode command enters the SSH Public Key-chain Configuration mode. The mode is used to manually specify other device public keys such as SSH client public keys.

Syntax

crypto key pubkey-chain ssh

Default Setting

No keys are specified.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

Related Commands

crypto key generate dsa

crypto key generate rsa

ip ssh pubkey-auth

user-key

key-string

show crypto key mypubkey

show crypto key pubkey-chain ssh

user-key

The **user-key** SSH Public Key-string Configuration mode command specifies which SSH public key is manually configured. To remove an SSH public key, use the **no** form of this command.

Syntax

user-key *username* {**rsa** | **dsa**}

no user-key *username*

Parameters

- *username* — Specifies the username of the remote SSH client. (Range: 1-48 characters)
- **rsa** — Indicates the RSA key pair.
- **dsa** — Indicates the DSA key pair.

Default Setting

No SSH public keys exist.

Command Mode

SSH Public Key-string Configuration mode

Command Usage

Follow this command with the **key-string** SSH Public Key-String Configuration mode command to specify the key.

Example

The following example enables manually configuring an SSH public key for SSH public key-chain **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row
```

Related Commands

crypto key generate dsa

crypto key generate rsa

ip ssh pubkey-auth

crypto key pubkey-chain ssh

key-string

show crypto key mypubkey

show crypto key pubkey-chain ssh

key-string

The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.

Syntax

key-string

key-string row *key-string*

Parameters

- **row —** Indicates the SSH public key row by row.
- *key-string* — Specifies the key in UU-encoded DER format; UU-encoded DER format is the same format in the authorized_keys file used by OpenSSH.

Default Setting

No keys exist.

Command Mode

SSH Public Key-string Configuration mode

Command Usage

Use the **key-string** SSH Public Key-string Configuration mode command to specify which SSH public key is to be interactively configured next. To complete the command, you must enter a row with no characters.

Use the **key-string row** SSH Public Key-string Configuration mode command to specify the SSH public key row by row. Each row must begin with a **key-string row** command. This command is useful for configuration files.

Example

The following example enters public key strings for SSH public key client **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9

Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row AAAAB3Nza
Console(config-pubkey-key)# key-string row C1yc2
```

Related Commands

crypto key generate dsa

crypto key generate rsa

ip ssh pubkey-auth

crypto key pubkey-chain ssh

user-key

show crypto key mypubkey

show crypto key pubkey-chain ssh

show ip ssh

The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

Syntax

show ip ssh

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the SSH server configuration.

```
Console# show ip ssh

SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:

IP address   SSH           Version     Cipher        Auth Code
             username

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

172.16.0.1   John Brown    2.0 3       DES           HMAC-SHA1
```

The following table describes significant fields shown above:

Field	Description
IP address	Client address
SSH username	User name
Version	SSH version number
Cipher	Encryption type (3DES, Blowfish, RC4)
Auth Code	Authentication Code (HMAC-MD5, HMAC-SHA1)

Related Commands

ip ssh port

ip ssh server

show crypto key mypubkey

The **show crypto key mypubkey** Privileged EXEC mode command displays the SSH public keys on the device.

Syntax

show crypto key mypubkey [**rsa** | **dsa**]

Parameters

- **rsa** — Indicates the RSA key.
- **dsa** — Indicates the DSA key.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the SSH public RSA keys on the device.

```
Console# show crypto key mypubkey rsa
RSA key data:
005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 87685768
Fingerprint(Hex): 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
Fingerprint(Bubble Babble): yteriuwt jgkljhglk yewiury hdskjfryt gfhkjglk
```

Related Commands

crypto key generate dsa

crypto key generate rsa

ip ssh pubkey-auth

crypto key pubkey-chain ssh

user-key

key-string

show crypto key pubkey-chain ssh

show crypto key pubkey-chain ssh

The **show crypto key pubkey-chain ssh** Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint** {**bubble-babble** | **hex**}]

Parameters

- *username* — Specifies the remote SSH client username.
- **bubble-babble** — Fingerprint in Bubble Babble format.
- **hex** — Fingerprint in Hex format.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Examples

The following example displays SSH public keys stored on the device.

```
Console# show crypto key pubkey-chain ssh

Username     Fingerprint

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

bob          9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86

john         98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8


Console# show crypto key pubkey-chain ssh username bob

Username: bob

Key: 005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B
55D6AB22 04AEF1BA A54028A6 9ACC01C5 129D99E4

Fingerprint: 9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

Related Commands

crypto key generate dsa

crypto key generate rsa

ip ssh pubkey-auth

crypto key pubkey-chain ssh

user-key

key-string

show crypto key mypubkey

Syslog Commands

Table 4-30. Syslog Commands

Command	Function	Mode	Page
logging on	Controls error message logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. To disable the logging process, use the **no** form of this command.	GC	4-591
logging	Logs messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.	GC	4-592
logging console	Limits messages logged to the console based on severity. To disable logging to the console, use the **no** form of this command.	GC	4-593
logging buffered	Limits syslog messages displayed from an internal buffer based on severity. To cancel using the buffer, use the **no** form of this command.	GC	4-594
logging buffered size	Changes the number of syslog messages stored in the internal buffer. To return to the default configuration, use the **no** form of this command.	GC	4-595
clear logging	Clears messages from the internal logging buffer.	PE	4-595
logging file	Limits syslog messages sent to the logging file based on severity. To cancel using the buffer, use the **no** form of this command.	GC	
clear logging file	Clears messages from the logging file.	PE	4-596
aaa logging	Enables logging AAA login events. To disable logging AAA login events, use the **no** form of this command.	GC	4-597
file-system logging	Enables logging file system events. To disable logging file system events, use the **no** form of this command.	GC	4-598
management logging	Enables logging management access list (ACL) events. To disable logging management access list events, use the **no** form of this command.	GC	4-598
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.	PE	4-599
show logging file	Displays the state of logging and the syslog messages stored in the logging file.S	PE	4-601
show syslog-servers	Displays the settings of the syslog servers.	PE	4-603

logging on

The **logging on** Global Configuration mode command controls error message logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. To disable the logging process, use the **no** form of this command.

Syntax

logging on

no logging on

Default Setting

Logging is enabled.

Command Mode

Global Configuration mode

Command Usage

The logging process controls the distribution of logging messages at various destinations, such as the logging buffer, logging file or syslog server. Logging on and off at these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging** Global Configuration mode commands. However, if the **logging on** command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example

The following example enables logging error messages.

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

Related Commands

show logging

show syslog-servers

logging

The **logging** Global Configuration mode command logs messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.

Syntax

logging {*ip-address* | *hostname*} [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]

no logging {*ip-address* | *hostname*}

Parameters

- *ip-address* — IP address of the host to be used as a syslog server.
- *hostname* — Specifies the host name of the syslog server. (Range: 1-158 characters)
- *port* — Specifies the port number for syslog messages. (Range: 1 - 65535)
- *level* — Specifies the severity level of logged messages sent to the syslog servers. Possible values: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational** and **debugging**.
- *facility* — Specifies the facility that is indicated in the message. Possible

values: **local0, local1, local2, local3, local4, local5, local 6, local7**.

- *text* — Syslog server description. (Range: 1-64 characters)

Default Setting

The default port number is 514.

The default logging message level is **informational**.

The default facility is local7.

Command Mode

Global Configuration mode

Command Usage

Up to 8 syslog servers can be used.

If no specific severity level is specified, the global values apply to each server.

Example

The following example limits logged messages sent to the syslog server with IP address 10.1.1.1 to severity level **critical**.

```
Console(config)# logging 10.1.1.1 severity critical
```

Related Commands

show logging

logging console

The **logging console** Global Configuration mode command limits messages logged to the console based on severity. To disable logging to the console, use the **no** form of this command.

Syntax

logging console *level*

no logging console

Parameters

- *level* — Specifies the severity level of logged messages displayed on the console. Possible values: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational, debugging.**

Default Setting

The default severity level is **informational**.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example limits logging messages displayed on the console to severity level **errors**.

```
Console(config)# logging console errors
```

Related Commands

logging

show logging

logging buffered

The **logging buffered** Global Configuration mode command limits syslog messages displayed from an internal buffer based on severity. To cancel using the buffer, use the **no** form of this command.

Syntax

logging buffered *level*

no logging buffered

Parameters

- *level* — Specifies the severity level of messages logged in the buffer. Possible values: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational, debugging.**

Default Setting

The default severity level is **informational**.

Command Mode

Global Configuration mode

Command Usage

All the syslog messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example

The following example limits syslog messages displayed from an internal buffer based on severity level **debugging**.

```
Console(config)# logging buffered debugging
```

Related Commands

logging

clear logging

show logging

logging buffered size

The **logging buffered size** Global Configuration mode command changes the number of syslog messages stored in the internal buffer. To return to the default configuration, use the **no** form of this command.

Syntax

logging buffered size *number*

no logging buffered size

Parameters

- *number* — Specifies the maximum number of messages stored in the history table. (Range: 20 - 400)

Default Setting

The default number of messages is 200.

Command Mode

Global Configuration mode

Command Usage

This command takes effect only after Reset.

Example

The following example changes the number of syslog messages stored in the internal buffer to 300.

```
Console(config)# logging buffered size 300
```

Related Commands

show logging

clear logging

The **clear logging** Privileged EXEC mode command clears messages from the internal logging buffer.

Syntax

clear logging

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example clears messages from the internal logging buffer.

```
Console# clear logging
Clear logging buffer [confirm]
```

Related Commands

logging

logging buffered

show logging

logging file

The **logging file** Global Configuration mode command limits syslog messages sent to the logging file based on severity. To cancel using the buffer, use the **no** form of this command.

Syntax

logging file *level*

no logging file

Parameters

- *level* — Specifies the severity level of syslog messages sent to the logging filePossible values:: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational** and **debugging.**

Default Setting

The default severity level is **errors**.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example limits syslog messages sent to the logging file based on severity level **alerts**.

```
Console(config)# logging file alerts
```

Related Commands

logging

clear logging file

show logging

clear logging file

The **clear logging file** Privileged EXEC mode command clears messages from the logging file.

Syntax

clear logging file

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [confirm]
```

Related Commands

logging

logging file

show logging

aaa logging

The **aaa logging** Global Configuration mode command enables logging AAA login events. To disable logging AAA login events, use the **no** form of this command.

Syntax

aaa logging login

no aaa logging login

Parameters

- **login** — Indicates logging messages related to successful login events, unsuccessful login events and other login-related events**.**

Default Setting

Logging AAA login events is enabled.

Command Mode

Global Configuration mode

Command Usage

Other types of AAA events are not subject to this command.

Example

The following example enables logging messages related to AAA login events.

```
Console(config)# aaa logging login
```

Related Commands

show logging

file-system logging

The **file-system logging** Global Configuration mode command enables logging file system events. To disable logging file system events, use the **no** form of this command.

Syntax

file-system logging copy

no file-system logging copy

file-system logging delete-rename

no file-system logging delete-rename

Parameters

- **copy** — Indicates logging messages related to file copy operations.
- **delete-rename** — Indicates logging messages related to file deletion and renaming operations.

Default Setting

Logging file system events is enabled.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enables logging messages related to file copy operations.

```
Console(config)# file-system logging copy
```

Related Commands

show logging

management logging

The **management logging** global configuration command enables logging management access list (ACL) events. To disable logging management access list events, use the **no** form of this command.

Syntax

management logging deny

no management logging deny

Parameters

- **deny** — Indicates logging messages related to deny actions of management ACLs.

Default Setting

Logging management ACL events is enabled.

Command Mode

Global Configuration mode

Command Usage

Other types of management ACL events are not subject to this command.

Example

The following example enables logging messages related to deny actions of management ACLs.

```
Console(config)# management logging deny
```

Related Commands

show logging

show logging

The **show logging** Privileged EXEC mode command displays the state of logging and the syslog messages stored in the internal buffer.

Syntax

show logging

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the state of logging and the syslog messages stored in the internal buffer.

```
Console# show logging



Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped (severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.
File logging: level notifications. File Messages: 0 Dropped (severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).
2 messages were not logged (resources)

Application filtering control

Application    Event            Status

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

AAA            Login            Enabled

File system    Copy             Enabled

File system    Delete-Rename    Enabled

Management     Deny             Enabled
ACL



Buffer log:
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state
to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state
to up

11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/2, changed state
to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/3, changed state
to up
11-Aug-2004 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/0, changed state to down

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/1, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/2, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/3, changed state to down
```

Related Commands

logging on

logging

logging console

logging buffered

logging buffered size

clear logging

logging file

clear logging file

aaa logging

file-system logging

management logging

show logging file

The **show logging file** Privileged EXEC mode command displays the state of logging and the syslog messages stored in the logging file.

Syntax

show logging file

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the logging state and the syslog messages stored in the logging file.

```
Console# show logging file



Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped (severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.
File logging: level notifications. File Messages: 0 Dropped (severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).
2 messages were not logged (resources)
```

```
Application filtering control

Application       Event             Status

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

AAA               Login             Enabled

File system       Copy              Enabled

File system       Delete-Rename     Enabled

Management ACL    Deny              Enabled



Buffer log:
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/0, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/1, changed
state to up

11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/2, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/3, changed
state to up
11-Aug-2004 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/0, changed state to down

11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/1, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/2, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/3, changed state to down
```

Related Commands

logging on

logging

logging console

logging buffered

logging buffered size

clear logging

logging file

clear logging file

aaa logging

file-system logging

management logging

show syslog-servers

The **show syslog-servers** Privileged EXEC mode command displays the settings of the syslog servers.

Syntax

show syslog-servers

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the settings of the syslog servers.

```
Console# show syslog-servers


Device Configuration
IP address             Port   Severity          Facility    Description
------------           ----   -------------     --------    -----------
192.180.2.27           514    Informational     local7
192.180.2.28           514    Warning           local7
```

Related Commands

logging on

System Management Commands

Table 4-31. System Management Commands

Command	Function	Mode	Page
Clock Commands	Sends ICMP echo request packets to another node on the network.	UE	4-348
traceroute	Discovers routes that packets actually take when traveling to their destination.	UE	4-606
telnet	Enables logging on to a host that supports Telnet.	UE	4-608
resume	Enables switching to another open Telnet session.	UE	4-611
reload	Reloads the operating system.	PE	4-612
hostname	Specifies or modifies the device host name. To remove the existing host name, use the **no** form of the command.	GC	4-612
stack master	Enables forcing the selection of a stack master. To return to the default configuration, use the **no** form of this command.	GC	4-613
stack reload	Reloads stack members.	PE	4-614
stack display-order	Configures the order of the units in the display. To return to the default configuration, use the **no** form of this command .t	GC	4-614
show stack	Displays information about the status of a stack.	UE	4-615
show users	Displays information about the active users.	UE	4-617
show sessions	Lists open Telnet sessions.	UE	4-617
show system	Displays system information.	UE	4-618
show version	Displays system version information.	UE	4-619
service cpu-utilization	Enables measuring CPU utilization. To return to the default configuration, use the **no** form of this command.	GC	4-620
show cpu utilization	Displays information about CPU utilization.	UE	4-621

ping

The **ping** User EXEC mode command sends ICMP echo request packets to another node on the network.

Syntax

ping {*ip-address* | *hostname* }[**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]

Parameters

- *ip-address* — IP address to ping.
- *hostname* — Host name to ping. (Range: 1-158 characters)
- *packet_size* — Number of bytes in a packet. The actual packet size is eight bytes larger than the specified size specified because the device adds header information. (Range: 56 - 1472 bytes)

- *packet_count* — Number of packets to send. If 0 is entered, it pings until stopped. (Range: 0-65535 packets)
- *time_out* — Timeout in milliseconds to wait for each reply. (Range: 50 - 65535 milliseconds)

Default Setting

Default packet size is 56 bytes.

Default number of packets to send is 4.

Default timeout value is 2000 milliseconds.

Command Mode

User EXEC mode

Command Usage

Press **Esc** to stop pinging.

Following are examples of unsuccessful pinging:

Destination does not respond. If the host does not respond, a “no answer from host” appears in ten seconds.

Destination unreachable. The gateway for this destination indicates that the destination is unreachable.

Network or host unreachable. The device found no corresponding entry in the route table.

Examples

The following example displays pinging results:

```
Console> ping 10.1.1.1

Pinging 10.1.1.1 with 64 bytes of data:



64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms



----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11



Console> ping yahoo.com
Pinging yahoo.com 66.218.71.198 with 64 bytes of data:
```

```
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms



----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

Related Commands

resume

traceroute

The **traceroute** User EXEC mode command discovers routes that packets actually take when traveling to their destination.

Syntax

traceroute {*ip-address* **|***hostname* }[**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]

Parameters

- *ip-address* — IP address of the destination host.
- *hostname* — Host name of the destination host. (Range: 1-158 characters)
- *packet_size* — Number of bytes in a packet. (Range: 40-1500)
- *max-ttl* — The largest TTL value that can be used. The **traceroute** command terminates when the destination is reached or when this value is reached. (Range:1-255)
- *packet_count* — The number of probes to be sent at each TTL level. (Range:1-10)
- *time_out* — The number of seconds to wait for a response to a probe packet. (Range:1-60)
- *ip-address* — One of the device’s interface addresses to use as a source address for the probes. The device normally selects what it feels is the best source address to use.
- *tos* — The Type-Of-Service byte in the IP Header of the packet. (Range: 0-255)

Default Setting

The default number of bytes in a packet is 40.

The default maximum TTL value is 30.

The default number of probes to be sent at each TTL level is 3.

The default timeout interval in seconds is 3.

Command Mode

User EXEC mode

Command Usage

The **traceroute** command takesadvantage of the error messages generated by the devices when a datagram exceeds its time-to-live (TTL) value.

The **traceroute** command starts by sending probe datagrams with a TTL value of one. This causes the first device to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time exceeded" error message indicates that an intermediate device has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded or when the user interrupts the trace by pressing **Esc**.

Examples

The following example discovers the routes that packets will actually take when traveling to their destination.

```
Console> traceroute umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
1 i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec 35 msec
6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80)  47 msec 45 msec 45 msec
7 so-0-2-0x1.aa1.mich.net (192.122.183.9)  56 msec  53 msec 54 msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec 57 msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22) 58 msec 58 msec 58
msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64)  62 msec 63 msec 63 msec
```

The following table describes significant fields shown above.

Field	Description
1	Indicates the sequence number of the device in the path to the host.
i2-gateway.stanford.edu	Host name of this device.
192.68.191.83	IP address of this device.
1 msec 1 msec 1 msec	Round-trip time for each probe sent.

The following table describes characters that may appear in the **traceroute** command output.

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation is required and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded.
S	Source route failed.
U	Port unreachable.

Related Commands

resume

telnet

The **telnet** User EXEC mode command enables logging on to a host that supports Telnet.

Syntax

telnet {*ip-address* | *hostname*} [*port*] [*keyword1......*]

Parameters

- *ip-address* — IP address of the destination host.
- *hostname* — Host name of the destination host. (Range: 1-158 characters)
- *port* — A decimal TCP port number, or one of the keywords listed in the Ports table in the Command Usage.
- *keyword* — One or more keywords listed in the Keywords table in the Command Usage.

Default Setting

The default port is the Telnet port (decimal23) on the host.

Command Mode

User EXEC mode

Command Usage

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

Special Telnet Sequences

Telnet Sequence	Purpose
Ctrl-shift-6-b	Break
Ctrl-shift-6-c	Interrupt Process (IP)
Ctrl-shift-6-h	Erase Character (EC)
Ctrl-shift-6-o	Abort Output (AO)
Ctrl-shift-6-t	Are You There? (AYT)
Ctrl-shift-6-u	Erase Line (EL)

At any time during an active Telnet session, Telnet commands can be listed by pressing the Ctrl-shift-6-? keys at the system prompt.

A sample of this list follows. Note that the Ctrl-shift-6 sequence appears as ^^ on the screen.

```
Console> ‘Ctrl-shift-6’ ?
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
Ctrl-shift-6 x suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened and switched. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the **telnet** User EXEC mode command.

Keywords Table

Options	Description
/echo	Enables local echo.
/quiet	Prevents onscreen display of all messages from the software.
/source-interface	Specifies the source interface.

/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-shift-6 x	Return to System Command Prompt

Ports Table

Keyword	Description	Port Number
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25

sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

This command lists concurrent telnet connections to remote hosts that were opened by the current telnet session to the local device. It does not list telnet connections to remote hosts that were opened by other telnet sessions.

Example

The following example displays connecting to 176.213.10.50 via Telnet.

```
Console> telnet 176.213.10.50
Esc U sends telnet EL
```

Related Commands

resume

resume

The **resume** User EXEC mode command enables switching to another open Telnet session.

Syntax

resume [*connection*]

Parameters

- *connection* — The connection number. (Range: 1 - 4 connections)

Default Setting

The default connection number is that of the most recent connection.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following command switches to open Telnet session number 1.

```
Console> resume 1
```

Related Commands

telnet

reload

The **reload** Privileged EXEC mode command reloads the operating system.

Syntax

reload

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

Caution should be exercised when resetting the device, to ensure that no other activity is being performed. In particular, the user should verify that no configuration files are being downloaded at the time of reset.

Example

The following example reloads the operating system.

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

Related Commands

telnet

hostname

The **hostname** Global Configuration mode command specifies or modifies the device host name. To remove the existing host name, use the **no** form of the command.

Syntax

hostname *name*

no hostname

Parameters

- *name* — The host name. of the device. (Range: 1-158 characters)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example specifies the device host name.

```
Console(config)# hostname Alcatel
Alcatel(config)#
```

Related Commands

telnet

stack master

The **stack master** Global Configuration mode command enables forcing the selection of a stack master. To return to the default configuration, use the **no** form of this command.

Syntax

stack master unit *unit*

no stack master

Parameters

- *unit* — Unit number of the new master (Range: 1-2)

Default Setting

Disables forcing the selection of a stack master.

Command Mode

Global Configuration mode

Command Usage

The following algorithm is used to select a unit as the master:

- If only one master-enabled unit is in the stack (1 or 2), it becomes the master.
- If a unit configured as a forced master, it becomes the master.

If a forced master unit is removed from a stack and placed in a different stack with another forced master unit, both are considered to be forced, and the election criteria continue as follows:

- The unit with the longer up-time is elected master. Units are considered to have the same up-time if they were powered up within ten minutes of each other.

- If both forced master units have the same up-time, Unit 1 is elected.

Example

The following example selects Unit 2 as the stack master.

```
Console(config)# stack master unit 2
```

Related Commands

stack reload

stack display-order

show stack

stack reload

The **stack reload** Privileged EXEC mode command reloads stack members.

Syntax

stack reload [*unit*]

Parameters

- *unit* — Number of the unit to be reloaded (Range: 1-6)

Default Setting

All units are reloaded.

Command Modes

Privileged EXEC mode

Command Usage

If no unit is specified, all units are reloaded.

Example

The following example reloads Unit 2 of the stack.

```
Console(config)# stack reload unit 2
```

Related Commands

stack master

stack display-order

show stack

stack display-order

The **stack display-order** Global Configuration mode command configures the order of the units in the display. To return to the default configuration, use the **no** form of this command .

Syntax

stack display-order top *unit* **bottom** *unit*

no stack display-order

Parameters

- **top** *unit* — Specifies the number of the unit displayed at the top. (Range: 1-8)
- **bottom** *unit* — Specifies the number of the unit displayed at the bottom. (Range: 1-8)

Default Setting

The master unit is displayed at the top.

Command Modes

Global Configuration mode

Command Usage

If the units are not adjacent in ring or chain topology, the units are not at the edge and the default display order is used.

Example

This example displays unit 8 at the top of the display and unit 1 at the bottom.

```
Console# config
Console(config)# stack display-order top 8 bottom 1
```

Related Commands

stack master

stack reload

show stack

show stack

The **show stack** User EXEC mode command displays information about the status of a stack.

Syntax

show stack [**unit** *unit*]

Parameters

- *unit* — Specifies the number of the unit. (Range: 1-8)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

Example

The following example displays stack status.

```
Console> show stack
Unit    Address              Software Master   Uplink     Downlink     Status
----    -----------------    -------- ------   ------     --------     ------
1       00:00:b0:87:12:11    1.0.0.0 Enabled   2          3            Slave
2       00:00:b0:87:12:13    1.0.0.0 Enabled   1          4            Master
4       00:00:b0:87:12:14    1.0.0.0           3          5            Slave
5       00:00:b0:87:12:15    1.0.0.0           4          6            Slave
6       00:00:b0:87:12:16    1.0.0.0           5          7            Slave
Configured order: Unit 1 at Top, Unit 2 at bottom


Console> show stack
Unit    Address              Software Master   Uplink     Downlink     Status
----    -----------------    -------- ------   ------     --------     ------
3       00:00:b0:87:12:13    1.0.0.0           1          4            Slave
4       00:00:b0:87:12:14    1.0.0.0           3          5            Slave
5       00:00:b0:87:12:15    1.0.0.0           4          6            Slave
6       00:00:b0:87:12:16    1.0.0.0           5          2            Slave
1       00:00:b0:87:12:12    1.0.0.0 Forced    6          1            Master
2       00:00:b0:87:12:11    1.0.0.0 Enabled   2          3            Slave
Configured order: Unit 1 at Top, Unit 6 at bottom
Can’t display order as requested.


Console> show stack 1
Unit 1:
MAC address: 00:00:b0:87:12:11
Master: Forced.
Product: OS-LS-6224. Software: 1.0.0.0
Status: Master
Active image: image-1.
Selected for next boot: image-2.
```

Related Commands

stack master

stack reload

stack display-order

show users

The **show users** User EXEC mode command displays information about the active users.

Syntax

show users

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays information about the active users.

```
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
```

Related Commands

show system

show sessions

The **show sessions** User EXEC mode command lists open Telnet sessions.

Syntax

show sessions

Default Setting

There is no default configuration for this command.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example lists open Telnet sessions.

```
Console> show sessions

Connection          Host                Address       Port     Byte
----------          -------------       ----------    -----    ----
1                   Remote device       172.16.1.1    23       89
2                   172.16.1.2          172.16.1.2    23       8
```

The following table describes significant fields shown above.

Field	Description
Connection	Connection number.
Host	Remote host to which the device is connected through a Telnet session.
Address	IP address of the remote host.
Port	Telnet TCP port number
Byte	Number of unread bytes for the user to see on the connection.

Related Commands

show system

show system

The **show system** User EXEC mode command displays system information.

Syntax

show system [**unit** *unit*]

Parameters

- *unit* — Specifies the number of the unit. (Range: 1-6)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the system information.

```
Console# show system

Unit              Type
----              -----------------
1                 Alcatel 6300

Unit              Main Power Supply          Redundant Power Supply
----              -----------------          ----------------------
1                 OPERATIONAL                NOT OPERATIONAL

Unit              Fan1              Fan2     Fan3    Fan4           Fan5
----              ----              ----     ----    ----           ----
1                 OK                OK       OK      OK             OK
```

Related Commands

show sessions

show version

The **show version** User EXEC mode command displays system version information.

Syntax

show version [**unit** *unit*]

Parameters

- *unit* — Specifies the number of the unit. (Range: 1-6)

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays system version information (only for demonstration purposes).

```
Console> show version
SW version 1.0.0.0          (date 23-Jul-2004 time 17:34:19)
Boot version 1.0.0.0        (date 11-Jan-2004 time 11:48:21)
HW version 1.0.0


Unit         SW version     Boot version                HW version
----         ----------     ------------                ----------
1            1.0.0.0        2.178                       1.0.0
2            1.0.0.0        2.178                       1.0.0
```

Related Commands

service cpu-utilization

service cpu-utilization

The **service cpu-utilization** Global Configuration mode command enables measuring CPU utilization. To return to the default configuration, use the **no** form of this command.

Syntax

service cpu-utilization

no service cpu-utilization

Default Setting

Disabled.

Command Mode

Global Configuration mode

Command Usage

Use the **show cpu utilization** Privileged EXEC command to view information on CPU utilization.

Example

The following example enables measuring CPU utilization.

```
Console(config)# service cpu-utilization
```

Related Commands

show cpu utilization

show cpu utilization

The **show cpu utilization** Privileged EXEC mode command displays information about CPU utilization.

Syntax

show cpu utilization

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

Use the **service cpu-utilization** Global Configuration mode command to enable measuring CPU utilization.

Example

The following example displays information about CPU utilization.

```
Console# show cpu utilization

CPU utilization service is on.

CPU utilization
--------------------------------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

TACACS+ Commands

Table 4-32. TACACS+ Commands

Command	Function	Mode	Page
tacacs-server hostt	Specifies a TACACS+ host. To delete the specified name or address, use the **no** form of this command.	GC	4-622
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. To disable the key, use the **no** form of this command.	GC	4-623
tacacs-server timeout	Sets the interval during which the device waits for a TACACS+ server to reply. To return to the default configuration, use the **no** form of this command.	GC	4-624
tacacs-server source-ip	Configures the source IP address to be used for communication with TACACS+ servers. To return to the default configuration, use the **no** form of this command.	GC	4-625
show tacacs	Displays configuration and statistical information about a TACACS+ server.	PE	4-625

tacacs-server host

The **tacacs-server host** Global Configuration mode command specifies a TACACS+ host. To delete the specified name or address, use the **no** form of this command.

Syntax

tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]

no tacacs-server host {*ip-address* | *hostname*}

Parameters

- *ip-address* — IP address of the TACACS+ server.
- *hostname* — Host name of the TACACS+ server. (Range: 1 - 158 characters)
- **single-connection** — Indicates a single-connection. Rather than have the device open and close a TCP connection to the daemon each time it must communicate, the single-connection option maintains a single open connection between the device and the daemon.
- *port-number* — Specifies a server port number. (Range: 0 - 65535)
- *timeout* — Specifies the timeout value in seconds. (Range: 1 - 30)
- *key-string* — Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "". (Range: 0 - 128 characters)
- *source* — Specifies the source IP address to use for the communication. 0.0.0.0 indicates a request to use the IP address of the outgoing IP

interface.

- *priority* — Determines the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0 - 65535)

Default Setting

No TACACS+ host is specified.

If no port number is specified, default port number 49 is used.

If no host-specific timeout, key-string or source value is specified, the global value is used.

If no TACACS+ server priority is specified, default priority 0 is used.

Command Mode

Global Configuration mode

Command Usage

Multiple **tacacs-server host** commands can be used to specify multiple hosts.

Example

The following example specifies a TACACS+ host.

```
Console(config)# tacacs-server host 172.16.1.1
```

Related Commands

tacacs-server key

tacacs-server timeout

tacacs-server source-ip

show tacacs

tacacs-server key

The **tacacs-server key** Global Configuration mode command sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. To disable the key, use the **no** form of this command.

Syntax

tacacs-server key *key-string*

no tacacs-server key

Parameters

- *key-string* — Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Range: 0-128 characters)

Default Setting

Empty string.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Examples

The following example sets the authentication encryption key.

```
Console(config)# tacacs-server key alcatel-s
```

Related Commands

tacacs-server host

tacacs-server timeout

tacacs-server source-ip

show tacacs

tacacs-server timeout

The **tacacs-server timeout** Global Configuration mode command sets the interval during which the device waits for a TACACS+ server to reply. To return to the default configuration, use the **no** form of this command.

Syntax

tacacs-server timeout *timeout*

no tacacs-server timeout

Parameters

- *timeout* — Specifies the timeout value in seconds. (Range: 1 - 30)

Default Setting

5 seconds

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Examples

The following example sets the timeout value to 30.

```
Console(config)# tacacs-server timeout 30
```

Related Commands

tacacs-server host

tacacs-server key

tacacs-server source-ip

show tacacs

tacacs-server source-ip

The **tacacs-server source-ip** Global Configuration mode command configures the source IP address to be used for communication with TACACS+ servers. To return to the default configuration, use the **no** form of this command.

Syntax

tacacs-server source-ip *source*

no tacacs-server source-ip *source*

Parameters

- *source* — Specifies the source IP address.

Default Setting

The source IP address is the address of the outgoing IP interface.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example specifies the source IP address.

```
Console(config)# tacacs-server source-ip 172.16.8.1
```

Related Commands

tacacs-server host

tacacs-server key

tacacs-server timeout

show tacacs

show tacacs

The **show tacacs** Privileged EXEC mode command displays configuration and statistical information about a TACACS+ server.

Syntax

show tacacs [*ip-address*]

Parameters

- *ip-address* — Name or IP address of the TACACS+ server.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays configuration and statistical information about a TACACS+ server.

```
Console# show tacacs


Device Configuration

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



IP          Status     Port   Single          TimeO    Source   Priority
address                       Connection      ut       IP

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

172.16.1.   Connecte   49     No              Globa    Global   1
1           d                                 l



Global values

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

TimeOut: 3

Device Configuration

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

Source IP: 172.16.8.1
```

Related Commands

tacacs-server host

tacacs-server key

tacacs-server timeout

tacacs-server source-ip

Triple Play Commands

Table 4-33. Triple Play Commands

Command	Function	Mode	Page
switchport customer vlan	Sets the port's VLAN when the interface is in customer mode	Interface Configurati on	4-627
switchport customer multicast-tv vlan	Enables the receiving of Multicast transmissions from a VLAN that is not the Customer port’s VLAN, while keeping the L2 segregation with subscribers on different Customer port VLANs.	Interface Configurati on	4-627
ip igmp snooping map cpe vlan	Maps CPE VLANs to multicast-TV VLANs.	Global Configurati on	4-628
show ip igmp snooping cpe vlans	Displays the CPE VLANs to Multicast TV VLANs mappings.	Privileged EXEC mode	4-629

switchport customer vlan

The **switchport customer vlan** Interface Configuration (Ethernet, port-channel) mode command sets the port's VLAN when the interface is in customer mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport customer vlan *vlan-id*

no switchport customer vlan

Parameters

- *vlan-id* — VLAN ID of the customer.

Default Configuration

No VLAN is configured.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

switchport customer multicast-tv vlan

The **switchport customer multicast-tv vlan** interface configuration command enables the receiving of Multicast transmissions from a VLAN that is not the Customer port’s VLAN, while keeping the L2 segregation with subscribers on different Customer port VLANs.

Syntax

switchport customer multicast-tv vlan {**add** *vlan-list* | **remove** *vlan-list*}

- *vlan-list* — List of Multicast TV VLANs.

Default Setting

The port is not member in any multicast TV VLAN.

Command Mode

Interface configuration (Ethernet, port-channel)

Command Usage

The user cannot transmit Multicast transmissions on Multicast TV VLANs.

Example

The following example configure port e1 to enable receiving multicast transmissions from a VLAN that is not the customer port's VLAN.

```
Console (config-if)# switchport customer multicast-tv vlan add 3000
```

Related Commands

ip igmp snooping map cpe vlan

show ip igmp snooping cpe vlans

ip igmp snooping map cpe vlan

The **ip igmp snooping map cpe vlan** global configuration command maps CPE VLANs to multicast-TV VLANs. Use the **no** form of this command to remove the mapping.

Syntax

ip igmp snooping map cpe vlan *vlan-id* **multicast-tv vlan** *vlan-id*

no ip igmp snooping map cpe vlan *vlan-id*

Parameters

- **cpe vlan** *vlan-id* — Specify the CPE VLAN.
- **multicast-tv vlan** *vlan-id* —Specify the Multicast VLAN.

Default Setting

No mapping exists.

Command Mode

Global configuration

Command Usage

Use this command to associate CPE VLAN to a multicast-TV VLAN.

If an IGMP message is received on a customer port tagged with a CPE VLAN, and there is a mapping from that CPE VLAN to a multicast-TV VLAN, the IGMP message would be associated with the multicast-TV VLAN.

Example

The following example maps an internal CPE VLAN number 4 to the Multicast TV VLAN number 300.

```
Console (config)# ip igmp snooping map cpe vlan 4 multicast-tv vlan 300
```

Related Commands

switchport customer multicast-tv vlan

show ip igmp snooping cpe vlans

show ip igmp snooping cpe vlans

The **show ip igmp snooping cpe vlans** Privileged EXEC mode command displays the CPE VLANs to Multicast TV VLANs mappings.

Syntax

show ip igmp snooping cpe vlans [**vlan** *vlan-id*]

Parameters

- *vlan-id* — CPE VLAN ID value.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the CPE VLANs to Multicast TV VLANs mappings.

```
Console# show ip igmp snooping cpe vlans

CPE VLAN     Multicast-TV VLAN

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

3            1118

3            1119
```

Related Commands

switchport customer multicast-tv vlan

ip igmp snooping map cpe vlan

show ip igmp snooping interface

The **show ip igmp snooping interface** Privileged EXEC mode command displays IGMP snooping configuration.

Syntax

show ip igmp snooping interface *vlan-id*

Parameters

- *vlan-id* — Specifies the valid VLAN number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows IGMP snooping information on multicast groups.

```
Console # show ip igmp snooping interface 1000
IGMP Snooping is globally enabled

IGMP Snooping admin: Enabled
Hosts and routers IGMP version: 2
IGMP snooping oper mode: Enabled
IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 172.16.1.1
IGMP snooping querier version admin: 3
IGMP snooping querier version oper: 2


IGMP host timeout is 300 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 300 sec
Automatic learning of multicast router ports is enabled
```

DHCP Snooping, IP Source Guard and ARP Inspection Commands

.

Table 4-34. DHCP Snooping, IP Source Guard and ARP Inspection Commands

Command	Function	Mode	Page
DHCP Snooping			
ip dhcp snooping	Use the ip dhcp snooping global configuration command to globally enable DHCP snooping.	GC	4-632
ip dhcp snooping vlan	Use the ip dhcp snooping vlan global configuration command to enable DHCP snooping on a VLAN.	GC	4-633
ip dhcp snooping trust	Use the ip dhcp snooping trust interface configuration command to configure a port as trusted for DHCP snooping purposes.	IC	4-634
ip dhcp information option allowed-untrusted	Use the ip dhcp information option allowed-untrusted global configuration command on a switch to configure it to accept DHCP packets with option-82 information from an untrusted port.	GC	4-634
ip dhcp information option	Use the ip dhcp information option global configuration command to enable DHCP option-82 data insertion.	GC	4-635
ip dhcp snooping verify	Use the ip dhcp snooping verify global configuration command to configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address.	GC	4-635
ip dhcp snooping database	Use the ip dhcp snooping database global configuration command to configure the DHCP snooping binding file.	GC	4-636
ip dhcp snooping database update-freq	Use the ip dhcp snooping database update-freq global configuration command to configure the update frequency ofthe DHCP snooping binding file.	GC	4-636
ip dhcp snooping binding	Use the ip dhcp snooping binding privileged EXEC command to configure the DHCP snooping binding database and to add binding entries to the database.	PE	4-637
clear ip dhcp snooping database	Use the clear ip dhcp snooping database privileged EXEC command to clear the DHCP binding database.	PE	4-638
show ip dhcp snooping	Use the show ip dhcp snooping EXEC command to display the DHCP snooping configuration.	UE	4-638
show ip dhcp snooping binding	Use the show ip dhcp snooping binding user EXEC command to display the DHCP snooping binding database and configuration information for all interfaces on a switch.	UE	4-639
IP Source Guard			
ip source-guard (global)	Use the ip source-guard global configuration command to globally enable IP source guard.	GC	4-640
ip source-guard (interface)	Use the ip source-guard interface configuration command to enable IP source guard on an interface.	ICE	4-640
ip source-guard binding	Use the ip source-guard binding global configuration command to configure static IP source bindings on the switch.	GC	4-641

Table 4-34. DHCP Snooping, IP Source Guard and ARP Inspection Commands

Command	Function	Mode	Page
ip source-guard tcam retries-freq	Use the ip source-guard tcam retries-freq global configuration command to configure the frequency of retries for TCAM resources for inactive IP source guard addresses	GC	4-642
ip source-guard tcam locate	Use the ip source-guard tcam locate privileged EXEC command to manually retry to locate TCAM resources for inactive IP source guard addresses.	PE	4-643
show ip source-guard	Use the show ip source-guard EXEC command to display the IP source guard configuration.	UE	4-643
show ip source-guard inactive	Use the show ip source-guard inactive EXEC command to display the IP source guard inactive addresses.	UE	4-644
ARP Inspection			
ip arp inspection	Use the ip arp inspection global configuration command to globally enable ARP inspection.	GC	4-645
ip arp inspection vlan	Use the ip arp inspection vlan global configuration command to enable ARP inspection based on DHCP snooping database on a VLAN.	GC	4-646
ip arp inspection trust	Use the ip arp inspection trust interface configuration command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected.	ICE	4-646
ip arp inspection validate	Use the ip arp inspection validate global configuration command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection.	GC	4-647
ip arp inspection list create	Use the ip arp inspection list create global configuration command to create static ARP binding list and to enter to the ARP list configuration mode.	GC	4-648
ip mac	Use the ip mac ARP-list configuration command to static ARP binding.	ALC	4-648
ip arp inspection list assign	Use the ip arp inspection list assign global configuration command to assign static ARP binding list to a VLAN.	GC	4-649
ip arp inspection logging interval	Use the ip arp inspection logging interval global configuration command to configure the minimal interval between successive ARP SYSLOG messages.	GC	4-650
show ip arp inspection	Use the show ip arp inspection EXEC command to display the ARP inspection configuration.	UE	4-646
show ip arp inspection list	Use the show ip arp inspection list priviledged EXEC command to display the static ARP binding list.	PE	4-651

ip dhcp snooping

The **ip dhcp snooping** Global Configuration mode command globally enables DHCP snooping. To return to the default configuration, use the **no** form of this command.

Syntax

ip dhcp snooping

no ip dhcp snooping

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

For any DHCP snooping configuration to take effect, DHCP snooping must be globally enable. DHCP snooping is not active until you enable snooping on a VLAN by using the **ip dhcp snooping vlan** global configuration command.

Example

The following example globally enables DHCP snooping.

```
Console # (config)# ip dhcp snooping
Console # (config)#
```

ip dhcp snooping vlan

The **ip dhcp snooping vlan** Global Configuration mode command enables DHCP snooping on a VLAN. To disable DHCP snooping on a VLAN, use the **no** form of this command.

Syntax

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping vlan *vlan-id*

Parameters

- *vlan-id* — Specifies the VLAN ID.

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP snooping must first be globally enable before enabling DHCP snooping on a VLAN.

Example

The following example enables DHCP snooping on vlan id 1.

```
Console # (config)# ip dhcp snooping vlan 1
Console # (config)#
```

ip dhcp snooping trust

The **ip dhcp snooping trust** Interface Configuration (Ethernet, Port-channel) mode command configures a port as trusted for DHCP snooping purposes. To return to the default configuration, use the **no** form of this command.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Configure as trusted ports, which are connected to a DHCP server or to other switches or routers. Configure as untrusted ports those that are connected to DHCP clients.

Example

The following example configures port 1/e16 as trusted for DHCP snooping.

```
Console # (config)# interface 1/e16
Console # (config-if)# ip dhcp snooping trust
Console # (config-if)#
```

ip dhcp information option allowed-untrusted

The **ip dhcp information option allowed-untrusted** Global Configuration mode command on a switch configures it to accept DHCP packets with option-82 information from an untrusted port. To configure the switch to drop these packets from an untrusted port, use the **no** form of this command.

Syntax

ip dhcp information option allowed-untrusted

no ip dhcp information option allowed-untrusted

Default Configuration

Discard DHCP packets with option-82 information from an untrusted port.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the switch to accept DHCP packets with option-82 information from an untrusted port.

```
Console # (config)# ip dhcp information option allowed-untrusted
Console # (config)#
```

ip dhcp information option

The **ip dhcp information option** Global Configuration mode command enables DHCP option-82 data insertion. To disable DHCP option-82 data insertion, use the **no** form of this command.

Syntax

ip dhcp information option

no ip dhcp information option

Default Configuration

DHCP option-82 data insertion is enabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP option 82 is enabled when DHCP snooping is enabled on VLANs.

Example

The following example enables DHCP option-82 data insertion.

```
Console # (config)# ip dhcp information option
Console # (config)#
```

ip dhcp snooping verify

The **ip dhcp snooping verify** Global Configuration mode command configures the switch to verify, on an untrusted port, that the source MAC address in a DHCP packet matches the client hardware address. To configure the switch to not verify the MAC addresses, use the **no** form of this command.

Syntax

ip dhcp snooping verify

no ip dhcp snooping verify

Default Configuration

The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the switch to verify, on an untrusted port, that the source MAC address in a DHCP packet matches the client hardware address.

```
Console # (config)# ip dhcp snooping verify
Console # (config)#
```

ip dhcp snooping database

The **ip dhcp snooping database** Global Configuration mode command configures the DHCP snooping binding file. To delete the binding file, use the **no** form of this command.

Syntax

ip dhcp snooping database

no ip dhcp snooping database

Default Configuration

The URL is not defined.

Command Mode

Global Configuration mode

User Guidelines

To ensure that the lease time in the database is accurate and the Simple Network Time Protocol (SNTP) is enabled and configured.

The switch writes binding changes to the binding file only when the switch system clock is synchronized with SNTP.

Example

The following example configures the DHCP snooping binding file.

```
Console # (config)# ip dhcp snooping database
Console # (config)#
```

ip dhcp snooping database update-freq

The **ip dhcp snooping database update-freq** Global Configuration Command configures the update frequency ofthe DHCP snooping binding file. To return to the default configuration, use the **no** form of this command.

Syntax

ip dhcp snooping database update-freq *seconds*

no ip dhcp snooping database update-freq

Parameters

- *seconds* — Specifies, in seconds, the update frequency. (Range: 600 – 86400)

Default Configuration

The default value is 1200.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the DHCP snooping binding file update frequency to 1500 seconds.

```
Console # (config)# ip dhcp snooping database update-freq 1500
Console # (config)#
```

ip dhcp snooping binding

The ip dhcp snooping binding Privileged EXEC mode command configures the DHCP snooping binding database and adds binding entries to the database. To delete entries from the binding database, use the no form of this command.

Syntax

ip dhcp snooping binding *mac-address vlan-id ip-address* {**ethernet** *interface* **| port-channel** *port-channel-number*} **expiry** *seconds*

no ip dhcp snooping binding *mac-address vlan-id*

Parameters

- *mac-address* — Specifies a MAC address.
- *vlan-id* — Specifies a VLAN number.
- *ip-address* — Specifies an IP address.
- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies the Port-channel number.
- **expiry** *seconds* — Specifies the interval, in seconds, after which the binding entry is no longer valid. (Range: 10 – 4294967295)

Default Configuration

No static binding exists.

Command Mode

Privileged EXEC mode

User Guidelines

After entering this command an entry would be added to the DHCP snooping database. If DHCP snooping binding file exists, the entry would be added to that file also.

The entry would be displayed in the show commands as a “DHCP Snooping entry”.

Example

The following example configures the DHCP snooping binding database.

```
Console # ip dhcp snooping binding 00:00:B4:00:7F:EE 1 10.6.22.195
ethernet 1/e16
Console #
```

clear ip dhcp snooping database

The **clear ip dhcp snooping database** Privileged EXEC mode command clears the DHCP binding database.

Syntax

clear ip dhcp snooping database

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

show ip dhcp snooping

The **show ip dhcp snooping** EXEC mode command displays the DHCP snooping configuration.

Syntax

show ip dhcp snooping [**ethernet** *interface* **| port-channel** *port-channel-number*]

Parameters

- *interface* — Specifies the Ethernet port.
- *port-channel-number* — Specifies the Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the DHCP snooping configuration.

```
Console# show ip dhcp snooping

DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 2, 7-18
DHCP snooping database: enabled
Option 82 on untrusted port is allowed
Relay agent information option 82 is enabled.
Verification of hwaddr field is enabled



Interface                            Trusted

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

1/1                                  Yes

1/2                                  Yes
```

show ip dhcp snooping binding

The **show ip dhcp snooping binding** User EXEC mode command displays the DHCP snooping binding database and configuration information for all interfaces on a switch.

Syntax

show ip dhcp snooping binding [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan*] [**ethernet** *interface* **| port-channel** *port-channel-number*]

Parameters

- *mac-address* — Specifies a MAC address.
- *ip-address* — Specifies an IP address.
- *vlan-id* — Specifies a VLAN number.
- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies the Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a switch.

```
Console# show ip dhcp snooping binding
Update frequency: 1200
Total number of binding: 3


Mac Address  IP Address  Lease (sec)  Type         VLAN         Interface

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

0060.704C.73 10.1.8.1    7983         snooping     3            1/21
FF

0060.704C.7B 10.1.8.2    92332        snooping (s) 3            1/22
C1
```

ip source-guard (global)

The **ip source-guard** Global Configuration mode command globally enables the IP source guard. To disable IP source guard, use the **no** form of this command.

Syntax

ip source-guard

no ip source-guard

Default Configuration

IP source guard is disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example globally enables the IP source guard.

```
 Console # (config)# ip source-guard
 Console # (config)#
```

ip source-guard (interface)

The **ip source-guard** Interface Configuration (Ethernet, Port-channel) mode command enables IP source guard on an interface. To disable IP source guard, use the **no** form of this command.

Syntax

ip source-guard

no ip source-guard

Default Configuration

IP source guard is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example globally enables the IP source guard on port 1/e16.

```
Console # (config)# interface ethernet 1/e16
Console # (config-if)# ip source-guard
Console # (config-if)#
```

ip source-guard binding

The **ip source-guard binding** Global Configuration mode command configures the static IP source bindings on the switch. To delete static bindings, use the **no** form of this command.

Syntax

ip source-guard binding *mac-address vlan-id ip-address* {**ethernet** *interface* **| port-channel** *port-channel-number*}

no ip source-guard binding *mac-address vlan-id*

Parameters

- *mac-address* — Specifies a MAC address.
- *vlan-id* — Specifies a VLAN number.
- *ip-address* — Specifies an IP address.
- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies the Port-channel number.

Default Configuration

No static binding exists.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the static IP source bindings on the switch for port 1/e16.

```
Console # (config)# ip source-guard binding 00:60:70:4C:73:FF 1
10.6.22.195 ethernet 1/e16
Console # (config)#
```

ip source-guard tcam retries-freq

The **ip source-guard tcam retries-freq** Global Configuration mode command configures the frequency of retries for TCAM resources for inactive IP source guard addresses. To return to the default configuration, use the **no** form of this command.

Sytnax

ip source-guard tcam retries-freq {*seconds* | **never**}

no ip source-guard tcam retries-freq

Parameters

- *seconds* — Specifies, in seconds, the retries frequency. (Range: 10 – 600)
- **never —** Specifies to not perform an automatic search for TCAM resources.

Default Configuration

The default value is 60.

Command Mode

Global Configuration mode

User Guidelines

Since the IP source guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations where IP source guard addresses are inactive because of a lack of TCAM resources.

By default, every minute the software conducts a search for available space in the TCAM for the inactive IP source guard addresses. You can use this command to change the frequency or to disable automatic retries for TCAM space.

The **ip source-guard tcam locate** Privileged EXEC mode command manually retries locating TCAM resources for the inactive IP source guard addresses.

The **show ip source-guard inactive** EXEC mode command displays the inactive IP source guard addresses.

Example

The following example globally sets the TCAM resources retry frequency to 50 seconds.

```
Console # (config)# ip source-guard tcam retries-freq 50
Console # (config)#
```

ip source-guard tcam locate

The **ip source-guard tcam locate** Privileged EXEC mode command manually retries to locate TCAM resources for inactive IP source guard addresses.

Syntax

ip source-guard tcam locate

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Since the IP source guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations where IP source guard addresses are inactive because of lack of TCAM resources.

By default, every minute the software conducts a search for available space in the TCAM for the inactive IP source guard addresses.

The **ip source-guard tcam retries-freq** Global Configuration mode command disables automatic retries for TCAM space, and manually retries locating TCAM resources for the inactive IP source guard addresses.

The **show ip source-guard inactive** EXEC mode command displays the inactive IP source guard addresses.

Example

The following example retries to locate TCAM resources for inactive IP source guard addresses.

```
Console # ip source-guard tcam locate
Console #
```

show ip source-guard

The s**how ip source-guard** EXEC mode command displays the IP source guard configuration.

Syntax

show ip source-guard [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan*] [**ethernet** *interface* **| port-channel** *port-channel-number*]

Parameters

- *mac-address* — Specifies a MAC address.
- *ip-address* — Specifies an IP address.
- *vlan-id* — Specifies a VLAN number.
- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies a port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the IP source guard configuration.

```
Console# show ip source-guard

IP source guard is enabled.


Interface  Filter     Status     IP Address MAC        VLAN       Type
                                            Address

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

1/21       IP         Active     10.1.8.1   0060.704C. 3          DHCP
                                            73FF

1/22       IP         Active     10.1.12.2  0060.704C. 4          DHCP
                                            7BC3

1/22       IP         Active     10.1.8.2   0060.704C. 3          DHCP
                                            7BC1

1/22       IP         Active     10.1.12.2  0060.704C. 4          DHCP
                                            7BC3

1/23       IP         Active     Deny All

1/24       IP         Active     10.1.8.218 0060.704C. 3          Static
                                            7BAC

1/32       IP         Inactive   10.1.8.32  0060.704C. 3          DHCP
                                            83FF
```

show ip source-guard inactive

The **show ip source-guard inactive** EXEC mode command displays the IP source guard inactive addresses.

Syntax

show ip source-guard inactive

Default Configuration

This command has no default configuration.

Command Mode

EXEC mode

User Guidelines

Since the IP source guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations where IP source guard addresses are inactive because of lack of TCAM resources.

By default, every minute the software conducts a search for available space in the TCAM for the inactive IP source guard addresses.

The **ip source-guard tcam retries-freq** Global Configuration mode command changes the frequency or disables automatic retries for TCAM space.

The **ip source-guard tcam locate** Privileged EXEC mode command retries locating TCAM resources for the inactive IP source guard addresses.

This command displays the inactive IP source guard addresses.

Example

The following example displays the IP source guard inactive addresses.

```
Console# show ip source-guard inactive

 TCAM resources search frequency: 10 minutes


Interface  Filter     IP Address MAC        VLAN       Type       Reason
                                 Address

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

1/32       IP         10.1.8.32  0060.704C. 3          3DHCP      Resource
                                 83FF                             Problem
```

ip arp inspection

The **ip arp inspection** Global Configuration mode command globally enables ARP inspection. To disable ARP inspection, use the **no** form of this command.

Syntax

ip arp inspection

no ip arp inspection

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example globally enables the ARP inspection.

```
Console # (config)# ip arp inspection
Console # (config)# 01-Jan-2000 23:07:53 %ARPINSP-I-PCKTLOG: ARP packet
dropped from port g3 with VLAN tag 1 and reason: packet verification failed
SRC MAC 00:00:5e:00:01:07 SRC IP 10.6.22.193 DST MAC 00:00:00:00:00:00 DST
IP 10.6.22.195
```

ip arp inspection vlan

The ip arp inspection vlan Global Configuration mode command enables ARP inspection based on DHCP snooping database on a VLAN. To disable ARP inspection on a VLAN, use the no form of this command.

Syntax

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan *vlan-id*

Parameters

- *vlan-id* — Specifies the VLAN ID.

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables ARP inspection on a VLAN based on the DHCP snooping database.The **ip arp inspection list assign** Global Configuration mode command enables static ARP inspection.

Example

The following example enables ARP inspection on VLAN ID 1.

```
Console # (config)# ip arp inspection vlan 1
Console # (config)#
```

ip arp inspection trust

The **ip arp inspection trust** Interface Configuration (Ethernet, Port-channel) mode command configures an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. To return to the default configuration, use the **no** form of this command.

Syntax

ip arp inspection trust

no ip arp inspection trust

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The switch does not check ARP packets, which are received on the trusted interface; it simply forwards the packets.

For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection log-buffer vlan** Global Configuration mode command.

Example

The following example configures an ARP inspection trust state on port 1/e16.

```
Console # (config)# interface ethernet 1/e16
Console # (config-if)# ip arp inspection trust
Console # (config-if)#
```

ip arp inspection validate

Use the **ip arp inspection validate** global configuration command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to return to the default settings.

Syntax

ip arp inspection validate

no ip arp inspection validate

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

The following are performed:

- **Source MAC**: Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed

on both ARP requests and responses.
- **Destination MAC**: Compare the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses.
- **IP addresses**: Compare the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

The following example validates ARP inspection.

```
Console # (config)# ip arp inspection validate
Console # (config)#
```

ip arp inspection list create

The **ip arp inspection list create** Global Configuration mode command creates a static ARP binding list and to enter the ARP list configuration mode. To delete the list, use the **no** form of this command.

Syntax

ip arp inspection list create *name*

no ip arp inspection list create *name*

Parameters

- *name* — Specifies the list name. (Range: 1-32 characters)

Default Configuration

No static ARP binding list exists.

Command Mode

Global Configuration mode

User Guidelines

This command enables static ARP inspection on a VLAN.

Example

The following example creates the static ARP binding list *arplist*.

```
Console # (config)# ip arp inspection list create arplist
Console # (config-arp-list)#
```

ip mac

The **ip mac** ARP-list Configuration mode command displays static ARP binding. To delete a binding, use the **no** form of this command.

Syntax

ip *ip-address* **mac** *mac-address*

no ip *ip-address* **mac** *mac-address*

Parameters

- *ip-address* — Specifies the IP address to be entered to the list.
- *mac-address* — Specifies the MAC address associated with the IP address.

Default Configuration

No binding is defined.

Command Mode

ARP-list Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays static ARP binding.

```
Console(config)# ip arp inspection list 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
```

ip arp inspection list assign

The **ip arp inspection list assign** Global Configuration mode command assigns static ARP binding lists to a VLAN. To delete the assignment, use the **no** form of this command.

Syntax

ip arp inspection list assign *vlan name*

no ip arp inspection list assign *vlan*

Parameters

- *vlan* — Specifies the VLAN name.
- *name* — Specifies the list name.

Default Configuration

No static ARP binding list assignment exists.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example assigns static ARP binding list *arplist* to VLAN *vlan1*.

```
 Console # (config)# ip arp inspection list assign arplist vlan1
 Console # (config)#
```

ip arp inspection logging interval

The **ip arp inspection logging interval** Global Configuration mode command configures the minimal interval between successive ARP SYSLOG messages. To return to the default configuration, use the **no** form of this command.

Syntax

ip arp inspection logging interval {*seconds* | **infinite**}

no ip arp inspection logging interval

Parameters

- *seconds* — Specifies the minimal interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0-86400)
- **infinite —** Specifies SYSLOG messages are not generated.

Default Configuration

The default value is 5 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the minimum ARP SYSLOG message interval to *10* seconds.

```
Console # (config)# ip arp inspection logging interval 10
Console # (config)#
```

show ip arp inspection

The show ip arp inspection EXEC mode command displays the ARP inspection configuration.

Syntax

show ip arp inspection [**ethernet** *interface* **| port-channel** *port-channel-number*]

Parameters

- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies a port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

EXEC

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the ARP inspection configuration.

```
Console# show ip arp inspection
IP ARP inspection is enabled.
IP ARP inspection is configured on following VLANs: 2, 7-18
Verification of packet header is enabled

Syslog messages interval: 5 seconds


Interface                             Trusted

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

1/1                                   yes

1/2                                   no
```

show ip arp inspection list

The **show ip arp inspection list** Priviledged EXEC mode command displays the static ARP binding list.

Syntax

show ip arp inspection list

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the static ARP binding list.

```
Console# show ip arp inspection list

List name: servers
Assigned to VLANs: 1,2


IP                                    ARP

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

172.16.1.1                            0060.704C.7321

172.16.1.2                            0060.704C.7322
```

User Interface Commands

Table 4-35. User Interface Commands

Command	Function	Mode	Page
do	To execute an EXEC-level command from the Global Configuration mode or any configuration submode.	All Configuration Modes	4-652
enable	Enters the Privileged EXEC mode.	UE	4-653
disable	Returns to the User EXEC mode.	PE	4-654
login	Changes a login username.	UE	4-654
configure	Enters the Global Configuration mode.t	PE	4-655
exit (Configuration)	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.	All Configuration Modes	4-655
exit	Closes an active terminal session by logging off the device.	PE,UE	4-656
end	Ends the current configuration session and returns to the Privileged EXEC mode.	All Configuration Modes	4-657
help	Displays a brief description of the help system.	All Command Modes	4-657
terminal datadump	Enables dumping all the output of a show command without prompting. To disable dumping, use the **no** form of this command.	UE	4-658
show history	Lists the commands entered in the current session.	UE	4-659
show privilege	Displays the current privilege level.	PE,UE	4-659

do

To execute an EXEC-level command from the Global Configuration mode or any configuration submode, use the **do** command in any configuration mode.

Syntax

do *command*

Parameters

- ***command*** — The EXEC command to be executed.

Default Setting

This command has no default configuration.

Command Mode

All configuration modes

Command Usage

There are no user guidelines for this command.

Example

The following example execute an EXEC-level command **show vlan**.

```
Console(Config)# do show vlan

VLAN         Name             Port           Type           Authorization

1            default 2/1-4    1/1-2          other          Required

10           VLAN0010         1/3-4          dynamic        Required

11           VLAN0011         1/1-2          static         Required

20           VLAN0020         1/3-4          static         Required

21           VLAN0021                        static         Required

30           VLAN0030                        static         Required

31           VLAN0031                        static         Required

91                            1/1-2          static         Not required

3928         GuestVLAN        1/17           static         Guest
```

Related Commands

configure

enable

The **enable** User EXEC mode command enters the Privileged EXEC mode.

Syntax

enable [*privilege-level*]

Parameters

- *privilege-level* — Privilege level to enter the system. (Range: 1 - 15)

Default Setting

The default privilege level is 15.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example enters Privileged EXEC mode:

```
Console> enable
enter password:
Console#
```

Related Commands

disable

disable

The **disable** Privileged EXEC mode command returns to the User EXEC mode.

Syntax

disable [*privilege-level*]

Parameters

- *privilege-level* — Privilege level to enter the system. (Range: 1 - 15)

Default Setting

The default privilege level is 1.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example return to Users EXEC mode.

```
Console# disable
Console>
```

Related Commands

enable

login

The **login** User EXEC mode command changes a login username.

Syntax

login

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example enters Privileged EXEC mode and logs in with username **admin**.

```
Console> login
User Name:admin
Password:*****
Console#
```

Related Commands

enable

configure

The **configure** Privileged EXEC mode command enters the Global Configuration mode.

Syntax

configure

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example enters Global Configuration mode.

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

Related Commands

enable

disable

exit (Configuration)

The **exit** command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

Syntax

exit

Default Setting

This command has no default configuration.

Command Mode

All configuration modes

Command Usage

There are no user guidelines for this command.

Example

The following example changes the configuration mode from Interface Configuration mode to Privileged EXEC mode.

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

Related Commands

configure

end

exit

The **exit** Privileged/User EXEC mode command closes an active terminal session by logging off the device.

Syntax

exit

Default Setting

This command has no default configuration.

Command Mode

Privileged and User EXEC modes

Command Usage

There are no user guidelines for this command.

Example

The following example closes an active terminal session.

```
Console> exit
```

Related Commands

configure

end

end

The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

Syntax

end

Default Setting

This command has no default configuration.

Command Mode

All configuration modes.

Command Usage

There are no user guidelines for this command.

Example

The following example changes from Global Configuration mode to Privileged EXEC mode.

```
Console(config)# end
Console#
```

Related Commands

exit

help

The **help** command displays a brief description of the help system.

Syntax

help

Default Setting

This command has no default configuration.

Command Mode

All command modes

Command Usage

There are no user guidelines for this command.

Example

The following example describes the help system.

```
Console# help
Help may be requested at any point in a command by entering a question
mark '?'. If nothing matches the currently entered incomplete command, the
help list is empty. This indicates that for a query at this point, there
is no command matching the current input. If the request is within a
command, enter backspace and erase the entered characters to a point where
the request results in a display.
Help is provided when:
1. There is a valid command and a help request is made for entering a
parameter or argument (e.g. 'show ?'). All possible parameters or
arguments for the entered command are displayed.
2. An abbreviated argument is entered and a help request is made for
arguments matching the input (e.g. 'show pr?').
```

Related Commands

login

configure

terminal datadump

The **terminal datadump** User EXEC mode command enables dumping all the output of a show command without prompting. To disable dumping, use the **no** form of this command.

Syntax

terminal datadump

no terminal datadump

Default Setting

Dumping is disabled.

Command Mode

User EXEC mode

Command Usage

By default, a **More** prompt is displayed when the output contains more lines than can be displayed on the screen. Pressing the **Enter** key displays the next line; pressing the Spacebar displays the next screen of output. The datadump command enables dumping all output immediately after entering the show command.

This command is relevant only for the current session.

Example

This example dumps all output immediately after entering a show command.

```
Console> terminal datadump
```

Related Commands

show history

show history

The **show history** User EXEC mode command lists the commands entered in the current session.

Syntax

show history

Default Setting

This command has no default configuration.

Command Mode

User EXEC mode

Command Usage

The buffer includes executed and unexecuted commands.

Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

Example

The following example displays all the commands entered while in the current Privileged EXEC mode.

```
Console# show version
SW version 3.131 (date 23-Jul-2004 time 17:34:19)
HW version 1.0.0

Console# show clock
15:29:03 Jun 17 2004

Console# show history
show version
show clock
show history

3 commands were logged (buffer size is 10)
```

Related Commands

history

history size

show privilege

The **show privilege** Privileged/User EXEC mode command displays the current privilege level.

Syntax

show privilege

Default Setting

This command has no default configuration.

Command Mode

Privileged and User EXEC modes

Command Usage

There are no user guidelines for this command.

Example

The following example displays the current privilege level for the Privileged EXEC mode.

```
Console# show privilege
Current privilege level is 15
```

Related Commands

enable password

username

VLAN Commands

Table 4-36. VLAN Commands

Command	Function	Mode	Page
vlan database	Enters the VLAN Configuration mode.	GC	4-662
vlan	Use the **vlan** VLAN Configuration mode command to create a VLAN. To delete a VLAN, use the **no** form of this command.	VC	4-663
default-vlan vlan	to create a VLAN	CM	4-664
interface vlan	Enters the Interface Configuration (VLAN) mode.	GC	4-664
interface range vlan	Enables simultaneously configuring multiple VLANs.	GC	4-665
name	Adds a name to a VLAN. To remove the VLAN name, use the **no** form of this command.	ICV	4-666
map protocol protocols-group	Maps a protocol to a group of protocols.	ICV	4-666
switchport general map protocols-group vlan	Maps a protocol to a group of protocols.	ICV	4-667
switchport mode	Configures the VLAN membership mode of a port. To return to the default configuration, use the **no** form of this command.	IC	4-668
switchport access vlan	Configures the VLAN ID when the interface is in access mode. To return to the default configuration, use the **no** form of this command.	IC	4-669
switchport trunk allowed vlan	Adds or removes VLANs to or from a trunk port.	IC	4-670
switchport trunk native vlan	Defines the native VLAN when the interface is in trunk mode. To return to the default configuration, use the **no** form of this command.	IC	4-671
switchport general allowed vlan	Adds or removes VLANs from a general port.	IC	4-672
switchport general pvid	Configures the PVID when the interface is in general mode. To return to the default configuration, use the **no** form of this command.	IC	4-673
switchport general ingress-filtering disable	Disables port ingress filtering. To return to the default configuration, use the **no** form of this command.	IC	4-674
switchport general acceptable-frame-type tagged-only	Discards untagged frames at ingress. To return to the default configuration, use the **no** form of this command.	IC	4-675
switchport forbidden vlan	Forbids adding specific VLANs to a port. To return to the default configuration, use the **remove** parameter for this command.	IC	4-676
map mac macs-group	maps a MAC address or range of MAC addresses to a group of MAC addresses	IC	4-677

Table 4-36. VLAN Commands

Command	Function	Mode	Page
switchport general map macs-group vlan	Sets a mac-based classification rule.	IC	4-677
map subnet subnets-group	Maps the IP subnet to a group of IP subnets.	IC	4-678
switchport general map subnets-group vlan	Sets a subnet-based classification rule.	IC	4-679
switchport protected	Overrides the FDB decision and sends all Unicast, Multicast and Broadcast traffic to an uplink port. To return to the default configuration, use the **no** form of the command .	IC	4-680
ip internal-usage-vlan	Reserves a VLAN as the internal usage VLAN of an interface. To return to the default configuration, use the **no** form of this command.	IC	4-681
show vlan	Displays VLAN information.	PE	4-682
show vlan internal usage	Displays a list of VLANs used internally by the device.	PE	4-683
show interfaces switchport	Displays the switchport configuration.	PE	4-684
switchport access multicast-tv vlan	Use the **switchport access multicast-tv vlan** Interface Configuration mode command to enable receiving multicast transmissions from a VLAN that is not the Access port VLAN, while keeping the L2 segregation with subscribers on different Access port VLANs. Use the **no** form of this command to disable receiving multicast transmissions.	IC	4-687
show vlan protocols-groups	Displays protocols-groups information.	PE	4-688
show vlan macs-groups	Displays macs-groups information.	PE	4-688
Show Vlan Subnets-groups	Displays Subnets-groups Information.	PE	4-689
show vlan multicast-tv	Use the show vlan multicast-TV command to display information on the source ports and receiver ports of multicast-TV VLAN.	PE	4-690

vlan database

The **vlan database** Global Configuration mode command enters the VLAN Configuration mode.

Syntax

vlan database

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example enters the VLAN database mode.

```
Console(config)# vlan database
Console(config-vlan)#
```

Related Commands

vlan

name

show vlan

vlan

Use the **vlan** VLAN Configuration mode command to create a VLAN. To delete a VLAN, use the **no** form of this command.

Syntax

vlan *vlan-range*

no vlan *vlan-range*

Parameters

- *vlan-range* — Specifies a list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.

Default Setting

This command has no default configuration.

Command Mode

VLAN Configuration mode

Command Usage

There are no user guidelines for this command.

Example

The following example VLAN number 1972 is created.

```
Console(config)# vlan database
Console(config-vlan)# vlan 1972
```

Related Commands

vlan database

name

show vlan

default-vlan vlan

Use the **vlan** VLAN Configuration mode command to create a VLAN. To restore the default configuration or delete a VLAN, use the **no** form of this command.

Syntax

default-vlan vlan *vlan-id*

no default-vlan vlan

Parameters

- *vlan-id* — VLAN ID of the default VLAN.

Default Configuration

The default configuration is set to one.

Command Mode

VLAN Configuration mode

User Guidelines

There are no user guidelines for this command.

interface vlan

The **interface vlan** Global Configuration mode command enters the Interface Configuration (VLAN) mode.

Syntax

interface vlan *vlan-id*

Parameters

- *vlan-id* — Specifies an existing VLAN ID.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

If the VLAN doesn't exist ("ghost VLAN") only a partial list of the commands are available under the interface VLAN context. The commands that are supported for VLAN that don't exist are:

1) IGMP snooping control

2) Bridge multicast configuration

Example

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27 255.255.255.0
```

Related Commands

vlan database

name

show vlan

interface range vlan

The **interface range vlan** Global Configuration mode command enables simultaneously configuring multiple VLANs.

Syntax

interface range vlan {*vlan-range* | **all**}

Parameters

- *vlan-range* — Specifies a list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.
- **all** — All existing static VLANs.

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution of the command continues on the other interfaces.

Example

The following example groups VLANs 221, 228 and 889 to receive the same command.

```
Console(config)# interface range vlan 221-228,889
Console(config-if)#
```

Related Commands

vlan database

name

show vlan

name

The **name** Interface Configuration mode command adds a name to a VLAN. To remove the VLAN name, use the **no** form of this command.

Syntax

name *string*

no name

Parameters

- *string* — Unique name to be associated with this VLAN. (Range: 1-32 characters)

Default Setting

No name is defined.

Command Mode

Interface Configuration (VLAN) mode. Cannot be configured for a range of interfaces (range context).

Command Usage

There are no user guidelines for this command.

Example

The following example gives VLAN number 19 the name **Marketing**.

```
Console(config)# interface vlan 19
Console(config-if)# name Marketing
```

Related Commands

vlan database

vlan

show vlan

map protocol protocols-group

The **map protocol protocols-group** VLAN Configuration command maps a protocol to a group of protocols. Use the **no** form of this command to delete the map.

Syntax

map protocol *protocol* [*encapsulation*] **protocols-group** *group*

no map protocol *protocol* [*encapsulation*]

Parameters

- *protocol* — The protocol is 16 bits protocol number or one of the reserved names that are defined in the usage guidelines. (Range: 0x0000 – 0x0600)

- *group* — Group number of group of protocols associated together. (Range: 1 – 2147483647)
- *encapsulation* — Currently the protocol “ethernet” is supported. If no option is indicated the default is “ethernet”.

Default Setting

There are no default settings for this command.

Command Mode

VLAN Configuration mode

Command Usage

The following protocol names are reserved for Ethernet Encapsulation:

- ip-arp
- ipx
- ip

Example

The following example maps a protocol 0x0000 to protocol group 1000 for Ethernet port 1/e16 .

```
Console(config-vlan)# map protocol 0x000 ethernet protocols-group 1000
Console(config-if)# switchport mode access
```

Related Commands

vlan database

vlan

show vlan

switchport general map protocols-group vlan

The **switchport general map protocols-group vlan** classification-rules interface configuration command sets a protocol-based classification rule. Use the **no** form of this command to delete a classification.

Syntax

switchport general map protocols-group *group* **vlan** *vlan-id*

no switchport general map protocols-group *group*

Parameters

- *group* — Group number as defined in the map protocol to protocols-group. (Range: 1 - 65535)
- *vlan-id* — Define the VLAN ID in the classifying rule.

Default Setting

There are no default settings for this command.

Command Mode

Interface configuration (Ethernet, port-channel)

Command Usage

The priority between VLAN classification rules is:

1) MAC based VLAN (Best match between the rules)
2) Subnet based VLAN (Best match between the rules)
3) Protocol based VLAN
4) PVID

Example

Console (config-if)# switchport general map protocols-group 1 vlan 8

The following example sets a protocol-based classification rule for Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general map protocols-group 1 vlan 8
```

Related Commands

vlan database

vlan

show vlan

switchport mode

The **switchport mode** Interface Configuration mode command configures the VLAN membership mode of a port. To return to the default configuration, use the **no** form of this command.

Syntax

switchport mode {**access** | **trunk | general**}

no switchport mode

Parameters

- **access** — Indicates an untagged layer 2 VLAN port.
- **trunk** — Indicates a trunking layer 2 VLAN port.
- **general** — Indicates a full 802-1q supported VLAN port.

Default Setting

All ports are in access mode, and belong to the default VLAN (whose VID=1).

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines.

Example

The following example configures Ethernet port 1/e16 as an untagged layer 2 VLAN port.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport mode access
```

Related Commands

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

show interfaces switchport

switchport access multicast-tv vlan

switchport access vlan

The **switchport access vlan** Interface Configuration mode command configures the VLAN ID when the interface is in access mode. To return to the default configuration, use the **no** form of this command.

Syntax

switchport access vlan {*vlan-id* | **dynamic**}

no switchport access vlan

Parameters

- *vlan-id* — Specifies the ID of the VLAN to which the port is configured.
- **dynamic**—Indicates that the port is assigned to a VLAN based on the source MAC address of the host connected to the port.

Default Setting

All ports belong to VLAN 1.

Command Mode

Interface configuration (Ethernet, port-channel) mode

Command Usage

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

Example

The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport access vlan 23
```

Related Commands

switchport mode

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

show interfaces switchport

switchport access multicast-tv vlan

switchport trunk allowed vlan

The **switchport trunk allowed vlan** Interface Configuration mode command adds or removes VLANs to or from a trunk port.

Syntax

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters

- **add** *vlan-list* — List of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list* — List of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Setting

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example adds VLANs 1, 2, 5 to 6 to the allowed list of Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
console(config-if)# switchport trunk allowed vlan add 1-2,5-6
```

Related Commands

switchport mode

switchport access vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

show interfaces switchport

switchport access multicast-tv vlan

switchport trunk native vlan

The **switchport trunk native vlan** Interface Configuration mode command defines the native VLAN when the interface is in trunk mode. To return to the default configuration, use the **no** form of this command.

Syntax

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

Parameters

- *vlan-id* — Specifies the ID of the native VLAN.

Default Setting

VID=1.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

The command adds the port as a member in the VLAN. If the port is already a member in the VLAN (not as a native), it should be first removed from the VLAN.

Example

The following example configures VLAN number 123 as the native VLAN when Ethernet port 1/e16 is in trunk mode.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport trunk native vlan 123
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

show interfaces switchport

switchport access multicast-tv vlan

switchport general allowed vlan

The **switchport general allowed vlan** Interface Configuration mode command adds or removes VLANs from a general port.

Syntax

switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]

switchport general allowed vlan remove *vlan-list*

Parameters

- **add** *vlan-list* — Specifies the list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list* — Specifies the list of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **tagged** — Indicates that the port transmits tagged packets for the VLANs.
- **untagged** — Indicates that the port transmits untagged packets for the VLANs.

Default Setting

If the port is added to a VLAN without specifying tagged or untagged, the default setting is tagged.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

This command enables changing the egress rule (e.g., from tagged to untagged) without first removing the VLAN from the list.

Example

The following example adds VLANs 2, 5, and 6 to the allowed list of Ethernet port 1/ e16 .

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general allowed vlan add 2,5-6 tagged
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

show interfaces switchport

switchport access multicast-tv vlan

switchport general pvid

The **switchport general pvid** Interface Configuration mode command configures the PVID when the interface is in general mode. To return to the default configuration, use the **no** form of this command.

Syntax

switchport general pvid *vlan-id*

no switchport general pvid

Parameters

- *vlan-id* — Specifies the PVID (Port VLAN ID).

Default Setting

If the default VLAN is enabled, PVID = 1. Otherwise, PVID=4095.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures the PVID for Ethernet port 1/e16, when the interface is in general mode.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general pvid 234
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

show interfaces switchport

switchport access multicast-tv vlan

switchport general ingress-filtering disable

The **switchport general ingress-filtering disable** Interface Configuration mode command disables port ingress filtering. To return to the default configuration, use the **no** form of this command.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Default Setting

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example disables port ingress filtering on Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general ingress-filtering disable
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

show interfaces switchport

switchport access multicast-tv vlan

switchport general acceptable-frame-type tagged-only

The **switchport general acceptable-frame-type tagged-only** Interface Configuration mode command discards untagged frames at ingress. To return to the default configuration, use the **no** form of this command.

Syntax

switchport general acceptable-frame-type tagged-only

no switchport general acceptable-frame-type tagged-only

Default Setting

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

There are no user guidelines for this command.

Example

The following example configures Ethernet port 1/e16 to discard untagged frames at ingress.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general acceptable-frame-type tagged-only
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport forbidden vlan

show interfaces switchport

switchport access multicast-tv vlan

switchport forbidden vlan

The **switchport forbidden vlan** Interface Configuration mode command forbids adding specific VLANs to a port. To return to the default configuration, use the **remove** parameter for this command.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters

- **add** *vlan-list* — Specifies the list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list* — Specifies the list of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Setting

All VLANs are allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Command Usage

This command can be used to prevent GVRP from automatically making the specified VLANs active on the selected ports.

Example

The following example forbids adding VLAN IDs 234 to 256 to Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport forbidden vlan add 234-256
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

show interfaces switchport

switchport access multicast-tv vlan

map mac macs-group

The **map mac macs-group** VLAN Configuration mode command maps a MAC address or range of MAC addresses to a group of MAC addresses. To delete the map, use the **no** form of this command.

Syntax

map mac *mac-address* {prefix-mask | **host**} **macs-group** *group*

no map mac *mac-address* {*prefix-mask* | **host**}

Parameters

- *mac-address* — Specifies the MAC address to be entered to the group.
- *prefix-mask* — Mask bits. The format is "/n", where n is an integer number that specifies the number of 1's in the mask.
- **host** — All 1's mask.
- *group* — Indicates the group number. (Range: 1-2147483647)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Configuration mode

User Guidelines

There are no user guidelines for this command.

switchport general map macs-group vlan

The **switchport general map macs-group vlan** interface configuration command sets a mac-based classification rule. Use the **no** form of this command to delete a classification.

Syntax

switchport general map macs-group *group* **vlan** *vlan-id*

no switchport general map macs-group *group*

Parameters

- *group* — Group number. (Range: 1 – 2147483647)
- *vlan-id* — Define the VLAN ID that is associated with the rule.

Default Setting

There is no default setting for this command.

Command Mode

Interface configuration (Ethernet, port-channel)

Command Usage

MAC based VLAN rules cannot contain overlapping ranges on the same interface. The priority between VLAN classification rules is:

1) MAC based VLAN (Best match between the rules)
2) Subnet based VLAN (Best match between the rules)
3) Protocol based VLAN
4) PVID

Example

The following example maps group 100 to VLAN 23 for Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general map macs-group 100 vlan 23
```

Related Commands

switchport mode

switchport access vlan

map subnet subnets-group

The **map subnet subnets-group** VLAN Configuration mode command maps the IP subnet to a group of IP subnets. To delete the map, use the **no** form of this command.

Syntax

map subnet ip-address *prefix-mask* **subnets-group** *group*

no map subnet *ip-address prefix-mask*

Parameters

- *ip-address* — Specifies the IP address prefix of the subnet to be entered to the group.
- *prefix-mask* — Mask bits. The format is IP address format.
- *group* — Indicates the group number. (Range: 1-2147483647)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Configuration mode

User Guidelines

There are no user guidelines for this command.

switchport general map subnets-group vlan

The **switchport general map subnets-group vlan** interface configuration command sets a subnet-based classification rule. Use the **no** form of this command to delete a classification.

Syntax

switchport general map subnets-group *group* **vlan** *vlan-id*

no switchport general map subnets-group *group*

Parameters

- *group* — Group number. (Range: 1 – 2147483647)
- *vlan-id* — Define the VLAN ID that is associated with the rule.

Default Setting

There is no default setting for this command.

Command Mode

Interface configuration (Ethernet, port-channel)

Command Usage

The priority between VLAN classification rules is:

1) MAC based VLAN (Best match between the rules)
2) Subnet based VLAN (Best match between the rules)
3) Protocol based VLAN
4) PVID

Example

The following example maps sub-group 200 to VLAN 46 for Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport general map subnets-group 200 vlan 46
```

Related Commands

switchport mode

switchport access vlan

switchport protected

The **switchport protected** Interface Configuration mode command overrides the FDB decision and sends all Unicast, Multicast and Broadcast traffic to an uplink GE port. To return to the default configuration, use the **no** form of the command .

Syntax

switchport protected {**ethernet** port | **port-channel** port-channel-number }

no switchport protected

Parameters

- *port* — Specifies the uplink Ethernet GE port.
- *port-channel-number*— Specifies the port-channel uplink GE port.

Default Setting

Overriding the FDB decision is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel)

Command Usage

Packets to the MAC address of the device are sent to the device and not forwarded to the uplink.

IGMP snooping works on PVE protected ports; however forwarding of query/ reports is not limited to the PVE uplink.

Example

The following example overrides the FDB decision and sends all Unicast, Multicast and Broadcast traffic to Ethernet port 1/g8.

```
Console# config
Console(config)# interface ethernet 1/g8
Console(config-if)# switchport protected
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

show interfaces switchport

switchport access multicast-tv vlan

ip internal-usage-vlan

The **ip internal-usage-vlan** Interface Configuration mode command reserves a VLAN as the internal usage VLAN of an interface. To return to the default configuration, use the **no** form of this command.

Syntax

ip internal-usage-vlan *vlan-id*

no ip internal-usage-vlan

Parameters

- *vlan-id* — Specifies the ID of the internal usage VLAN.

Default Setting

The software reserves a VLAN as the internal usage VLAN of an interface.

Command Mode

Interface Configuration (Ethernet, port-channel) mode. The command cannot be configured for a range of interfaces.

Command Usage

- An internal usage VLAN is required when an IP interface is configured on an Ethernet port or port-channel.
- This command enables the user to configure the internal usage VLAN of a port. If an internal usage VLAN is not configured and the user wants to configure an IP interface, an unused VLAN is selected by the software.
- If the software selected a VLAN for internal use and the user wants to use that VLAN as a static or dynamic VLAN, the user should do one of the following:
- Remove the IP interface.
- Create the VLAN and recreate the IP interface.
- Use this command to explicitly configure a different VLAN as the internal usage VLAN.

Example

The following example reserves an unused VLAN as the internal usage VLAN of ethernet port 1/e8.

```
Console# config
Console(config)# interface ethernet 1/e8
Console(config-if)# ip internal-usage-vlan
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

show interfaces switchport

switchport access multicast-tv vlan

show vlan

The **show vlan** Privileged EXEC mode command displays VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

Parameters

- *vlan-id* — specifies a VLAN ID.
- *vlan-name* — Specifies a VLAN name string. (Range: 1 - 32 characters)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays all VLAN information.

```
Console# show vlan


VLAN     Name          Ports                 Type          Authorization
----     -------       --------              ----          -------------
1        default       1/e1-e2, 2/e1-e4      other         Required
10       VLAN0010      1/e3-e4               dynamic       Required
11       VLAN0011      1/e1-e2               static        Required
20       VLAN0020      1/e3-e4               static        Required
21       VLAN0021                            static        Required
30       VLAN0030                            static        Required
31       VLAN0031                            static        Required
```

```
91       VLAN0011     1/e1-e2               static       Not Required
3978     Guest VLAN   1/e17                 guest        -
```

Related Commands

vlan database

vlan

name

show vlan internal usage

The **show vlan internal usage** Privileged EXEC mode command displays a list of VLANs used internally by the device.

Syntax

show vlan internal usage

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays VLANs used internally by the device.

```
Console# show vlan internal usage


VLAN         Usage                   IP address          Reserved
----         ---------               ----------          --------
1007         Eth 1/e21               Active              No
1008         Eth 1/e22               Inactive            Yes
1009         Eth 1/e23               Active              Yes
```

Related Commands

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport forbidden vlan

show interfaces switchport

The **show interfaces switchport** Privileged EXEC mode command displays the switchport configuration.

Syntax

show interfaces switchport {ethernet *interface* | **port-channel** *port-channel-number*}

Parameters

- *interface* — A valid Ethernet port number.
- *port-channel-number* — A valid port-channel number.

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the switchport configuration for Ethernet port 1/e1.

```
Console# show interface switchport ethernet 1/e1

Port 1/e1:

VLAN Membership mode: General


Operating parameters:

PVID: 1 (default)

Ingress Filtering: Enabled

Acceptable Frame Type: All

GVRP status: Enabled

Protected: Enabled, Uplink is 1/e9.


Port 1/e1 is member in:

Vlan             Name                   Egress rule         Type

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

1                default                untagged            System

8                VLAN008                tagged              Dynamic

11               VLAN011                tagged              Static
```

```
72                VLAN0072                untagged            Static


Static configuration:

PVID: 1 (default)

Ingress Filtering: Enabled

Acceptable Frame Type: All


Port 1/e1 is statically configured to:

Vlan              Name                    Egress rule

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

1                 default                 untagged

11                VLAN011                 tagged

72                VLAN0072                untagged


Forbidden VLANS:

VLAN              Name

----              ----

73                out


Console# show interface switchport ethernet 1/e2

Port 1/e2:

VLAN Membership mode: General


Operating parameters:

PVID: 4095 (discard vlan)

Ingress Filtering: Enabled

Acceptable Frame Type: All


Port 1/e1 is member in:

Vlan              Name                    Egress rule         Type

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

91                IP Telephony            tagged              Static
```

```
Static configuration:
PVID: 8
Ingress Filtering: Disabled
Acceptable Frame Type: All

Port 1/e2 is statically confgiured to:
Vlan             Name                   Egress rule
----             ------------           -----------
8                VLAN0072               untagged
91               IP Telephony           tagged

Forbidden VLANS:
VLAN             Name
----             ----
73               out

Port 2/e19

Static configuration:
PVID: 2922
Ingress Filtering: Enabled
Acceptable Frame Type: Untagged
GVRP status: Disabled
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

switchport access multicast-tv vlan

switchport access multicast-tv vlan

Use the **switchport access multicast-tv vlan** Interface Configuration mode command to enable receiving multicast transmissions from a VLAN that is not the Access port VLAN, while keeping the L2 segregation with subscribers on different Access port VLANs. Use the **no** form of this command to disable receiving multicast transmissions.

Syntax

switchport access multicast-tv vlan *vlan-id*

no switchport access multicast-tv vlan

Parameters

- *vlan-id* — VLAN ID of the Multicast TV VLAN.

Default Configuration

Disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The user can receive multicast transmit transmissions on the multicast TV VLAN, but cannot transmit

All IGMP reports are associated with the multicast TV VLAN.

Example

The following example configures Multicast TV VLAN 20 on Ethernet port 1/e16.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# switchport access multicast-tv vlan 20
```

Related Commands

switchport mode

switchport access vlan

switchport trunk allowed vlan

switchport trunk native vlan

switchport general allowed vlan

switchport general pvid

switchport general ingress-filtering disable

switchport general acceptable-frame-type tagged-only

switchport forbidden vlan

show interfaces switchport

show vlan protocols-groups

The **show vlan protocols-groups** EXEC command displays protocols-groups information.

Syntax

show vlan protocols-groups

Default Configuration

There are no user default configuration for this command.

Command Mode

Priviledged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures displays IPMP Snooping configuration.

```
Console> show vlan protocols-groups

Protocol                 Encapsulation            Group

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

0x800 (IP)               Ethernet                 1

0x806 (ARP)              Ethernet                 1

0x8898                   Ethernet                 3
```

Related Commands

switchport mode

switchport access vlan

show vlan macs-groups

The **show vlan protocols-groups** Privileged EXEC mode command displays macs-groups information.

Syntax

show vlan macs-groups

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays macs-groups information.

```
Console# show vlan macs-groups


MAC                   Prefix                        Group

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

0060.704C.73FF        FFFF.FFFF.0000                1

0060.704D.73FF        FFFF.FFFF.0000                1
```

show vlan subnets-groups

The **show vlan subnets-groups** Privileged EXEC mode command displays macs-groups information.

Syntax

show vlan subnets-groups

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays subnets-groups information.

```
Console# show vlan subnets-groups


MAC                    Prefix         Group

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

172.16.1.0             255.255.255.   1
                       0

172.16.2.0             255.255.255.   1
                       0
```

show vlan multicast-tv

Use the **show multicast-tv** command to display information on the source ports and receiver ports of multicast-tv vlan.

Syntax

show vlan multicast-tv *vlan-id*

Parameters

- *vlan-id* — VLAN ID of the Multicast TV VLAN.

Default Configuration

This command has no default configuration.

Command Mode

Priviledged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures displays IPMP Snooping configuration.

```
Console# show ip igmp multicast-tv 1000
Source Ports           Receiver Ports
1/8, 1/9               2/1-18, 3/1-18, 4/1-18
```

The following table describes significant fields shown above:

Field	Description
Source Ports	Ports that can transmit and receive traffic to the VLAN.
Receiver Ports	orts that can only receive traffic from the VLAN.

Related Commands

show interfaces switchport

Web Server Commands

Table 4-37. Web Server Commands			
Command	Function	Mode	Page
ip http server	Enables configuring the device from a browser. To disable this function, use the **no** form of this command.	GC	4-691
ip http port	Specifies the TCP port to be used by the Web browser interface. To return to the default configuration, use the **no** form of this command.	GC	4-692
ip http exec-timeout	Sets the interval, which the system waits to user input in http sessions before automatic logoff.	GC	4-693
ip https server	Enables configuring the device from a secured browser. To return to the default configuration, use the **no** form of this command.	GC	4-693
ip https port	Specifies the TCP port used by the server to configure the device through the Web browser. To return to the default configuration, use the **no** form of this command.t	GC	4-694
ip https exec-timeout	sets the interval that the system waits to user input in https sessions before automatic logoff.	GC	4-695
crypto certificate generate	Generates a self-signed HTTPS certificate.	GE	4-695
crypto certificate request	Generates and displays certificate requests for HTTPS.	PE	4-696
crypto certificate import	Imports a certificate signed by the Certification Authority for HTTPS.	GC	4-698
ip https certificate	Configures the active certificate for HTTPS. To return to the default configuration, use the **no** form of this command.	GC	4-699
show crypto certificate mycertificate	Displays the SSH certificates of the device.	PE	4-699
show ip http	Displays the HTTP server configuration.	PE	4-700
show ip https	Displays the HTTPS server configuration.	PE	4-701

ip http server

The **ip http server** Global Configuration mode command enables configuring the device from a browser. To disable this function, use the **no** form of this command.

Syntax

ip http server

no ip http server

Default Setting

HTTP server is enabled.

Command Mode

Global Configuration

Command Usage

Only a user with access level 15 can use the Web server.

Example

The following example enables configuring the device from a browser.

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

Related Commands

ip http port

show ip http

ip http port

The **ip http port** Global Configuration mode command specifies the TCP port to be used by the Web browser interface. To return to the default configuration, use the **no** form of this command.

Syntax

ip http port *port-number*

no ip http port

Parameters

- *port-number* — Port number for use by the HTTP server. (Range: 1 - 65535)

Default Setting

The default port number is 80.

Command Mode

Global Configuration

Command Usage

Use the **crypto certificate generate** Global Configuration mode command to generate an HTTPS certificate.

Specifying 0 as the port number effectively disables HTTP access to the device.

Example

The following example configures the http port number to 100.

```
Console(config)# ip http port 100
```

Related Commands

ip http server

show ip http

ip http exec-timeout

The **ip http exec-timeout** Global Configuration mode command sets the interval, which the system waits to user input in http sessions before automatic logoff. To restore the default configuration, use the no form of this command.

Syntax

ip http exec-timeout *minutes* [*seconds*]

no ip http exec-timeout

Parameters

- *minutes* — Integer that specifies the number of minutes.
- *seconds* — Additional time intervals in seconds.

Default Configuration

The default is 10 minutes.

Command Mode

Global Configuration mode

User Guidelines

This command also configures the exec-timeout for HTTPS in case the HTTPS timeout was not set.

To specify no timeout, enter the ip https exec-timeout 0 0 command.

ip https server

The **ip https server** Global Configuration mode command enables configuring the device from a secured browser. To return to the default configuration, use the **no** form of this command.

Syntax

ip https server

no ip https server

Default Setting

Disabled.

Command Mode

Global Configuration mode

Command Usage

Use the **crypto certificate generate** Global Configuration mode command to generate an HTTPS certificate.

Example

The following example enables configuring the device from a secured browser.

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

Related Commands

ip https port

ip https certificate

show ip https

ip https port

The **ip https port** Global Configuration mode command specifies the TCP port used by the server to configure the device through the Web browser. To return to the default configuration, use the **no** form of this command.

Syntax

ip https port *port-number*

no ip https port

Parameters

- *port-number* — Port number to be used by the HTTP server. (Range: 0 - 65535)

Default Setting

The default port number is 443.

Command Mode

Global Configuration mode

Command Usage

Specifying 0 as the port number effectively disables HTTP access to the device.

Example

The following example configures the https port number to 100.

```
Console(config)# ip https port 100
```

Related Commands

ip https server

ip https certificate

show ip https

ip https exec-timeout

The **ip https exec-timeout** Global Configuration mode command sets the interval that the system waits to user input in https sessions before automatic logoff. To restore the default configuration, use the no form of this command.

Syntax

ip https exec-timeout *minutes* [*seconds*]

no ip https exec-timeout

Parameters

- *minutes* — Integer that specifies the number of minutes. (Range: 1 - 65535)
- *seconds* — Additional time intervals in seconds. (Range: 0-59)

Default Configuration

The default configuration is the exec-timeout set by the ip http exec-timeout command.

Command Mode

Global Configuration mode

User Guidelines

To specify no timeout, enter the ip https exec-timeout 0 0 command.

crypto certificate generate

The **crypto certificate generate** Global Configuration mode command generates a self-signed HTTPS certificate.

Syntax

crypto certificate [*number*] **generate** [**key-generate** *length*][**cn** *common-name*][**ou** *organization-unit*][or *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*] [**duration** *days*]

Parameters

- *number* — Specifies the certificate number. (Range: 1 - 2)
- **key-generate** — Regenerate the SSL RSA key.
- *length* — Specifies the SSL RSA key length. (Range: 512 - 2048)
- *common- name* — Specifies the fully qualified URL or IP address of the device. (Range: 1 - 64)
- *organization* — Specifies the organization name. (Range: 1 - 64)
- *organization-unit* — Specifies the organization-unit or department name. (Range: 1 - 64)
- *location* — Specifies the location or city name. (Range: 1 - 64)
- *state* — Specifies the state or province name. (Range: 1 - 64)
- *country* — Specifies the country name. (Range: 2 - 2)
- *days* — Specifies number of days certification is valid. (Range: 30 - 3650)

Default Setting

The Certificate and SSL's RSA key pairs do not exist.

If no certificate number is specified, the default certificate number is 1.

If no RSA key length is specified, the default length is 1024.

If no URL or IP address is specified, the default common name is the lowest IP address of the device at the time that the certificate is generated.

If the number of days is not specified, the default period of time that the certification is valid is 365 days.

Command Mode

Global Configuration mode

Command Usage

The command is not saved in the device configuration; however, the certificate and keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

Use this command to generate a self-signed certificate for the device.
If the RSA keys do not exist, parameter **key-generate** must be used.

Example

The following example regenerates an HTTPS certificate.

```
Console(config)# crypto certificate 1 generate key-generate
```

Related Commands

crypto certificate request

crypto certificate import

ip https certificate

show crypto certificate mycertificate

crypto certificate request

The **crypto certificate request** Privileged EXEC mode command generates and displays certificate requests for HTTPS.

Syntax

crypto certificate *number* **request** [**cn** *common-name*]**[ou** *organization-unit***][or** *organization***] [loc** *location***] [st** *state***] [cu** *country***]**

Parameters

- *number* — Specifies the certificate number. (Range: 1 - 2)
- *common-name* — Specifies the fully qualified URL or IP address of the device. (Range: 1- 64)
- *organization-unit* — Specifies the organization-unit or department name. (Range: 1- 64)

- *organization* — Specifies the organization name. (Range: 1- 64)
- *location* — Specifies the location or city name. (Range: 1- 64)
- *state* — Specifies the state or province name. (Range: 1- 64)
- *country* — Specifies the country name. (Range: 1- 2)

Default Setting

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

Command Usage

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request you must first generate a self-signed certificate using the **crypto certificate generate** Global Configuration mode command. Be aware that you have to reenter the certificate fields.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** Global Configuration mode command to import the certificate into the device. This certificate replaces the self-signed certificate.

Example

The following example generates and displays a certificate request for HTTPS.

```
Console# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa

g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----
CN= router.gm.com
0= General Motors
C= US
```

Related Commands

crypto certificate generate

crypto certificate import

ip https certificate

show crypto certificate mycertificate

crypto certificate import

The **crypto certificate import** Global Configuration mode command imports a certificate signed by the Certification Authority for HTTPS.

Syntax

crypto certificate *number* **import**

Parameters

- *number* — Specifies the certificate number. (Range: 1 - 2)

Default Setting

This command has no default configuration.

Command Mode

Global Configuration mode

Command Usage

Use this command to enter an external certificate (signed by Certification Authority) to the device. To end the session, enter an empty line.

The imported certificate must be based on a certificate request created by the **crypto certificate request** Privileged EXEC mode command.

If the public key found in the certificate does not match the device's SSL RSA key, the command fails.

This command is not saved in the device configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).

Examples

The following example imports a certificate signed by Certification Authority for HTTPS.

```
Console(config)# crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

Related Commands

crypto certificate generate

crypto certificate request

ip https certificate

show crypto certificate mycertificate

ip https certificate

The **ip https certificate** Global Configuration mode command configures the active certificate for HTTPS. To return to the default configuration, use the **no** form of this command.

Syntax

ip https certificate *number*

no ip https certificate

Parameters

- *number* — Specifies the certificate number. (Range: 1 - 2)

Default Setting

Certificate number 1.

Command Mode

Global Configuration mode

Command Usage

The **crypto certificate generate** command should be used to generate HTTPS certificates.

Example

The following example configures the active certificate for HTTPS.

```
Console(config)# ip https certificate 1
```

Related Commands

ip https server

ip https port

show ip https

crypto certificate generate

crypto certificate request

crypto certificate import

show crypto certificate mycertificate

show crypto certificate mycertificate

The **show crypto certificate mycertificate** Privileged EXEC mode command displays the SSH certificates of the device.

Syntax

show crypto certificate mycertificate [*number***]**

Parameters

- *number* — Specifies the certificate number. (Range: 1- 2)

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the certificate.

```
Console# show crypto certificate mycertificate 1
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----



Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

Related Commands

crypto certificate generate

crypto certificate request

crypto certificate import

ip https certificate

show ip http

The **show ip http** Privileged EXEC mode command displays the HTTP server configuration.

Syntax

show ip http

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the HTTP server configuration.

```
Console# show ip http
HTTP server enabled. Port: 80
```

Related Commands

ip http server

ip http port

show ip https

The **show ip https** Privileged EXEC mode command displays the HTTPS server configuration.

Syntax

show ip https

Default Setting

This command has no default configuration.

Command Mode

Privileged EXEC mode

Command Usage

There are no user guidelines for this command.

Example

The following example displays the HTTP server configuration.

```
Console# show ip https
HTTPS server enabled. Port: 443



Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2004 to 8/9/2005
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788



Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2004 to 8/9/2005
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```

Related Commands

ip https server

ip https port

ip https certificate

Appendix A. Configuration Examples

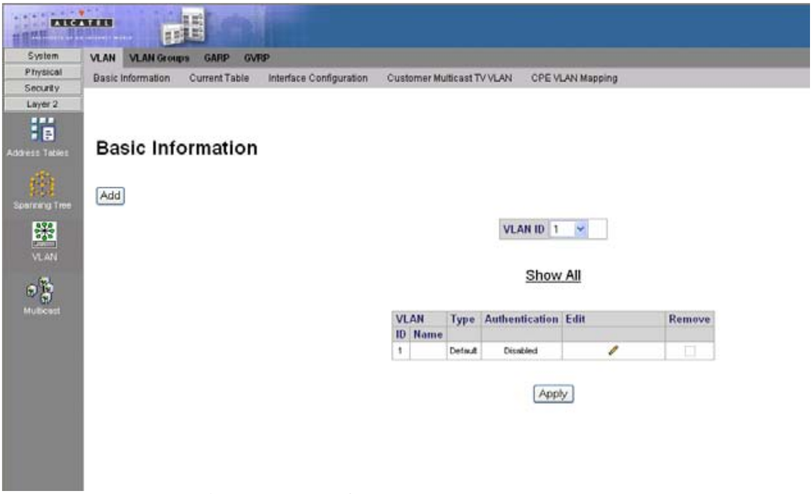
This appendix contains configuration example for the Customer VLANs, and Multicast TV, and contains the following sections:

- Configuring QinQ
- Configuring Multicast TV
- Configuring Customer VLANs

Configuring QinQ

This section contains information for configuring Customer VLANs using the Web Interface and using the CLI. QinQ tagging allows network managers to add an additional tag to previously tagged packets. Customer VLANs are configured using QinQ. Adding additional tags to the packets helps create more VLAN space. The added tag provides an VLAN ID to each customer, this ensures private and segregated network traffic. The VLAN ID tag is assigned to a customer port in the service providers network. The designated port then provides additional services to the packets with the double-tags. This allows administrators to expand service to VLAN users. To configure customer VLANs:

1. Click **Layer 2 > VLAN > VLAN > Basic Information**. The *VLAN Basic Information Page* opens.



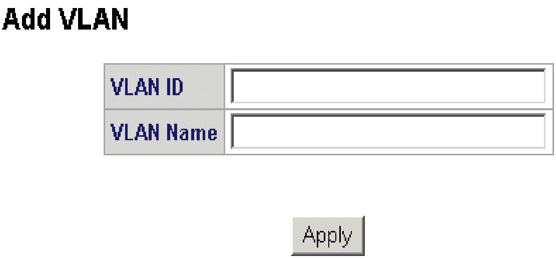
Basic Information

VLAN ID 1

VLAN ID	VLAN Name	Type	Authentication	Edit	Remove
1		Default	Disabled	✎	□

Figure 1. VLAN Basic Information Page

2. Click Add . The *Add 802.1q VLAN Page* opens:



Add VLAN

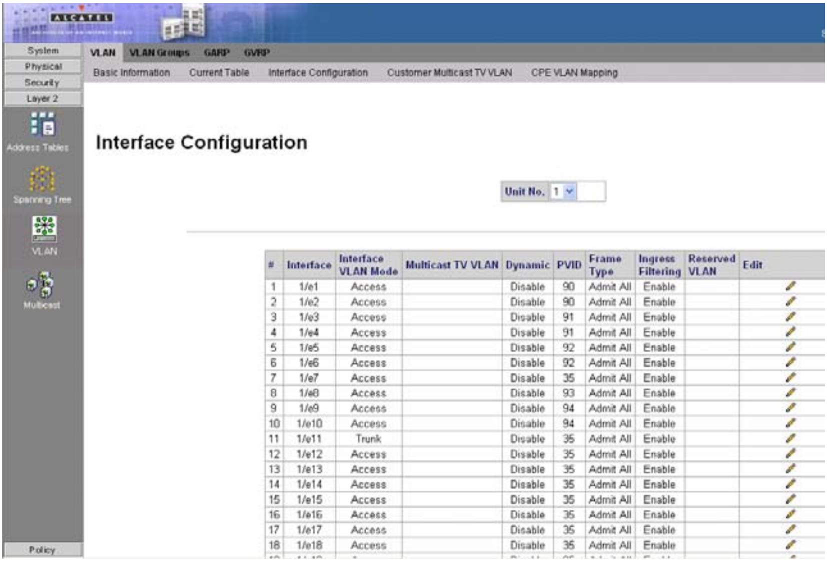
VLAN ID	
VLAN Name	

Figure 2. Add 802.1q VLAN Page

3. Define the *VLAN ID* and *VLAN Name* field.

4. Click Apply.

5. Click **Layer 2 > VLAN > VLAN > Interface Configuration**. The *VLAN Interface Configuration Page* opens.



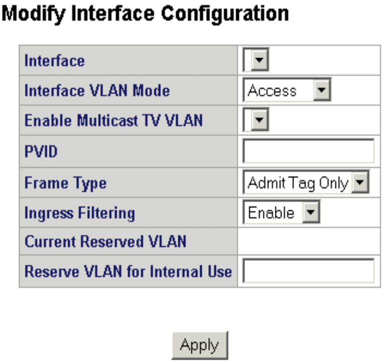
Interface Configuration

Unit No. 1

#	Interface	Interface VLAN Mode	Multicast TV VLAN	Dynamic	PVID	Frame Type	Ingress Filtering	Reserved VLAN	Edit
1	1/e1	Access		Disable	90	Admit All	Enable		✎
2	1/e2	Access		Disable	90	Admit All	Enable		✎
3	1/e3	Access		Disable	91	Admit All	Enable		✎
4	1/e4	Access		Disable	91	Admit All	Enable		✎
5	1/e5	Access		Disable	92	Admit All	Enable		✎
6	1/e6	Access		Disable	92	Admit All	Enable		✎
7	1/e7	Access		Disable	35	Admit All	Enable		✎
8	1/e8	Access		Disable	93	Admit All	Enable		✎
9	1/e9	Access		Disable	94	Admit All	Enable		✎
10	1/e10	Access		Disable	94	Admit All	Enable		✎
11	1/e11	Trunk		Disable	35	Admit All	Enable		✎
12	1/e12	Access		Disable	35	Admit All	Enable		✎
13	1/e13	Access		Disable	35	Admit All	Enable		✎
14	1/e14	Access		Disable	35	Admit All	Enable		✎
15	1/e15	Access		Disable	35	Admit All	Enable		✎
16	1/e16	Access		Disable	35	Admit All	Enable		✎
17	1/e17	Access		Disable	35	Admit All	Enable		✎
18	1/e18	Access		Disable	35	Admit All	Enable		✎

Figure 3. VLAN Interface Configuration Page

6. Click on a previously defined customer VLAN row. The *Modify VLAN Interface Configuration Page* opens:



Modify Interface Configuration

Interface	▾
Interface VLAN Mode	Access ▾
Enable Multicast TV VLAN	▾
PVID	
Frame Type	Admit Tag Only ▾
Ingress Filtering	Enable ▾
Current Reserved VLAN	
Reserve VLAN for Internal Use	

Figure 4. Modify VLAN Interface Configuration Page

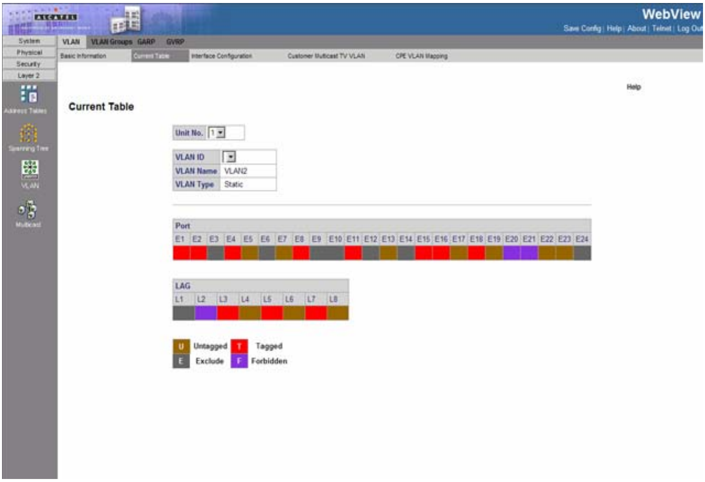
7. Select the interface.

8. Set the *VLAN Interface Mode* field to *Customer*.

9. Define the remaining fields.

10. Click Apply. The VLAN interface settings are saved, and the device is updated.

11. Click **Layer 2 > VLAN > VLAN > Current Table**. The *VLAN Current Table* opens.



Current Table

Unit No.	1 ▾

VLAN ID	▾
VLAN Name	VLAN2
VLAN Type	Static

Port																							
E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18	E19	E20	E21	E22	E23	E24
🟥	🟥	⬛	🟥	🟫	⬛	🟫	🟥	⬛	⬛	🟥	⬛	🟫	⬛	🟥	🟥	🟫	🟥	🟫	🟪	🟪	🟫	🟫	⬛

LAG							
L1	L2	L3	L4	L5	L6	L7	L8
⬛	🟪	🟥	🟫	🟥	🟫	🟥	🟫

🟫 U Untagged 🟥 T Tagged
⬛ E Exclude 🟪 F Forbidden

Figure 5. VLAN Current Table

12. Select the VLAN ID.

13. Add the ports to the VLAN.

14. Click Apply. The customer VLAN is defined, and the device is updated.

Configuring Customer VLANs using the CLI

As an example for configuring QinQ. The following figure illustrates the configuration example being described.

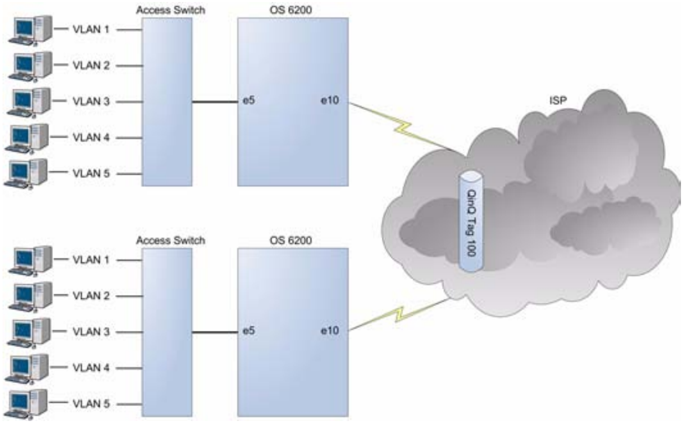


Figure 6. QinQ Configuration Example

To configure QinQ, perform the following:

1. Enter the global configuration mode.

```
Console>enable
Console#config
Console (config)#
```

2. Enter the VLAN configuration mode.

```
Console (config)# vlan database
Console (config-vlan)#
```

3. Create VLAN in the VLAN database.

```
Console (config-vlan)# vlan 100
Console (config-vlan)# exit
```

4. Configure port e5 as a customer port for VLAN 100:

```
Console (config)# interface ethernet e5
Console (config-if)# switchport mode customer
Console (config-if)# switchport customer vlan 100
Console (config-if)# exit
Console (config)#
```

5. Configure port e10 as a trunked port, tagged for VLAN 100.

```
Console (config)# interface ethernet e10
Console (config-if)# switchport mode trunk
Console (config-if)# switchport trunk allowed vlan add 100
Console (config-if)# exit
Console (config)#
```

The following is an example of the QinQ show commands

```
console# show interfaces switchport ethernet 1/e5
Port: 1/e5
Port Mode: Customer
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 100
Protected: Disabled

Port is member in:


 Vlan              Name              Egress rule    Port Membership Type
 ----     -----------------------    -----------    --------------------
 100                100              Untagged       Static


Forbidden VLANS:


 Vlan              Name
 ----     -----------------------




Classification rules:

Protocol based VLANs:


 Group ID          Vlan ID
 --------    ------------------




Mac based VLANs:
  Group ID         Vlan ID
  --------    ------------------



Subnet based VLANs:


  Group ID         Vlan ID
  --------    ------------------


console#
```

Configuring Multicast TV

For an example of configuring Multicast TV, triple play, there are two service providers each with two customers CPE 1 and CPE 2. The example configuration is for transmitting multicast streams from both service providers A and B, to each of the CPE customers. For this purpose port e4 is configured as a trunked port, tagged for VLANs 1001, 1048, 3000, 3001, with port e1 and e48 configured as the triple play ports connected to the customer site.

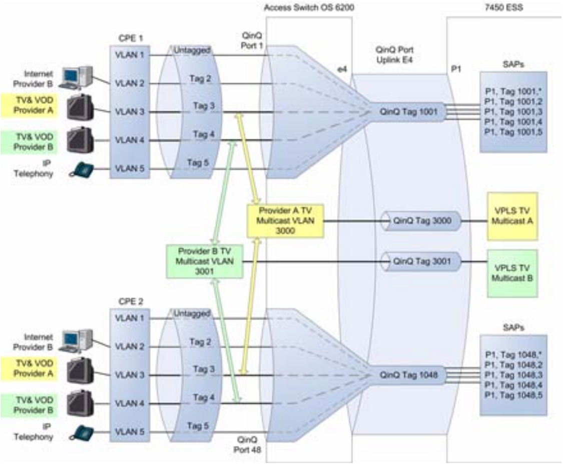


Figure 7. Triple Play Configuration

To configure triple play using CLI, perform the following:

1. Enter the global configuration mode.

```
Console>enable
Console#config
Console (config)#
```

2. Enter the VLAN configuration mode.

```
Console (config)# vlan database
Console (config-vlan)#
```

3. Create VLANs for customer port 1 and port 48 for QinQ. Each customer has separate VLAN.

```
Console (config-vlan)# vlan 1001
Console (config-vlan)# vlan 1048
```

4. Create a VLAN for configuring Multicast TV provider A.

```
Console (config-vlan)# vlan 3000
```

5. Create a VLAN for configuring Multicast TV provider B.

```
Console (config-vlan)# vlan 3001
```

6. Map the internal CPE VLAN 3 to the Multicast TV VLAN 3001.

```
Console (config)# ip igmp snooping map cpe vlan 3 multicast-tv vlan
3001
```

7. Map the internal CPE VLAN 4 to the Multicast TV VLAN 3000.

```
Console (config)# ip igmp snooping map cpe vlan 4 multicast-tv vlan
3000
```

8. Configure the VLAN membership mode of port e1 as a customer port on VLAN 1001.

```
Console (Config)# interface ethernet e1
Console (config-if)# switchport mode customer
Console (config-if)# switchport customer vlan 1001
```

9. Configure port e1 to enable receiving multicast transmissions from a VLAN that is not the customer port’s VLAN.

```
Console (config-if)# switchport customer multicast-tv vlan add 3000
Console (config-if)# switchport customer multicast-tv vlan add 3001
```

10. Configure the VLAN membership mode of port e48 as a customer port on VLAN 1048.

```
Console (Config)# interface ethernet e48
Console (config-if)# switchport mode customer
Console (config-if)# switchport customer vlan 1048
```

11. Configure port e48 to enable receiving multicast transmissions from a VLAN that is not the customer port’s VLAN.

```
Console (config-if)# switchport customer multicast-tv vlan add 3000
Console (config-if)# switchport customer multicast-tv vlan add 3001
```

12. To configure the QinQ uplink, configure port e4 as a trunked port, tagged for VLANs 1001, 1048, 3000 and 3001.

```
Console (Config)# interface ethernet e4
Console (config-if)# switchport mode trunk
Console (config-if)# switchport trunk allowed vlan add 1001
Console (config-if)# switchport trunk allowed vlan add 1048
Console (config-if)# switchport trunk allowed vlan add 3000
Console (config-if)# switchport trunk allowed vlan add 3001
```

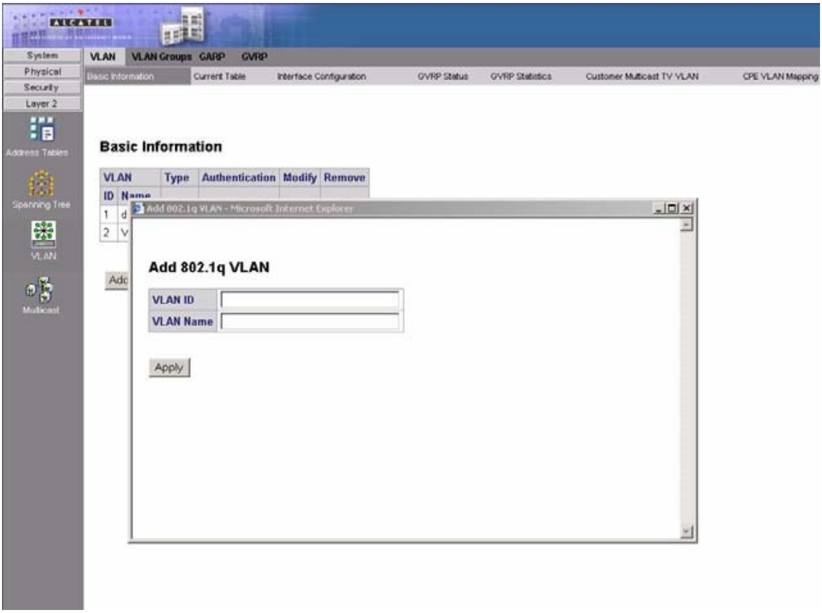
13. View the configuration.

```
Console# show ip igmp snooping cpe vlans

CPE VLAN     Multicast-TV VLAN

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

3            1118

3            1119
```

To configure triple play using the Webview, perform the following:

1. Click **Layer 2 > VLAN > VLAN > Basic Information**. The *VLAN Basic Information Page* opens.

2. Click Add. The *Add VLAN Membership Page* opens:



Basic Information

VLAN		Type	Authentication	Modify	Remove
ID	Name				
1	d				
2	V				

Add 802.1q VLAN

VLAN ID	
VLAN Name	

Figure 8. Add VLAN Membership Page

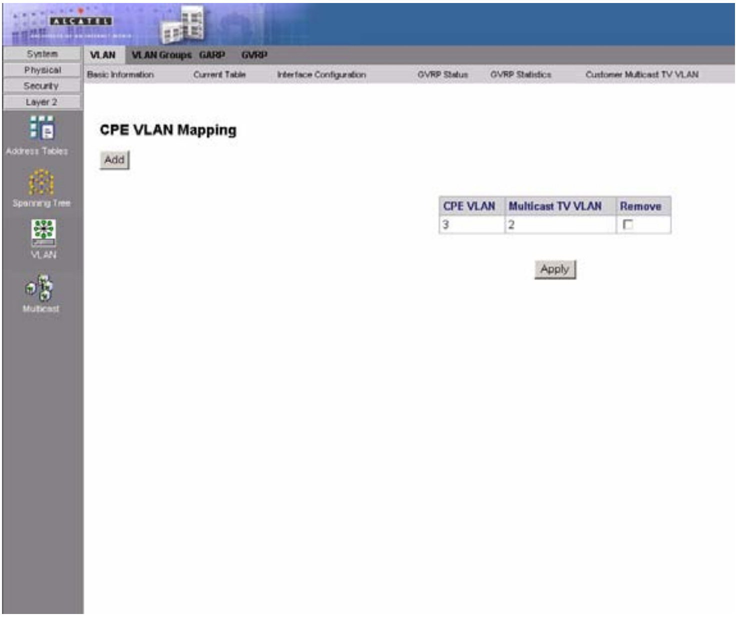
3. Create VLANs for customer port 1 and port 48 for QinQ. Each customer has separate VLAN. For this example use 1001 and 1048.

4. With the same screen create a VLAN for configuring Multicast TV provider A as 3000, and create a VLAN for configuring Multicast TV provider B as 3001.

5. Click Apply.

6. Close the *Add VLAN Membership Page*.

7. Click **Layer 2 > VLAN > VLAN > CPE VLAN Mapping**. The *CPE VLAN Mapping Page* opens.



CPE VLAN Mapping

CPE VLAN	Multicast TV VLAN	Remove
3	2	□

Figure 9. CPE VLAN Mapping Page

8. Click Add . The *Add CPE VLAN Mapping Page* opens:

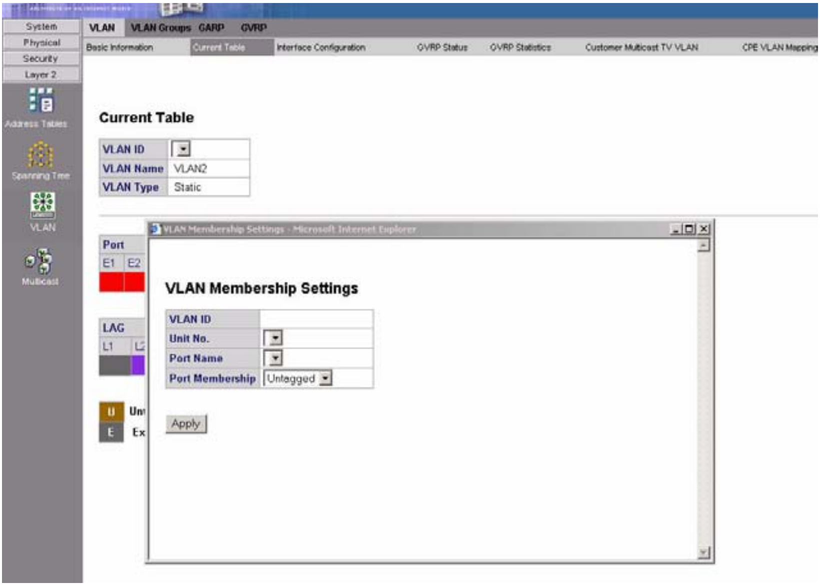
9. Map the internal CPE VLAN 3 to the Multicast TV VLAN 3001, and map the internal CPE VLAN 4 to the Multicast TV VLAN 3000.

10. Click Apply .

11. Close the *Add CPE VLAN Mapping Page*.

12. Click **Layer 2 > VLAN > VLAN > Current Table**. The *VLAN Current Table Page* opens.

13. Select VLAN ID number 1001 and double-click port e1. The *VLAN Membership Settings* page opens.



Current Table

VLAN ID	
VLAN Name	VLAN2
VLAN Type	Static

VLAN Membership Settings

VLAN ID	
Unit No.	
Port Name	
Port Membership	Untagged

Figure 10. CPE VLAN Mapping Page

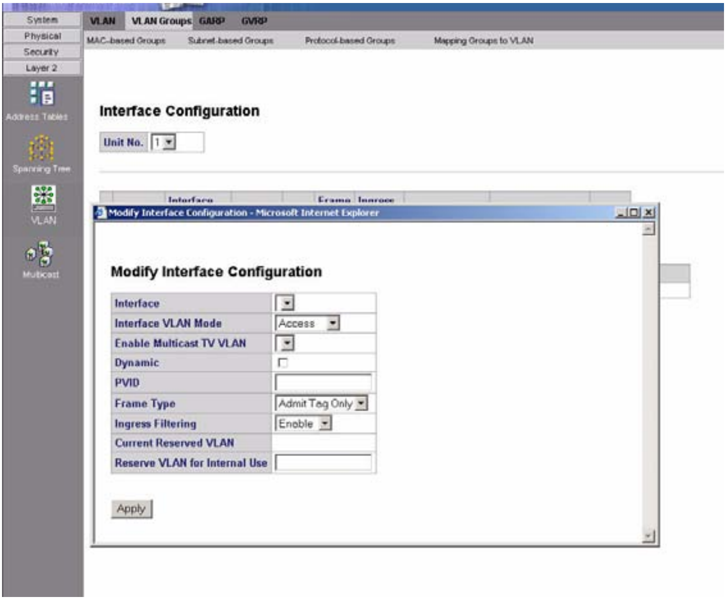
14. In the **Port Membership** field, select **Include**.

15. Click Apply .

16. Close the *VLAN Membership Settings Page*.

17. Click **Layer 2 > VLAN > VLAN > Interface Configuration**. The *VLAN Interface Configuration Page* opens.

18. Click ✎ on the row displaying port e1 configuration. The *VLAN Interface Settings Page* opens.



Interface Configuration

Unit No. 1

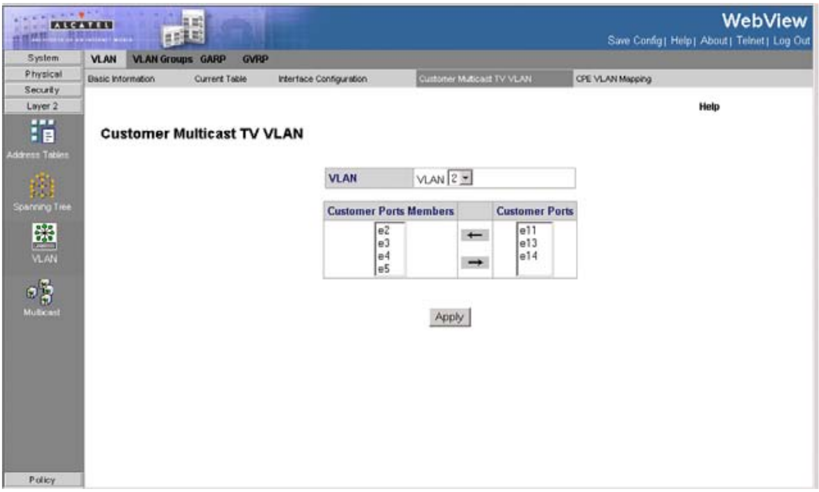
Modify Interface Configuration

Interface	
Interface VLAN Mode	Access
Enable Multicast TV VLAN	
Dynamic	□
PVID	
Frame Type	Admit Tag Only
Ingress Filtering	Enable
Current Reserved VLAN	
Reserve VLAN for Internal Use	

Apply

Figure 11. VLAN Interface Settings Page

19. In the **Port VLAN Mode** field, select **Customer**.
20. Click Apply .
21. Close the *VLAN Interface Settings Page*.
22. Repeat steps 18 to 21 configuring port e48 as a customer port on VLAN 1048.
23. Click **Layer 2 > VLAN > VLAN > Customer Multicast TV VLAN**. The *Customer Multicast VLAN Page* opens.
24. In the **VLAN** field, select 3000.



Customer Multicast TV VLAN

VLAN: VLAN 2

Customer Ports Members		Customer Ports
e2 e3 e4 e5		e11 e13 e14

Figure 12. Customer Multicast TV VLAN Page

25. Select port e1 and e48.

26. Click Apply.

27. Repeat steps 15 to 17 for VLANs 3001.

Configuring Customer VLANs

This section contains information for configuring Customer VLANs using the Web Interface and using the Command Line Interface. This section includes the following topics:

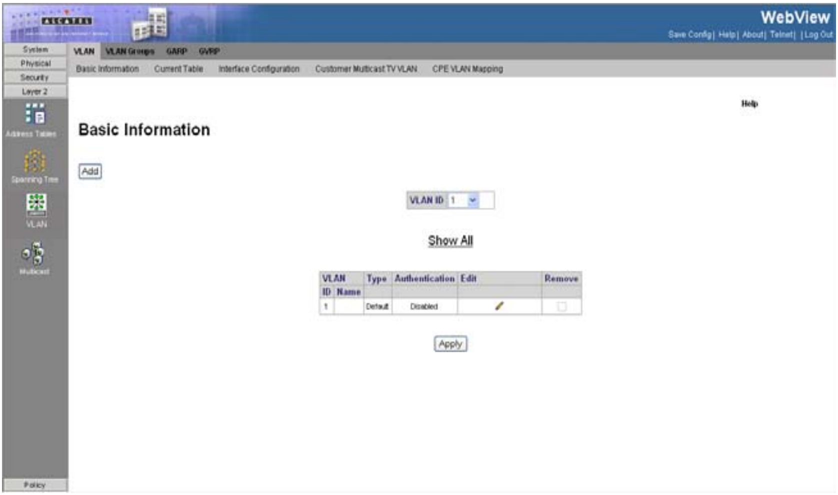
- Configuring Customer VLANs Using the Web Interface
- Configuring Customer VLANs using the CLI

Configuring Customer VLANs Using the Web Interface

Customer VLANs are configured using QinQ. QinQ tagging allows network managers to add an additional tag to previously tagged packets. Adding additional tags to the packets helps create more VLAN space. The added tag provides an VLAN ID to each customer, this ensures private and segregated network traffic. The VLAN ID tag is assigned to a customer port in the service providers network. The designated port then provides additional services to the packets with the double-tags. This allows administrators to expand service to VLAN users.

To configure customer VLANs:

1. Click **Layer 2 > VLAN > VLAN > Basic Information**. The *VLAN Basic Information Page* opens.



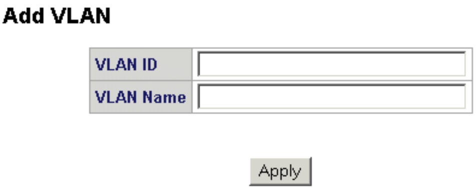
Basic Information

VLAN ID 1

VLAN ID	VLAN Name	Type	Authentication	Edit	Remove
1		Default	Disabled	✎	□

Figure 13. VLAN Basic Information Page

2. Click Add . The *Add VLAN Page* opens:



Add VLAN

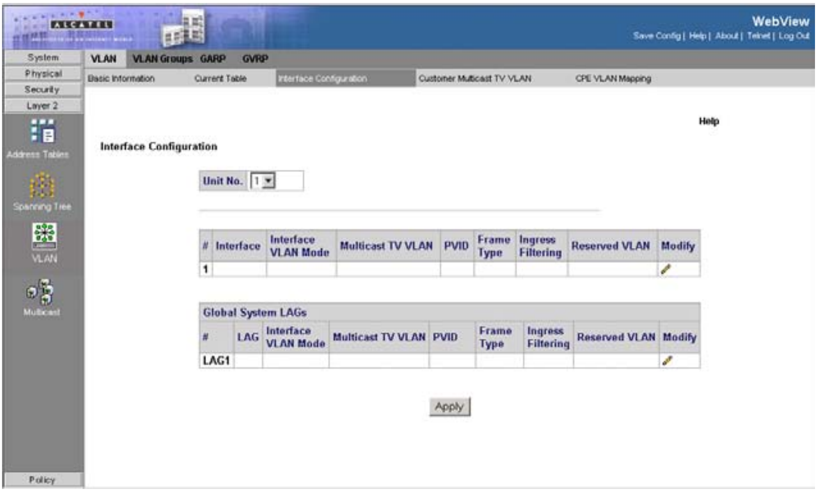
VLAN ID	
VLAN Name	

Figure 14. Add VLAN Page

3. Define the *VLAN ID* and *VLAN Name* field.

4. Click Apply .

5. Click **Layer 2 > VLAN > VLAN > Interface Configuration**. The *VLAN Interface Configuration Page* opens.



Interface Configuration

Unit No. 1

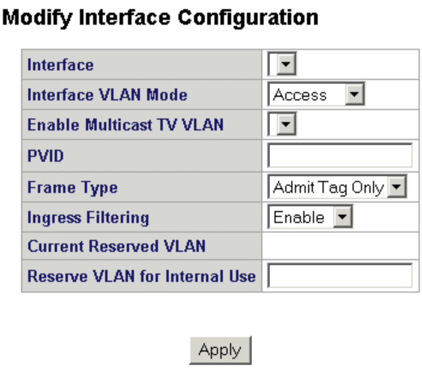
#	Interface	Interface VLAN Mode	Multicast TV VLAN	PVID	Frame Type	Ingress Filtering	Reserved VLAN	Modify
1								✎

Global System LAGs								
#	LAG	Interface VLAN Mode	Multicast TV VLAN	PVID	Frame Type	Ingress Filtering	Reserved VLAN	Modify
LAG1								✎

Apply

Figure 15. VLAN Interface Configuration Page

6. Click ✎ on previously defined customer VLAN row. The *Modify VLAN Interface Configuration Page* opens:



Modify Interface Configuration

Interface	
Interface VLAN Mode	Access
Enable Multicast TV VLAN	
PVID	
Frame Type	Admit Tag Only
Ingress Filtering	Enable
Current Reserved VLAN	
Reserve VLAN for Internal Use	

Apply

Figure 16. Modify VLAN Interface Configuration Page

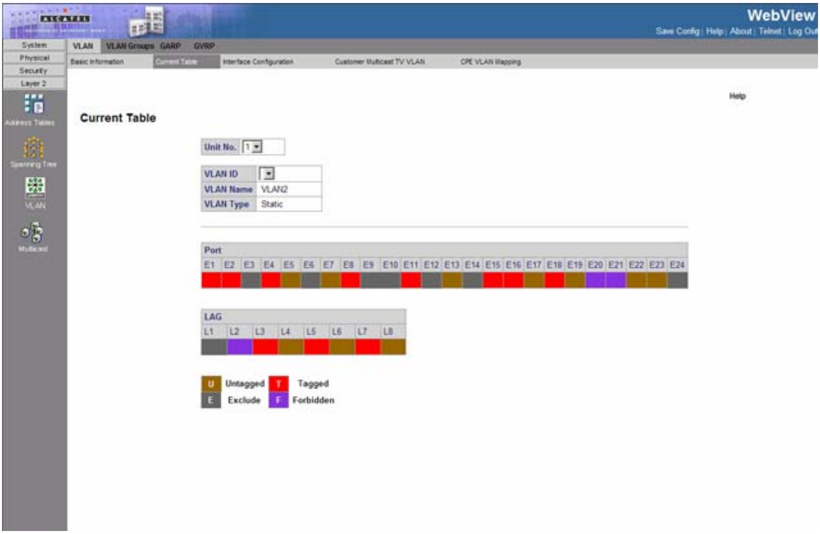
7. Select the interface.

8. Set the *Interface VLAN Mode* field to *Customer*.

9. Define the remaining fields.

10. Click Apply . The VLAN interface settings are saved, and the device is updated.

11. Click **Layer 2 > VLAN > VLAN > Current Table**. The *VLAN Current Table* opens.



Current Table

Unit No.	1

VLAN ID	
VLAN Name	VLAN2
VLAN Type	Static

Port																							
E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18	E19	E20	E21	E22	E23	E24
🟥	🟥	⬛	🟥	🟫	⬛	🟫	🟥	⬛	⬛	🟥	⬛	🟫	⬛	🟥	🟥	🟫	🟥	🟫	🟪	🟪	🟫	🟫	⬛

LAG							
L1	L2	L3	L4	L5	L6	L7	L8
⬛	🟪	🟥	🟫	🟥	🟫	🟥	🟫

U Untagged T Tagged
E Exclude F Forbidden

Figure 17. VLAN Current Table

12. Select the VLAN ID.

13. Add the ports to the VLAN.

14. Click Apply . The customer VLAN is defined, and the device is updated.

Appendix B. Software Specifications

Software Features

Authentication

Local, RADIUS, TACACS, Port (802.1x), HTTPS, SSH, Port Security

Access Control Lists

IP, MAC (up to 32 lists)

AMAP

Alcatel Mapping Adjacency Protocol

SNMPv3

Management access via MIB database
Trap management to specified hosts

DHCP Client

DNS Server

Port Configuration

1000BASE-T: 10/100/1000 Mbps, half/full duplex
1000BASE-SX/LX: 1000 Mbps, full duplex
100Base-FX: 100Mbps, full duplex

Flow Control

Full Duplex: IEEE 802.3x
Half Duplex: Back pressure

Broadcast Storm Control

Traffic throttled above a critical threshold

Port Mirroring

Multiple source ports, one destination port

Rate Limits

Input Limit
Output limit
Range (configured per port)

Port Trunking

Static trunks (Cisco EtherChannel compliant)
Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Protocol

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

VLAN Support

Up to 255 groups; port-based, protocol-based, or tagged (802.1Q),
GVRP for automatic VLAN learning, private VLANs

Class of Service

Supports eight levels of priority and Weighted Round Robin Queueing
(which can be configured by VLAN tag or port),
Layer 3/4 priority mapping: IP Precedence, IP DSCP

Multicast Filtering

IGMP Snooping (Layer 2)

Additional Features

BOOTP client
SNTP (Simple Network Time Protocol)
SNMP (Simple Network Management Protocol)
RMON (Remote Monitoring, groups 1,2,3,9)

Management Features

In-Band Management

Telnet, Web-based HTTP or HTTPS, SNMP manager, or Secure Shell

Out-of-Band Management

RS-232 RJ-45 console port

Software Loading

TFTP in-band or XModem out-of-band

SNMP

Management access via MIB database
Trap management to specified hosts

RMON

Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

Standards

IEEE 802.3 Ethernet,
IEEE 802.3u Fast Ethernet
IEEE 802.3x Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3z Gigabit Ethernet,
IEEE 802.3ab 1000BASE-T
IEEE 802.3ac VLAN tagging
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.3ad Link Aggregation Control Protocol
IEEE 802.1D Spanning Tree Protocol and traffic priorities
IEEE 802.1p Priority tags

IEEE 802.1s Multiple Spanning Tree Protocol
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Authentication
ARP (RFC 826)
DHCP (RFC 1541)
HTTPS
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
RADIUS+ (RFC 2618)
RMON (RFC 1757 groups 1,2,3,9)
SNMP (RFC 1157)
SNTP (RFC 2030)
SNMPv2 (RFC 1907)
SSH (Version 2.0)
TFTP (RFC 1350)

Management Information Bases

Bridge MIB (RFC 1493)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP Multicasting related MIBs
MAU MIB (RFC 2668)
MIB II (RFC 1212, 1213)
Port Access Entity MIB (IEEE 802.1x)
Private MIB
Quality of Service MIB
RADIUS Authentication Client MIB (RFC 2621)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMP framework MIB (RFC 2571)
SNMP-MPD MIB (RFC 2572)

SNMP Target MIB, SNMP Notification MIB (RFC 2573)
SNMP User-Based SM MIB (RFC 2574)
SNMP View Based ACM MIB (RFC 2575)
SNMP Community MIB (RFC 2576)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2013)
Trap (RFC 1215)
UDP MIB (RFC 2012)

Appendix C. Troubleshooting

Problems Accessing the Management Interface

Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, Web browser, or SNMP software	• Be sure the switch is powered up. • Check network cabling between the management station and the switch. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. • Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. • If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot access the on-board configuration program via a serial port connection	• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps). • Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	• Contact your local distributor.

Using System Logs

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Designate the SNMP host that is to receive the error messages.
4. Repeat the sequence of commands or other actions that lead up to the error.
5. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
6. Contact your distributor’s service engineer.

For example:

```
Console(config)#logging on
Console(config)#logging file debugging
Console(config)#snmp-server host 192.168.1.23
```

Appendix D. Glossary

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1x Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol (GARP)

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5 Message Digest Algorithm

An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1x.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Secure Shell (SSH)

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Transmission Control Protocol/Internet Protocol (TCP/IP)

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

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Index