Dell™ PowerConnect™ 3400 Series

CLI Reference Guide

Notes, Notices, and Cautions

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

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

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

September 2006 Rev. A01

Contents

4 AAA Commands

5 ACL Commands

6 Address Table Commands

7 Clock

8 Configuration and Image Files

9 DHCP Filtering

10 Ethernet Configuration Commands

11 GVRP Commands

12 IGMP Snooping Commands

13 IP Addressing Commands

14 LACP Commands

22 QoS Commands

23 Radius Commands

24 RMON Commands

25 SNMP Commands

26 Spanning-Tree Commands

27 SSH Commands

28 Syslog Commands

29 System Management

30 TACACS+ Commands

31 User Interface

32 VLAN Commands

33 Web Server

34 802.1x Commands

1

Command Groups

Introduction

The Command Language Interface (CLI) is a network management application operated through an ASCII terminal without the use of a Graphical User Interface (GUI) driven software application. By directly entering commands, you achieve greater configuration flexibility. The CLI is a basic command-line interpreter similar to the UNIX C shell.

You can configure and maintain a device by entering commands from the CLI, which is based solely on textual input and output; you enter commands using a terminal keyboard and the textual output displays via a terminal monitor. You can access the CLI from a VT100 terminal connected to the console port of the device or through a Telnet connection from a remote host.

The first time you use the CLI from the console a Setup Wizard is invoked. The Setup Wizard guides you in setting up a minimum configuration, so that the device can be managed from the Web Based Interface. Refer to the *Getting Started Guide* and *User Guide* for more information on the Setup Wizard.

This guide describes how the Command Line Interface (CLI) is structured, describes the command syntax, and describes the command functionality.

This guide also provides information for configuring the PowerConnect device, details the procedures, and provides configuration examples. Basic installation configuration is described in the *User's Guide* and must be completed before using this document.

Command Groups

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

Command Group	Description
AAA	Configures connection security including authorization and passwords.
ACL	Configures and displays ACL information.
Address Table	Configures bridging address tables.
Configuration and Image Files	Manages the device configuration files.
Clock	Configures clock commands on the device.
DHCP Filtering	Configures DHCP filtering commands.

Ethernet Configuration	Configures all port configuration options for, example ports, storm control, and auto-negotiation.
GVRP	Configures and displays GVRP configuration and information.
IGMP Snooping	Configures IGMP snooping and displays IGMP configuration and IGMP information.
IP Addressing	Configures and manages IP addresses on the device.
LACP	Configures and displays LACP information.
Line	Configures the console and remote Telnet connection.
LLDP	Configures and displays LLDP information.
Management ACL	Configures and displays management access-list information.
PHY Diagnostics	Diagnoses and displays the interface status.
Port Channel	Configures and displays Port Channel information.
Port Monitor	Monitors activity on specific target ports.
QoS	Configures and displays QoS information.
RADIUS	Configures and displays RADIUS information.
RMON	Displays RMON statistics.
SNMP	Configures SNMP communities, traps and displays SNMP information.
Spanning Tree	Configures and reports on Spanning Tree protocol.
SSH	Configures SSH authentication.
Syslog Commands	Manages and displays syslog messages.
System Management	Configures the device clock, name and authorized users.
TACACS	Configures TACACS+ commands.
User Interface	Describes user commands used for entering CLI commands.
VLAN	Configures VLANs and displays VLAN information.
Web Server	Configures Web based access to the device.
802.1x	Configures commands related to 802.1x security protocol.

AAA Commands

Command Group	Description	Access Mode
aaa authentication login	Defines login authentication.	Global Configuration
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels.	Global Configuration
login authentication	Specifies the login authentication method list for a remote telnet or console.	Line Configuration
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.	Line Configuration
ip http authentication	Specifies authentication methods for HTTP server users.	Global Configuration
ip https authentication	Specifies authentication methods for HTTPS server users.	Global Configuration
show authentication methods	Displays information about the authentication methods.	Privileged EXEC
password	Specifies a password on a line.	Line Configuration
enable password	Sets a local password to control access to normal and privilege levels.	Global Configuration
username	Establishes a username-based authentication system.	Global Configuration
passwords min-length	Sets the minimum required length for passwords in the local database.	Global Configuration
passwords aging	Sets the expiration time for username and enable passwords.	Global Configuration
password-aging	Sets the expiration time of line passwords in the local database.	Line Configuration
passwords history	Sets the number of required password changes before a password in the local database can be reused.	Global Configuration
passwords history hold-time	Sets the number of days a password is relevant for tracking its password history.	Global Configuration
passwords lockout	Sets the number of failed login attempts before a user account is locked.	Global Configuration
aaa login-history file	Enables writing to the login history file.	Global Configuration
set username active	Reactivates a locked user account.	Privileged EXEC

set line active	Reactivates a locked line.	Privileged EXEC
set enable-password active	Reactivates a locked local password.	Privileged EXEC
show passwords configuration	Displays information about password management.	Privileged EXEC
show users login-history	Displays information about the login history of users.	Privileged EXEC
show users accounts	Displays information about the local user database.	Privileged EXEC

ACL Commands

Command Group	Description	Access Mode
mac access-list	Creates Layer 2 ACLs.	Global Configuration
deny (MAC)	Denies traffic if the conditions defined in the permit statement match.	MAC Access-List Configuration
service-acl	Applies an ACL to the input interface.	Interface (VLAN) Configuration
show access-lists	Displays ACLs defined on the device.	Privileged EXEC
show interfaces access-lists	Displays access lists applied on interfaces.	Privileged EXEC

Address Table Commands

Command Group	Description	Access Mode
bridge address	Adds a static MAC-layer station source address to the bridge table.	Interface (VLAN) Configuration
bridge multicast filtering	Enables filtering of multicast addresses.	Global Configuration
bridge multicast address	Registers MAC-layer multicast addresses to the bridge table, and adds static ports to the group.	Interface (VLAN) Configuration
bridge multicast forbidden address	Forbids adding a specific multicast address to specific ports.	Interface (VLAN) Configuration
bridge multicast forward-all	Enables forwarding all multicast frames on a port.	Interface (VLAN) Configuration
bridge multicast forbidden forward-all	Forbids a port from becoming a forward-all multicast port.	Interface (VLAN) Configuration
bridge aging-time	Sets the address table aging time.	Global Configuration

clear bridge	Removes any learned entries from the forwarding database.	Privileged EXEC
port security	Disables new address learning/forwarding on an interface.	Interface Configuration
port security mode	Configures the port security learning mode.	Interface Configuration
port security max	Configures the maximum number of addresses that may be learned on the port while the port is in port security mode.	Interface Configuration
port security routed secure-address	Adds MAC-layer secure addresses to a routed port.	Interface Configuration
show bridge address-table	Displays all entries in the bridge-forwarding database.	Privileged EXEC
show bridge address-table static	Displays statically created entries in the bridge-forwarding database.	Privileged EXEC
show bridge address-table count	Displays the number of addresses present in the bridge-forwarding database.	Privileged EXEC
show bridge multicast address-table	Displays all entries in the bridge-forwarding database.	Privileged EXEC
show bridge multicast filtering	Displays the multicast filtering configuration.	Privileged EXEC
show ports security	Displays the port-lock status.	Privileged EXEC
show ports security addresses	Displays current dynamic addresses in locked ports.	Privileged EXEC

Clock Commands

Command Group	Description	Access Mode
clock set	Manually sets the system clock.	Privileged EXEC
clock source	Configures an external time source for the system clock.	Global Configuration
clock timezone	Sets the time zone for display purposes.	Global Configuration
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).	Global Configuration
sntp authentication-key	Defines an authentication key for Simple Network Time Protocol (SNTP).	Global Configuration
sntp authenticate	Grants authentication for received Network Time Protocol (NTP) traffic from servers.	Global Configuration
sntp trusted-key	Authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize.	Global Configuration
sntp client poll timer	Sets the polling time for the Simple Network Time Protocol (SNTP) client.	Global Configuration
sntp broadcast client enable	Enables the Simple Network Time Protocol (SNTP) broadcast clients.	Global Configuration
sntp anycast client enable	Enables anycast clients.	Global Configuration
sntp client enable (Interface)	Enables the Simple Network Time Protocol (SNTP) client on an interface.	Interface Configuration
sntp unicast client enable	Enables the device to use the Simple Network Time Protocol (SNTP) to request and accept Simple Network Time Protocol (SNTP) traffic from servers.	Global Configuration
sntp unicast client poll	Enables polling for the Simple Network Time Protocol (SNTP) predefined unicast clients.	Global Configuration
sntp server	Configures the device to use the Simple Network Time Protocol (SNTP) to request and accept Simple Network Time Protocol (SNTP) traffic from a server.	Global Configuration
show clock	Displays the time and date from the system clock.	User EXEC
show sntp configuration	Shows the configuration of the Simple Network Time Protocol (SNTP).	Privileged EXEC
show sntp status	Shows the status of the Simple Network Time Protocol (SNTP).	Privileged EXEC

Configuration and Image Files Commands

Command Group	Description	Access Mode
copy	Copies files from a source to a destination.	Privileged EXEC
delete	Deletes a file from a Flash memory device.	Privileged EXEC
delete startup-config	Deletes the startup-config file.	Privileged EXEC
dir	Displays a list of files on a flash file system.	Privileged EXEC
more	Displays a file.	Privileged EXEC
rename	Renames a file.	Privileged EXEC
boot system	Specifies the system image that the device loads at startup.	Privileged EXEC
show running-config	Displays the contents of the currently running configuration file.	Privileged EXEC
show startup-config	Displays the startup configuration file contents.	Privileged EXEC
show bootvar	Displays the active system image file that the device loads at startup.	Privileged EXEC

DHCP Filtering Commands

Command Group	Description	Access Mode
ip dhcp filtering vlan	Enable filtering of DHCP requests on a VLAN.	Global Configuration
ip dhcp filtering trust	Configure a port as trusted for DHCP filtering purposes.	Interface Configuration
show ip dhcp filtering	Display the DHCP filtering configuration.	EXEC

Ethernet Configuration Commands

Command Group	Description	Access Mode
interface ethernet	Enters the interface configuration mode to configure an Ethernet type interface.	Global Configuration
interface range ethernet	Enters the interface configuration mode to configure multiple Ethernet type interfaces.	Global Configuration
shutdown	Disables interfaces.	Interface Configuration

description	Adds a description to an interface.	Interface Configuration
duplex	Configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation.	Interface Configuration
speed	Configures the speed of a given Ethernet interface when not using auto-negotiation.	Interface Configuration
negotiation	Enables auto-negotiation operation for the speed and duplex parameters of a given interface.	Interface Configuration
flowcontrol	Configures the Flow Control on a given interface.	Interface Configuration
mdix	Enables automatic crossover on a given interface.	Interface Configuration
back-pressure	Enables Back Pressure on a given interface.	Interface Configuration
clear counters	Clears statistics on an interface.	User EXEC
set interface active	Reactivates an interface that was suspended by the system.	Privileged EXEC
show interfaces advertise	Displays auto negotiation advertisement data.	Privileged EXEC
show interfaces configuration	Displays the configuration for all interfaces.	Privileged EXEC
show interfaces status	Displays the status for all interfaces.	Privileged EXEC
show interfaces description	Displays the description for all interfaces.	Privileged EXEC
show interfaces counters	Displays traffic seen by the physical interface.	Privileged EXEC
port storm-control include-multicast	Enables the device to count multicast packets with broadcast packets.	Interface Configuration
port storm-control broadcast enable	Enables broadcast storm control.	Interface Configuration
port storm-control broadcast rate	Configures the maximum broadcast rate.	Interface Configuration
show ports storm-control	Displays the storm control configuration.	Privileged User EXEC

GVRP Commands

Command Group	Description	Mode
gvrp enable (Global)	Enables GVRP globally.	Global Configuration
gvrp enable (Interface)	Enables GVRP on an interface.	Interface Configuration
garp timer	Adjusts the GARP application join, leave, and leaveall GARP timer values.	Interface Configuration
gvrp vlan-creation-forbid	Enables or disables dynamic VLAN creation.	Interface Configuration
gvrp registration-forbid	De-registers all VLANs, and prevents dynamic VLAN registration on the port.	Interface Configuration
clear gvrp statistics	Clears all the GVRP statistics information.	Privileged EXEC
show gvrp configuration	Displays GVRP configuration information.	User EXEC
show gvrp statistics	Displays GVRP statistics.	User EXEC
show gvrp error-statistics	Displays GVRP error statistics.	User EXEC

IGMP Snooping Commands

Command Group	Description	Access Mode
ip igmp snooping (Global)	Enables Internet Group Management Protocol (IGMP) snooping.	Global Configuration
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.	Interface (VLAN)
ip igmp snooping mrouter learn-pim-dvmrp	Enables automatic learning of multicast router ports.	Interface (VLAN)
ip igmp snooping host-time-out	Configures the host-time-out.	Interface (VLAN)
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out.	Interface (VLAN)
ip igmp snooping leave-time-out	Configures the leave-time-out.	Interface (VLAN)
show ip igmp snooping mrouter	Displays information on dynamically learned multicast router interfaces.	User EXEC
show ip igmp snooping interface	Displays IGMP snooping configuration.	User EXEC

show ip igmp snooping groups	Displays multicast groups learned by IGMP snooping.	User EXEC

IP Addressing

Command Group	Description	Access Mode
ip address	Sets an IP address.	Interface Configuration
ip address dhcp	Acquires an IP address on an interface from the DHCP server.	Interface Configuration
ip default-gateway	Defines a default gateway (router).	Global Configuration
show ip interface	Displays the usability status of interfaces configured for IP.	Privileged EXEC
arp	Adds a permanent entry in the ARP cache.	Global Configuration
arp timeout	Configures how long an entry remains in the ARP cache.	Global Configuration
clear arp-cache	Deletes all dynamic entries from the ARP cache.	Privileged EXEC
show arp	Displays entries in the ARP table.	Privileged EXEC
ip domain-lookup	Enables the IP Domain Naming System (DNS)-based host name-to-address translation.	Global Configuration
ip domain-name	Defines a default domain name, that the software uses to complete unqualified host names.	Global Configuration
ip name-server	Sets the available name servers.	Global Configuration
ip host	Defines static host name-to-address mapping in the host cache.	Global Configuration
clear host	Deletes entries from the host name-to-address cache.	Privileged EXEC
clear host dhcp	Deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).	Privileged EXEC
show hosts	Displays the default domain name, a list of name server hosts, the static and cached list of host names and addresses.	Privileged EXEC

LACP Commands

Command Group	Description	Access Mode
lacp system-priority	Configures the system LACP priority.	Global Configuration
lacp port-priority	Configures the priority value for physical ports.	Interface Configuration
lacp timeout	Assigns an administrative LACP timeout.	Interface Configuration
show lacp ethernet	Displays LACP information for Ethernet ports.	Privileged EXEC
show lacp port-channel	Displays LACP information for a port-channel.	Privileged EXEC

LLDP Commands

Command Group	Description	Access Mode
lldp enable (global)	Enables Link Layer Discovery Protocol.	Global configuration
lldp enable (interface)	Enables Link Layer Discovery Protocol (LLDP) on an interface.	Interface configuration (Ethernet)
lldp timer	Specifies how often the software sends Link Layer Discovery Protocol (LLDP) updates.	Global configuration
lldp hold-multiplier	Specifies the amount of time the receiving device should hold a Link Layer Discovery Protocol packet before discarding it.	Global configuration
lldp reinit-delay	Specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.	Global configuration
lldp tx-delay	Specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.	Global configuration
lldp optional-tlv	Specifies which optional TLVs from the basic set should be transmitted.	Interface configuration (Ethernet)
lldp management-address	Specifies the management address that would be advertised from an interface.	Interface configuration (Ethernet)
clear lldp rx	Restarts the LLDP RX state machine and clears the neighbors table.	Privileged EXEC
show lldp configuration	Displays the Link Layer Discovery Protocol (LLDP) configuration.	Privileged EXEC
show lldp local	Displays the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port.	Privileged EXEC
show lldp neighbors	Displays information about discovered neighboring devices using Link Layer Discovery Protocol (LLDP)	Privileged EXEC

Line Commands

Command Group	Description	Access Mode
line	Identifies a specific line for configuration and enters the line configuration command mode.	Global Configuration
speed	Configures the baud rate of the line.	Line Configuration
autobaud	Configures the line for automatic baud rate detection (autobaud).	Line Configuration
exec-timeout	Configures the interval that the system waits until user input is detected.	Line Configuration
history	Enables the command history function.	Line Configuration
history size	Configures the command history buffer size for a particular line.	Line Configuration
terminal history	Enables the command history function for the current terminal session.	User EXEC
terminal history size	Configures the command history buffer size for the current terminal session.	User EXEC
show line	Displays line parameters.	User EXEC

Management ACL Commands

Command Group	Description	Access Mode
management access-list	Defines a management access-list, and enters the access-list for configuration.	Global Configuration
permit (Management)	Defines a permit rule.	Management Access-level
deny (Management)	Defines a deny rule.	Management Access-level
management access-class	Defines which management access-list is used.	Global Configuration
show management access-list	Displays management access-lists.	Privileged EXEC
show management access-class	Displays the active management access-list.	Privileged EXEC

PHY Diagnostics Commands

Command Group	Description	Access Mode
test copper-port tdr	Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.	Privileged EXEC
show copper-ports tdr	Displays the last TDR (Time Domain Reflectometry) tests on specified ports.	User EXEC
show copper-ports cable-length	Displays the estimated copper cable length attached to a port.	User EXEC
show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics.	Privileged EXEC

Port Channel Commands

Command Group	Description	Access Mode
interface port-channel	Enters the interface configuration mode of a specific port-channel.	Global Configuration
interface range port-channel	Enters the interface configuration mode to configure multiple port-channels.	Global Configuration
channel-group	Associates a port with a port-channel.	Interface Configuration
show interfaces port-channel	Displays port-channel information.	Privileged EXEC

Port Monitor Commands

Command Group	Description	Access Mode
port monitor	Starts a port monitoring session.	Interface Configuration
port monitor vlan-tagging	Transmits tagged ingress mirrored packets.	Interface Configuration
show ports monitor	Displays port monitoring status.	User EXEC

Power-over-Ethernet Commands

Command Group	Description	Access Mode
power inline	Configures the administrative mode of the inline power on an interface.	Interface Configuration
power inline powered-device	Adds a description of the powered device type attached to the interface.	Interface Configuration
power inline priority	Displays port monitoring status.	Interface Configuration
power inline usage-threshold	Configures the administrative mode of the inline power on an interface.	Global Configuration
power inline traps enable	Adds a description of the powered device type attached to the interface.	Global Configuration
show power inline	Displays port monitoring status.	User EXEC

QoS Commands

Command Group	Description	Access Mode
qos	Enables quality of service (QoS) on the device and enters QoS basic mode.	Global Configuration
show qos	Displays the QoS status.	User EXEC
wrr-queue cos-map	Maps assigned CoS values to select one of the egress queues.	Global Configuration
priority-queue out num-of-queues	Configures the number of expedite queues.	Global Configuration
show qos interface	Displays interface QoS data.	User EXEC
qos map dscp-queue	Modifies the DSCP to CoS map.	Global Configuration
qos trust (Global)	Configures the system to basic mode and the "trust" state.	Global Configuration
qos trust (Interface)	Enables each port trust state.	Interface Configuration
qos cos	Configures the default port CoS value.	Interface Configuration
show qos map	Displays all the maps for QoS.	User EXEC

Radius Commands

Command Group	Description	Access Mode
radius-server host	Specifies a RADIUS server host.	Global Configuration
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.	Global Configuration
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.	Global Configuration
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.	Global Configuration
radius-server timeout	Sets the interval for which a device waits for a server host to reply.	Global Configuration
radius-server deadtime	Improves RADIUS response times when servers are unavailable.	Global Configuration
show radius-servers	Displays the RADIUS server settings.	Privileged EXEC

RMON Commands

Command Group	Description	Mode
show rmon statistics	Displays RMON Ethernet Statistics.	User EXEC
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.	Interface Configuration
show rmon collection history	Displays the requested history group configuration.	User EXEC
show rmon history	Displays RMON Ethernet statistics history.	User EXEC
rmon alarm	Configures alarm conditions.	Global Configuration
show rmon alarm-table	Displays the alarms table.	User EXEC
show rmon alarm	Displays alarm configurations.	User EXEC
rmon event	Configures a RMON event.	Global Configuration
show rmon events	Displays the RMON event table.	User EXEC
show rmon log	Displays the RMON logging table.	User EXEC
rmon table-size	Configures the maximum RMON tables sizes.	Global Configuration

SNMP Commands

Command Group	Description	Access Mode
snmp-server community	Sets up the community access string to permit access to SNMP protocol.	Global Configuration
snmp-server view	Creates and modifies view entries.	Global Configuration
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.	Global Configuration
snmp-server user	Configures a new SNMP v3 user.	Global Configuration
snmp-server engineID local	Specifies an SNMP EngineID on the local device.	Global Configuration
snmp-server enable traps	Enables the device to send SNMP traps or SNMP notifications.	Global Configuration
snmp-server filter	Creates and modifies filter entries.	Global Configuration
snmp-server host	Specifies an SNMP notification recipient.	Global Configuration
snmp-server v3-host	Specifies an SNMP v3 notification recipient.	Global Configuration
snmp-server trap authentication	Enables the device to send Simple Network Management Protocol traps when authentication failed.	Global Configuration
snmp-server contact	Sets up a system contact.	Global Configuration
snmp-server location	Sets up the information on where the device is located.	Global Configuration
snmp-server set	Sets SNMP MIB value by the CLI.	Global Configuration
show snmp	Displays the SNMP status.	Privileged EXEC
show snmp engineid	Displays the local SNMP EngineID.	Privileged EXEC
show snmp views	Displays the configuration of SNMP views.	Privileged EXEC
show snmp groups	Displays the configuration of SNMP groups.	Privileged EXEC
show snmp filters	Displays the configuration of SNMP filters.	Privileged EXEC
show snmp users	Displays the configuration of SNMP users.	Privileged EXEC

Spanning Tree Commands

Command Group	Description	Access Mode
spanning-tree	Enables spanning tree functionality.	Global Configuration
spanning-tree mode	Configures the spanning tree protocol.	Global Configuration
spanning-tree forward-time	Configures the spanning tree bridge forward time.	Global Configuration
spanning-tree hello-time	Configures the spanning tree bridge Hello Time.	Global Configuration
spanning-tree max-age	Configures the spanning tree bridge maximum age.	Global Configuration
spanning-tree priority	Configures the spanning tree priority.	Global Configuration
spanning-tree disable	Disables spanning tree on a specific port.	Interface Configuration
spanning-tree cost	Configures the spanning tree path cost for a port.	Interface Configuration
spanning-tree port-priority	Configures port priority.	Interface Configuration
spanning-tree portfast	Enables PortFast mode.	Interface Configuration
spanning-tree link-type	Overrides the default link-type setting.	Interface Configuration
spanning-tree pathcost method	Sets the default path cost method.	Global Configuration
spanning-tree bpdu	Defines BPDU handling when spanning tree is disabled on an interface.	Global Configuration
clear spanning-tree detected-protocols	Restarts the protocol migration process on all interfaces or on the specified interface.	Privileged EXEC
spanning-tree mst priority	Configures the device priority for the specified spanning-tree instance.	Global Configuration
spanning-tree mst max-hops	Configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out.	Global Configuration
spanning-tree mst port-priority	Configures the priority of a port.	Interface Configuration

spanning-tree mst cost	Configures the path cost for multiple spanning tree (MST) calculations.	Interface Configuration
spanning-tree mst configuration	Enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.	Global Configuration
instance (mst)	Maps VLANs to the MST instance.	MST Configuration
name (mst)	Defines the configuration name.	MST Configuration
revision (mst)	Defines the configuration revision number.	MST Configuration
show (mst)	Displays the current or pending MST region configuration.	MST Configuration
exit (mst)	Exits the MST region configuration mode and applies all configuration changes.	MST Configuration
abort (mst)	Exits the MST region configuration mode without applying configuration changes.	MST Configuration
show spanning-tree	Displays spanning tree configuration.	Privileged EXEC
spanning-tree guard root	Enables root guard on all the spanning tree instances in the interface.	Interface Configuration

SSH Commands

Command Group	Description	Access Mode
ip ssh port	Specifies the port to be used by the SSH server.	Global Configuration
ip ssh server	Enables the device to be configured from a SSH server.	Global Configuration
crypto key generate dsa	Generates DSA key pairs.	Global Configuration
crypto key generate rsa	Generates RSA key pairs.	Global Configuration
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions.	Global Configuration
crypto key pubkey-chain ssh	Enters SSH Public Key-chain configuration mode.	Global Configuration
user-key	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command.	SSH Public Key
key-string	Manually specifies a SSH public key.	SSH Public Key
show ip ssh	Displays the SSH server configuration.	Privileged EXEC

show crypto key mypubkey	Displays the SSH public keys stored on the device.	Privileged EXEC
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the device.	Privileged EXEC
crypto slogin key generate dsa	Generates DSA key pairs for secure login to a remote access server.	Global Configuration
crypto slogin key generate rsa	Generates RSA key pairs for secure login to a remote access server.	Global Configuration
show crypto slogin key mypubkey	Displays the secure login public key of the device.	Privileged EXEC

Syslog Commands

Command Group	Description	Access Mode
logging on	Controls error messages logging.	Global Configuration
logging	Logs messages to a syslog server.	Global Configuration
logging console	Limits messages logged to the console based on severity.	Global Configuration
logging buffered	Limits syslog messages displayed from an internal buffer based on severity.	Global Configuration
logging buffered size	Changes the number of syslog messages stored in the internal buffer.	Global Configuration
clear logging	Clears messages from the internal logging buffer.	Privileged EXEC
logging file	Limits syslog messages sent to the logging file based on severity.	Global Configuration
clear logging file	Clears messages from the logging file.	Privileged EXEC
aaa logging	Enables logging AAA login events.	Global Configuration
file-system logging	Enables logging file system events.	Global Configuration
management logging	Enables logging management access list events.	Global Configuration
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.	Privileged EXEC
show logging file	Displays the state of logging and the syslog messages stored in the logging file.	Privileged EXEC

show syslog-servers	Displays the syslog servers settings.	Privileged EXEC

System Management Commands

Command Group	Description	Access Mode
ping	Sends ICMP echo request packets to another node on the network.	User EXEC
traceroute	Discovers the routes that packets will actually take when traveling to their destination.	User EXEC
telnet	Logs in to a host that supports Telnet.	User EXEC
resume	Switches to another open Telnet session	User EXEC
reload	Reloads the operating system.	Privileged EXEC
hostname	Specifies or modifies the device host name.	Global Configuration
stack master	Forces selection of a stack master.	Global Configuration
stack reload	Reloads stack members.	Privileged EXEC
stack display-order	Configures the display order of the units in a stack.	Global Configuration
show stack	Displays information about stack status.	User EXEC
show users	Displays information about the active users.	User EXEC
show sessions	Lists the open Telnet sessions.	User EXEC
show system	Displays system information.	User EXEC
show version	Displays the system version information.	User EXEC
asset-tag	Specifies the device asset-tag.	Global Configuration
show system id	Displays the service ID information.	User EXEC
service cpu-utilization	Enables measuring CPU utilization.	Global Configuration
show cpu utilization	Displays information about the CPU utilization of active processes.	Privileged EXEC

TACACS Commands

Command Group	Description	Mode
tacacs-server host	Specifies a TACACS+ host.	Global Configuration
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon.	Global Configuration
tacacs-server source-ip	Specifies the source IP address that will be used for the communication with TACACS+ servers.	Global Configuration
tacacs-server timeout	Sets the timeout value.	Global Configuration
show tacacs	Displays configuration and statistics for a TACACS+ servers.	Privileged EXEC

User Interface Commands

Command Group	Description	Access Mode
enable	Enters the privileged EXEC mode.	User EXEC
disable	Returns to User EXEC mode.	Privileged EXEC
login	Changes a login username.	Priv/User EXEC
configure	Enables the global configuration mode.	Privileged EXEC
exit (Configuration)	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.	All
exit	Closes an active terminal session by logging off the device.	Priv/User EXEC
end	Ends the current configuration session and returns to the Privileged EXEC mode.	After Privileged EXEC
help	Displays a brief description of the help system.	All
terminal datadump	Enables dumping all output of a show command without prompting.	User EXEC
show history	Lists the commands entered in the current session.	Privileged EXEC
show privilege	Displays the current privilege level.	User EXEC

VLAN Commands

Command Group	Description	Access Mode
vlan database	Enters the VLAN database configuration mode.	Global Configuration
vlan	Creates a VLAN.	VLAN Database
interface vlan	Enters the interface configuration (VLAN) mode.	Global Configuration
interface range vlan	Enters the interface configuration mode to configure multiple VLANs.	Global Configuration
name	Configures a name to a VLAN.	Interface (VLAN) Configuration
private-vlan primary	Defines the primary PVLAN.	Interface (VLAN) Configuration
private-vlan isolated	Defines the isolated VLAN of the PVLAN.	Interface (VLAN) Configuration
private-vlan community	Associates the primary VLAN and community VLANs.	Interface (VLAN) Configuration
switchport mode	Configures the VLAN membership mode of a port.	Interface Configuration
switchport access vlan	Configures the VLAN ID when the interface is in access mode.	Interface Configuration
switchport private-vlan	Defines the private-vlan port VLANs.	Interface Configuration
show vlan private-vlan	Displays information about private VLANs.	Privileged EXEC
switchport trunk allowed vlan	Adds or removes VLANs from a port in general mode.	Interface Configuration
switchport trunk native vlan	Defines the port as a member of the specified VLAN, and the VLAN ID is the "port default VLAN ID (PVID)".	Interface Configuration
switchport general allowed vlan	Adds or removes VLANs from a general port.	Interface Configuration
switchport general pvid	Configures the PVID when the interface is in general mode.	Interface Configuration
switchport general ingress-filtering disable	Disables port ingress filtering.	Interface Configuration

switchport general acceptable-frame-type tagged-only	Discards untagged frames at ingress.	Interface Configuration
switchport forbidden vlan	Forbids adding specific VLANs to a port.	Interface Configuration
switchport customer vlan	Sets the port's VLAN when the interface is in customer mode.	Interface Configuration
ip internal-usage-vlan	Reserves a VLAN as the internal usage VLAN of an interface.	Interface Configuration
mac-to-vlan	Adds MAC addresses to the MAC-to-VLAN database.	VLAN Configuration
show vlan mac-to-vlan	Displays the MAC-to-VLAN database.	Privileged EXEC
show vlan	Displays VLAN information.	Privileged EXEC
show vlan internal usage	Displays a list of VLANs used internally by the device.	Privileged EXEC
show interfaces switchport	Displays switchport configuration.	Privileged EXEC

Web Server Commands

Command Group	Description	Access Mode
ip http server	Enables the device to be configured from a browser.	Global Configuration
ip http port	Specifies the TCP port for use by a web browser to configure the device.	Global Configuration
ip https port	Configures a TCP port for use by a secure web browser to configure the device.	Global Configuration
ip https server	Enables the device to be configured from a secured browser.	Global Configuration
crypto certificate generate	Generates a HTTPS certificate.	Global Configuration
crypto certificate request	Generates and displays certificate requests for HTTPS.	Privileged EXEC
crypto certificate import	Imports a certificate signed by Certification Authority for HTTPS.	Global Configuration
ip https certificate	Configures the active certificate for HTTPS.	Global Configuration

show ip http	Displays the HTTP server configuration.	Privileged EXEC
show ip https	Displays the HTTPS server configuration.	Privileged EXEC
show crypto certificate mycertificate	Displays the SSL certificates of the device.	Privileged EXEC

802.1x Commands

Command	Description	Access Mode
aaa authentication dot1x	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x.	Global Configuration
dot1x system-auth-control	Enables 802.1x globally.	Global Configuration
dot1x port-control	Enables manual control of the authorization state of the port	Interface Configuration
dot1x re-authentication	Enables periodic re-authentication of the client.	Interface Configuration
dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.	Interface Configuration
dot1x re-authenticate	Manually initiates a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.	Privileged EXEC
dot1x timeout quiet-period	Sets the number of seconds that the device remains in the quiet state following a failed authentication exchange.	Interface Configuration
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.	Interface Configuration
dot1x max-req	Sets the maximum number of times that the device sends an EAP - request/identity frame to the client, before restarting the authentication process.	Interface Configuration
dot1x timeout supp-timeout	Sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client.	Interface Configuration
dot1x timeout server-timeout	Sets the time for the retransmission of packets to the authentication server.	Interface Configuration
show dot1x	Allows multiple hosts on an 802.1x-authorized port, that has the **dot1x port-control** interface configuration command set to **auto**.	Privileged EXEC

show dot1x users	Displays active 802.1x authenticated users.	Privileged EXEC
show dot1x statistics	Displays 802.1x statistics for the specified interface.	Privileged EXEC
dot1x auth-not-req	Enables unauthorized users access to that VLAN.	Interface (VLAN) Configuration
dot1x multiple-hosts	Allows multiple hosts (clients) on an 802.1x-authorized port, that has the **dot1x port-control** Interface Configuration mode command set to **auto**.	Interface Configuration
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.	Interface Configuration
dot1x guest-vlan	Defines a guest VLAN.	Interface Configuration
dot1x guest-vlan enable	Enables unauthorized users on the interface to access the guest VLAN.	Interface Configuration
show dot1x advanced	Displays 802.1x advanced features for the device or for the specified interface.	Privileged EXEC

2

Command Modes

GC (Global Configuration) Mode

Command	Description
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels.
aaa authentication login	Defines login authentication.
aaa authentication dot1x	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x.
aaa logging	Enables logging AAA login events.
aaa login-history file	Enables writing to the login history file.
arp	Adds a permanent entry in the ARP cache.
arp timeout	Configures how long an entry remains in the ARP cache
asset-tag	Specifies the device asset-tag.
bridge aging-time	Sets the address table aging time.
bridge multicast filtering	Enables filtering of multicast addresses.
clock source	Configures an external time source for the system clock
clock timezone	Sets the time zone for display purposes
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
crypto certificate generate	Generates a HTTPS certificate.
crypto certificate import	Imports a certificate signed by Certification Authority for HTTPS.
crypto key generate dsa	Generates DSA key pairs.
crypto key generate rsa	Generates RSA key pairs.
crypto key pubkey-chain ssh	Enters SSH Public Key-chain configuration mode.
crypto slogin key generate dsa	Generates DSA key pairs for secure login to a remote access server.
crypto slogin key generate rsa	Generates RSA key pairs for secure login to a remote access server.
dot1x system-auth-control	Enables 802.1x globally.

enable password	Sets a local password to control access to normal and privilege levels.
end	Ends the current configuration session and returns to the previous command mode.
file-system logging	Enables logging file system events.
gvrp enable (Global)	Enables GVRP globally.
hostname	Specifies or modifies the device host name.
interface ethernet	Enters the interface configuration mode to configure an Ethernet type interface.
interface port-channel	Enters the interface configuration mode of a specific port-channel.
interface range ethernet	Enters the interface configuration mode to configure multiple ethernet type interfaces.
interface range port-channel	Enters the interface configuration mode to configure multiple port-channels.
interface range vlan	Enters the interface configuration mode to configure multiple VLANs.
interface vlan	Enters the interface configuration (VLAN) mode.
ip default-gateway	Defines a default gateway.
ip domain-lookup	Enables the IP Domain Naming System (DNS)-based host name-to-address translation.
ip domain-name	Defines a default domain name, that the software uses to complete unqualified host names.
ip host	Defines static host name-to-address mapping in the host cache.
ip http authentication	Specifies authentication methods for HTTP server users.
ip http port	Specifies the TCP port for use by a web browser to configure the device.
ip http server	Enables the device to be configured from a browser.
ip https authentication	Specifies authentication methods for HTTPS server users.
ip https certificate	Configures the active certificate for HTTPS.
ip https server	Enables the device to be configured from a secured browser.
ip https port	Configures a TCP port for use by a secure web browser to configure the device.
ip igmp snooping (Global)	Enables Internet Group Management Protocol (IGMP) snooping
ip name-server	Sets the available name servers.
ip ssh port	Specifies the port to be used by the SSH server.
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions.

ip ssh server	Enables the device to be configured from a SSH server.
lacp system-priority	Configures the system LACP priority.
line	Identifies a specific line for configuration and enters the line configuration command mode.
logging	Logs messages to a syslog server.
logging buffered	Limits syslog messages displayed from an internal buffer based on severity.
logging buffered size	Changes the number of syslog messages stored in the internal buffer.
logging console	Limits messages logged to the console based on severity.
logging file	Limits syslog messages sent to the logging file based on severity.
logging on	Controls error messages logging.
mac access-list	Creates Layer 2 ACLs.
management access-class	Defines which management access-list is used.
management access-list	Defines a management access-list, and enters the access-list for configuration.
management logging	Enables logging management access list events.
passwords aging	Sets the expiration time for passwords in the local database.
passwords history	Sets the number of required password changes before a password in the local database can be reused.
passwords history hold-time	Sets the number of days a password is relevant for tracking its password history.
passwords lockout	Sets the number of failed login attempts before a user account is locked.
passwords min-length	Sets the minimum required length for passwords in the local database.
power inline traps enable	Adds a description of the powered device type attached to the interface.
power inline usage-threshold	Configures the administrative mode of the inline power on an interface.
priority-queue out num-of-queues	Enables the egress queues to be SP queues.
qos	Enables Quality of Service (QoS) on the device and enters QoS basic or advance mode.
qos map dscp-queue	Modifies the DSCP to CoS map.
qos trust (Global)	Configure the system to "trust" state.
radius-server deadtime	Improves RADIUS response times when servers are unavailable.

radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.
radius-server timeout	Sets the interval for which a device waits for a server host to reply.
rmon alarm	Configures alarm conditions.
rmon event	Configures a RMON event.
rmon table-size	Configures the maximum RMON tables sizes.
service cpu-utilization	Enables measuring CPU utilization.
snmp-server community	Sets up the community access string to permit access to SNMP protocol.
snmp-server contact	Sets up a system contact.
snmp-server enable traps	Enables the device to send SNMP traps or SNMP notifications.
snmp-server engineID local	Specifies an SNMP EngineID on the local device.
snmp-server filter	Creates and modifies filter entries.
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
snmp-server host	Specifies the recipient of Simple Network Management Protocol notification operation.
snmp-server v3-host	Specifies an SNMP v3 notification recipient.
snmp-server location	Sets up the information on where the device is located.
snmp-server set	Sets SNMP MIB value by the CLI.
snmp-server trap authentication	Enables the device to send Simple Network Management Protocol traps when authentication failed.
snmp-server user	Configures a new SNMP v3 user.
snmp-server view	Creates and modifies view entries.
sntp authenticate	Grants authentication for received Simple Network Time Protocol (SNTP) traffic from servers.
sntp authentication-key	Defines an authentication key for Simple Network Time Protocol (SNTP).
spanning-tree	Enables spanning tree functionality.

spanning-tree bpdu	Defines BPDU handling when spanning tree is disabled on an interface
spanning-tree forward-time	Configures the spanning tree bridge forward time.
spanning-tree hello-time	Configures the spanning tree bridge Hello Time.
spanning-tree max-age	Configures the spanning tree bridge maximum age.
spanning-tree mode	Configures the spanning tree protocol.
spanning-tree mst configuration	Enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.
spanning-tree mst max-hops	Configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out.
spanning-tree mst priority	Configures the device priority for the specified spanning-tree instance.
spanning-tree pathcost method	Sets the default pathcost method.
spanning-tree priority	Configures the spanning tree priority.
stack display-order	Configures the display order of the units in a stack.
stack master	Forces selection of a stack master.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon.
tacacs-server source-ip	Specifies the source IP address that will be used for the communication with TACACS+ servers.
tacacs-server timeout	Sets the timeout value.
tacacs-server host	Specifies a TACACS+ host.
username	Establishes a username-based authentication system.
vlan database	Enters the VLAN database configuration mode.
wrr-queue cos-map	Maps CoS values to a specific egress queu

IC (Interface Configuration) Mode

Command	Description
back-pressure	Enables Back Pressure on a given interface.
bridge multicast forward-all	Enables forwarding all multicast frames on a port.
bridge multicast forbidden forward-all	Forbids a port from becoming a forward-all multicast port.
channel-group	Associates a port with a Port-channel.
description	Adds a description to an interface.

dot1x guest-vlan	Defines a guest VLAN.
dot1x guest-vlan enable	Enables unauthorized users on the interface to access the guest VLAN.
dot1x max-req	Sets the maximum number of times that the device sends an EAP - request/identity frame to the client, before restarting the authentication process.
dot1x multiple-hosts	Allows multiple hosts (clients) on an 802.1x-authorized port, that has the **dot1x port-control** Interface Configuration mode command set to **auto**.
dot1x port-control	Enables manual control of the authorization state of the port
dot1x re-authentication	Enables periodic re-authentication of the client.
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.
dot1x timeout quiet-period	Sets the number of seconds that the device remains in the quiet state following a failed authentication exchange.
dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.
dot1x timeout server-timeout	Sets the time for the retransmission of packets to the authentication server
dot1x timeout supp-timeout	Sets the time for the retransmission of an EAP-request frame to the client.
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.
duplex	Configures the full/half duplex operation of a given ethernet interface when not using auto-negotiation.
flowcontrol	Configures the Flow Control on a given interface.
garp timer	Adjusts the GARP application join, leave, and leaveall GARP timer values.
gvrp enable (Interface)	Enables GVRP on an interface.
gvrp registration-forbid	De-registers all VLANs, and prevents dynamic VLAN registration on the port.
gvrp vlan-creation-forbid	Enables or disables dynamic VLAN creation.
ip address	Sets an IP address
ip address dhcp	Acquires an IP address on an interface from the DHCP server.
ip internal-usage-vlan	Reserves a VLAN as the internal usage VLAN of an interface.
lacp port-priority	Configures the priority value for physical ports.
lacp timeout	Assigns an administrative LACP timeout.

mdix	Enables automatic crossover on a given interface.
name	Configures a name to a VLAN.
negotiation	Enables auto-negotiation operation for the speed and duplex parameters of a given interface.
power inline	Configures the administrative mode of the inline power on an interface.
power inline powered-device	Adds a description of the powered device type attached to the interface.
power inline priority	Displays port monitoring status
port monitor	Starts a port monitoring session.
port security	Disables new address learning/forwarding on an interface.
port monitor vlan-tagging	Transmits tagged ingress mirrored packets.
port security max	Configures the maximum number of addresses that may be learned on the port while the port is in port security mode
port security mode	Configures the port security learning mode
port security routed secure-address	Adds MAC-layer secure addresses to a routed port.
port storm-control broadcast enable	Enables broadcast storm control.
port storm-control broadcast rate	Configures the maximum broadcast rate.
port storm-control include-multicast	Enables the device to count multicast packets.
private-vlan community	Associates the primary VLAN and community VLANs.
private-vlan isolated	Defines the isolated VLAN of the PVLAN.
private-vlan primary	Defines the primary PVLAN.
qos cos	Configures the default port CoS value.
qos trust (Interface)	Enables each port trust state while the system is in basic mode.
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.
service-acl	Applies an ACL to the input interface.
shutdown	Disables interfaces.
sntp client enable (Interface)	Enables the Simple Network Time Protocol (SNTP) client on an interface.
spanning-tree cost	Configures the spanning tree path cost for a port.
spanning-tree disable	Disables spanning tree on a specific port.

spanning-tree link-type	Overrides the default link-type setting.
spanning-tree mst cost	Configures the path cost for multiple spanning tree (MST) calculations.
spanning-tree mst port-priority	Configures the priority of a port.
spanning-tree portfast	Enables PortFast mode.
spanning-tree port-priority	Configures port priority.
speed	Configures the speed of a given Ethernet interface when not using auto-negotiation.
switchport private-vlan	Defines the private-vlan port VLANs.

LC (Line Configuration) Mode

Command	Description
autobaud	Configures the line for automatic baud rate detection (autobaud)
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.
history	Enables the command history function.
history size	Configures the command history buffer size for a particular line.
login authentication	Specifies the login authentication method list for a remote telnet or console.
password	Specifies a password on a line.
password-aging	Sets the expiration time of line passwords in the local database.
speed	Configures the baud rate of the line.

MA (Management Access-level) Mode

Command	Description
deny (Management)	Defines a deny rule.
permit (Management)	Defines a permit rule.

MC (MST Configuration) Mode

Command	Description
abort (mst)	Exits the MST region configuration mode without applying configuration changes.
exit (mst)	Exits the MST region configuration mode and applies all configuration changes.
instance (mst)	Maps VLANs to the MST instance.
name (mst)	Defines the configuration name.
revision (mst)	Defines the configuration revision number.
show (mst)	Displays the current or pending MST region configuration.

ML (MAC Access-List) Mode

Command	Description
deny (MAC)	Denies traffic if the conditions defined in the permit statement match.

PE (Privileged EXEC) Mode

Command	Description
boot system	Specifies the system image that the device loads at startup.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear bridge	Removes any learned entries from the forwarding database.
clear gvrp statistics	Clears all the GVRP statistics information.
clear host	Deletes entries from the host name-to-address cache
clear host dhcp	Deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).
clear logging	Clears messages from the internal logging buffer.
clear logging file	Clears messages from the logging file
clear spanning-tree detected-protocols	Restarts the protocol migration process on all interfaces or on the specified interface.
clock set	Manually sets the system clock.
configure	Enters the Global Configuration mode.
copy	Copies files from a source to a destination.
crypto certificate request	Generates and displays certificate requests for HTTPS.

delete	Deletes a file from a Flash memory device.
delete startup-config	Deletes the startup-config file.
dir	Displays a list of files on a flash file system.
dot1x re-authenticate	Manually initiates a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.
exit	Closes an active terminal session by logging off the device.
login	Changes a login username.
more	Displays a file.
reload	Reloads the operating system.
rename	Renames a file.
set enable-password active	Reactivates a locked local password.
set interface active	Reactivates an interface that was suspended by the system.
set line active	Reactivates a locked line.
set username active	Reactivates a locked user account.
show access-lists	Displays ACLs defined on the device.
show arp	Displays entries in the ARP table.
show authentication methods	Displays information about the authentication methods.
show bootvar	Displays the active system image file that the device loads at startup
show bridge address-table	Displays all entries in the bridge-forwarding database.
show bridge address-table count	Displays the number of addresses present in all VLANs or at specific VLAN.
show bridge multicast address-table	Displays multicast MAC or IP address table information.
show bridge multicast filtering	Displays the multicast filtering configuration.
show crypto key mypubkey	Displays the SSH public keys stored on the device.
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the device.
show crypto certificate mycertificate	Displays the SSL certificates of the device
show crypto slogin key mypubkey	Displays the secure login public key of the device.
show dot1x	Displays 802.1x status for the device or for the specified interface.
show dot1x advanced	Displays 802.1x enhanced features for the device or for the specified interface.

show dot1x users	Displays 802.1x users for the device.
show dot1x statistics	Displays 802.1x statistics for the specified interface.
show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics
show hosts	Displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses.
show interfaces access-lists	Displays access lists applied on interfaces.
show interfaces advertise	Displays autonegotiation advertisement data.
show interfaces configuration	Displays the configuration for all interfaces.
show interfaces counters	Displays traffic seen by the physical interface.
show interfaces description	Displays the description for all interfaces.
show interfaces port-channel	Displays Port-channel information.
show interfaces status	Displays the status for all interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip ssh	Displays the SSH server configuration.
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.
show logging file	Displays the state of logging and the syslog messages stored in the logging file.
show management access-class	Displays the active management access-list.
show management access-list	Displays management access-lists.
show passwords configuration	Displays information about password management.
show ports security	Displays the port-lock status.
show ports security addresses	Displays current dynamic addresses in locked ports
show ports storm-control	Displays the storm control configuration.
show cpu utilization	Displays information about the CPU utilization of active processes.
show radius-servers	Displays the RADIUS server settings.
show running-config	Displays the contents of the currently running configuration file.
show snmp	Displays the SNMP status.
show snmp engineid	Displays the local SNMP EngineID.
show snmp filters	Displays the configuration of SNMP filters.
show snmp groups	Displays the configuration of SNMP groups.
show snmp users	Displays the configuration of SNMP users.

show snmp views	Displays the configuration of SNMP views.
show spanning-tree	Displays spanning tree configuration.
show startup-config	Displays the startup configuration file contents.
show syslog-servers	Displays the syslog servers settings.
show tacacs	Displays configuration and statistics for a TACACS+ servers.
show users accounts	Displays information about the local user database.
show users login-history	Displays information about the login history of users.
show vlan internal usage	Displays a list of VLANs used internally by the device.
show vlan mac-to-vlan	Displays the MAC-to-VLAN database.
show vlan private-vlan	Displays information about private VLANs.
stack reload	Reloads stack members
test copper-port tdr	Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.

SP (SSH Public Key) Mode

Command	Description
key-string	Manually specifies a SSH public key.
user-key	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command

UE (User EXEC) Mode

Command	Description
clear counters	Clears statistics on an interface.
enable	Enters the Privileged EXEC mode.
exit	Closes an active terminal session by logging off the device.
login	Changes a login username.
ping	Sends ICMP echo request packets to another node on the network.
show clock	Displays the time and date from the system clock.
show copper-ports cable-length	Displays the estimated copper cable length attached to a port.
show copper-ports tdr	Displays the last TDR (Time Domain Reflectometry) tests on specified ports.
show gvrp configuration	Displays GVRP configuration information.

show gvrp error-statistics	Displays GVRP error statistics.
clear gvrp statistics	Displays GVRP statistics.
show history	Lists the commands entered in the current session.
show ip igmp snooping mrouter	Enables automatic learning of multicast switch ports in the context of a specific VLAN.
show ip igmp snooping groups	Displays multicast groups learned by IGMP snooping.
show ip igmp snooping interface	Displays IGMP snooping configuration.
show ip igmp snooping mrouter	Displays information on dynamically learned multicast router interfaces.
show lacp ethernet	Displays LACP information for Ethernet ports.
show lacp port-channel	Displays LACP information for a port-channel.
show line	Displays line parameters.
show ports monitor	Displays port monitoring status
show power inline	Displays information about inline power.
show privilege	Displays the current privilege level.
show qos	Displays the QoS status.
show qos interface	Assigns CoS values to select one of the egress queues.
show qos map	Displays all the maps for QoS.
show rmon alarm	Displays alarm configurations.
show rmon alarm-table	Displays the alarms table.
show rmon collection history	Displays the requested history group configuration.
show rmon events	Displays the RMON event table.
show rmon history	Displays RMON Ethernet Statistics history.
show rmon log	Displays the RMON logging table.
show rmon statistics	Displays RMON Ethernet Statistics.
show stack	Displays information about stack status.
show system	Displays system information.
show system id	Displays the service id information.
show users	Displays information about the active users.
show version	Displays the system version information.
terminal datadump	Enables dumping all output of a show command without prompting.

terminal history	Enables the command history function for the current terminal session.
terminal history size	Configures the command history buffer size for the current terminal session.

VC (VLAN Configuration) Mode

Command	Description
bridge address	Adds a static MAC-layer station source address to the bridge table.
bridge multicast address	Registers MAC-layer multicast addresses to the bridge table, and adds static ports to the group.
bridge multicast forbidden address	Forbids adding a specific multicast address to specific ports.
bridge multicast forbidden forward-all	Enables forbidding forwarding of all multicast frames to a port.
bridge multicast forward-all	Enables forwarding of all multicast frames on a port.
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.
ip igmp snooping host-time-out	Configures the host-time-out.
ip igmp snooping leave-time-out	Configures the leave-time-out.
ip igmp snooping mrouter learn-pim-dvmrp	Enables automatic learning of multicast router ports.
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out.
mac-to-vlan	Adds MAC addresses to the MAC-to-VLAN database.
vlan	Creates a VLAN.
dot1x auth-not-req	Enables unauthorized users access to that VLAN.
name	Configures a name to a VLAN.

3

Using the CLI

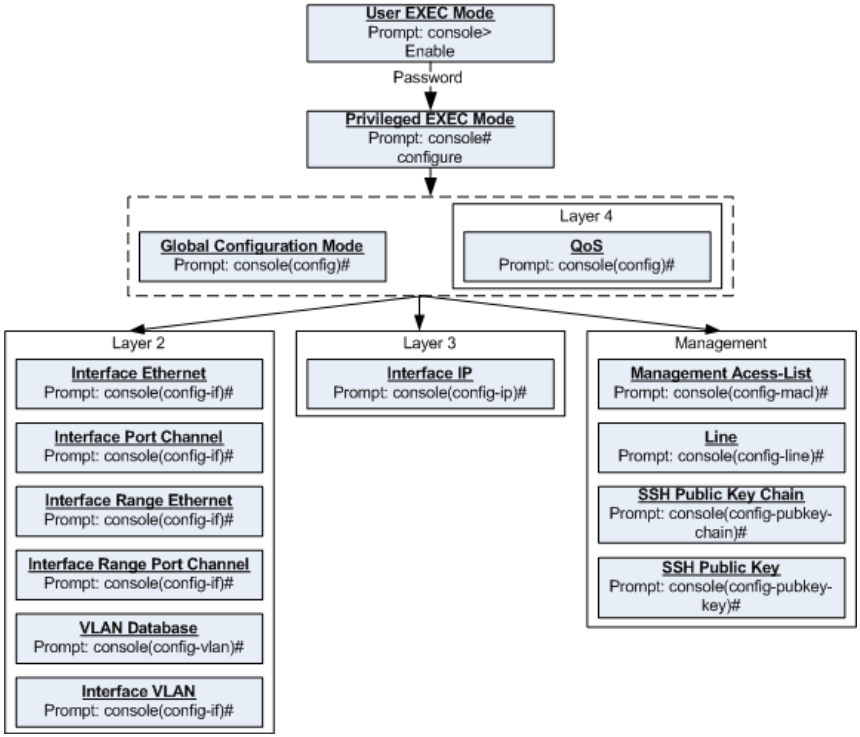
This chapter describes how to start using the CLI and describes the command editing features to assist in using the CLI.

CLI Command Modes

Introduction

To assist in configuring the device, the Command Line Interface (CLI) is divided into different command modes. Each command mode has its own set of specific commands. Entering a question mark "?" at the system prompt (console prompt) displays a list of commands available for that particular command mode.

From each mode a specific command is used to navigate from one command mode to another. The standard order to access the modes is as follows: *User EXEC* mode, *Privileged EXEC* mode, *Global Configuration* mode, and *Interface Configuration* mode. The following figure illustrates the command mode access path.



When starting a session, the initial mode is the User EXEC mode. Only a limited subset of commands are available in the User EXEC mode. This level is reserved for tasks that do not change the configuration. To enter the next level, the Privileged EXEC mode, a password is required.

The Privileged EXEC mode gives access to commands that are restricted on User EXEC mode and provides access to the device Configuration mode.

The Global Configuration mode manages the device configuration on a global level.

The Interface Configuration mode configures specific interfaces in the device.

User EXEC Mode

After logging into the device, the user is automatically in the User EXEC command mode unless the user is defined as a privileged user. In general, the User EXEC commands allow the user to perform basic tests, and list system information.

The user-level prompt consists of the device host name followed by the angle bracket (>).

```
Console>
```

The default host name is Console unless it was changed using the **hostname** command in the Global Configuration mode.

Privileged EXEC Mode

Privileged access is password protected to prevent unauthorized use because, many of the privileged commands set operating system parameters. The password is not displayed on the screen and is case sensitive.

Privileged users enter directly into the Privileged EXEC mode. To enter the Privileged EXEC mode from the User EXEC mode, perform the following steps:

1. At the prompt enter the **enable** command and press <Enter>. A password prompt appears.
2. Enter the password and press <Enter>. The password is displayed as *. The Privileged EXEC mode prompt is displayed. The Privileged EXEC mode prompt consists of the device host name followed by **#**.

```
Console#
```

To return from the Privileged EXEC mode to the User EXEC mode, use the **disable** command. The following example illustrates how to access the Privileged EXEC mode and return to the User EXEC mode:

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

The **exit** command is used to return from any mode to the previous mode except when returning to the User EXEC mode from the Privileged EXEC mode. For example, the **exit** command is used to return from the Interface Configuration mode to the Global Configuration mode.

Global Configuration Mode

Global Configuration mode commands apply to features that affect the system as a whole, rather than just a specific interface. The **configure** Privileged EXEC mode command is used to enter the Global Configuration mode.

To enter the Global Configuration mode, at the Privileged EXEC mode prompt enter the command **configure** and press <Enter>. The Global Configuration mode prompt is displayed. The Global Configuration mode prompt consists of the device host name followed by (config) and **#**.

```
Console(config)#
```

To return from the Global Configuration mode to the Privileged EXEC mode, the user can use one of the following commands:

- **exit**
- **end**
- **Ctrl+Z**

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

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

Interface Configuration Mode and Specific Configuration Modes

Interface Configuration mode commands modify specific interface operations. The following are the Interface Configuration modes:

- **Line Interface** — Contains commands to configure the management connections. These include commands such as line timeout settings, etc. The **line** Global Configuration mode command is used to enter the Line Configuration command mode.
- **VLAN Database** — Contains commands to create a VLAN as a whole. The **vlan database** Global Configuration mode command is used to enter the VLAN Database Interface Configuration mode.
- **Management Access List** — Contains commands to define management access-lists. The **management access-list** Global Configuration mode command is used to enter the Management Access List Configuration mode.

- **Ethernet** — Contains commands to manage port configuration. The **interface ethernet** Global Configuration mode command is used to enter the Interface Configuration mode to configure an Ethernet type interface.
- **Port Channel** — Contains commands to configure port-channels, for example, assigning ports to a port-channel. Most of these commands are the same as the commands in the Ethernet interface mode, and are used to manage the member ports as a single entity. The **interface port-channel** Global Configuration mode command is used to enter the Port Channel Interface Configuration mode.
- **SSH Public Key-chain** — Contains commands to manually specify other device SSH public keys. The **crypto key pubkey-chain ssh** Global Configuration mode command is used to enter the SSH Public Key-chain Configuration mode.
- **QoS —** Contains commands related to service definitions. The **qos** Global Configuration mode command is used to enter the QoS services configuration mode.
- **MAC Access-List—** Configures conditions required to allow traffic based on MAC addresses. The **mac access-list** Global Configuration mode command is used to enter the MAC access-list configuration mode..

Starting the CLI

The device can be managed over a direct connection to the device console port or via a Telnet connection. The device is managed by entering command keywords and parameters at the prompt. Using the device command-line interface (CLI) is very similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure that the device has a defined IP address, corresponding management access is granted, and the workstation used to access the device is connected to the device prior to using CLI commands.

NOTE: The following steps are for use on the console line only.

To start using the CLI, perform the following steps:

1. Connect the DB9 null-modem or cross over cable to the RS-232 serial port of the device to the RS-232 serial port of the terminal or computer running the terminal emulation application.

NOTE: The default data rate, for Carrier, is 115,200 (Console port on unit shows a default data rate of 9600).

   a. Set the data format to 8 data bits, 1 stop bit, and no parity.

   b. Set Flow Control to **none**.

   c. Under **Properties**, select **VT100 for Emulation** mode.

   d. Select **Terminal keys** for **Function, Arrow, and Ctrl keys**. Ensure that the setting is for **Terminal keys** (not **Windows keys**).

NOTICE: When using HyperTerminal with Microsoft® Windows 2000,ensure that Windows® 2000 Service Pack 2 or later is installed.With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal's VT100 emulation. Go to www.microsoft.com for information on Windows 2000 service packs.

For more information, see **Dell™ PowerConnect™ 3400 Series User's Guide**.

2. Enter the following commands to begin the configuration procedure:

```
Console> enable

Console# configure

Console(config)#
```

3. Configure the device and enter the necessary commands to complete the required tasks.
4. When finished, exit the session with the **exit** command.

When a different user is required to log onto the system, use the **login** Privileged EXEC mode command. This effectively logs off the current user and logs on the new user.

Editing Features

Entering Commands

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/e11**, **show**, **interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/e11** specifies the port.

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 alansmith
```

When working with the CLI, the command options are not displayed. The command is not selected from a menu, but is manually entered. To see what commands are available in each mode or within an interface configuration, the CLI provides a method of displaying the available commands, the command syntax requirements and in some instances, parameters required to complete the command. The standard command to request help is the character **?**.

There are two instances where help information can be displayed:

- **Keyword lookup** — The character **?** is entered in place of a command. A list of all valid commands and corresponding help messages are is displayed.
- **Partial keyword lookup** — If a command is incomplete and or the character **?** is entered in place of a parameter. The matched keyword or parameters for this command are displayed.

To assist in using the CLI, there is an assortment of editing features. The following features are described:

- Terminal Command Buffer
- Command Completion
- Keyboard Shortcuts

Copying and Pasting Text

Up to 100 lines of text (i.e., commands) can be copied and pasted into the device.

NOTE: This editing features are for Telnet only.

NOTE: It is the user's responsibility to ensure that the text copied into the device consists of legal commands only.

When copying and pasting commands from a configuration file, make sure that the following conditions exist:

- A device Configuration mode has been accessed.
- The commands contain no encrypted data, like encrypted passwords or keys. Encrypted data cannot be copied and pasted into the device.

Setup Wizard

The CLI supports a Setup Wizard. This is an easy-to-use user interface which quickly guides the user in setting up basic device information, so that the device can be easily managed from a Web Based Interface. Refer to the **Getting Started Guide** and **User Guide** for more information on the Setup Wizard.

Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a *First In First Out (FIFO)* basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

Keyword	Description
Up-arrow key Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command. Repeats the key sequence to recall successively older commands.
Down-arrow key	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command syntax to enable or disable the history buffer, see **history**.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 216. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see **history size**.

To display the history buffer, see **show history**.

Negating the Effect of Commands

For many configuration commands, the prefix keyword ***no*** can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

Command Completion

An appropriate error message displays if the entered command is incomplete or invalid; or has missing or invalid parameters. This assists in entering the correct command.

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

Keyboard Key	Description
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow key	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any configuration mode.
Backspace key	Deletes one character left to the cursor position.

CLI Command Conventions

When entering commands there are certain command entry standards that apply to all commands. The following table describes the command conventions.

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated by the | character. One option must be selected. For example, **flowcontrol {auto|on|off}** means that for the **flowcontrol** command either **auto**, **on** or **off** must be selected.
Italic font	Indicates a parameter.
<Enter>	Indicates an individual key on the keyboard. For example, <Enter> indicates the **Enter** key.
Ctrl+F4	Any combination of keys pressed simultaneously on the keyboard.
`Screen Display`	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and **all** is an option, the default for the command is **all** when no parameters are defined. For example, the command **interface range port-channel** has the option of either entering a range of channels, or selecting **all**. When the command is entered without a parameter, it automatically defaults to **all**.

4

AAA Commands

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*}

- **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 Configuration

The local user database is checked. This has the same effect as the command **aaa authentication login default local**.

NOTE: On the console, login succeeds without any authentication check if the authentication method is not defined.

Command Mode

Global Configuration mode

User Guidelines

- 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, so that user authentication is performed as follows: Authentication is attempted at the RADIUS server. If the RADIUS server is not available, authentication is attempted at the local user database. If there is no database, then no authentication is performed.

```
Console(config)# aaa authentication login radius local none
```

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*}

- **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 Configuration

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

User Guidelines

- 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
```

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

- **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 Configuration

Uses the default set with the command **aaa authentication login**.

Command Mode

Line Configuration mode

User Guidelines

- 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
```

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

- **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 Configuration

Uses the default set with the **aaa authentication enable** command.

Command Mode

Line Configuration mode

User Guidelines

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
```

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

- *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 Configuration

The local user database is checked. This has the same effect as the command **ip http authentication local**.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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

- *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 Configuration

The local user database is checked. This has the same effect as the command **ip https authentication local**.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

show authentication methods

The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

Syntax

show authentication methods

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 authentication configuration.

```
Console# sh authentication methods
Login Authentication Method Lists
---------------------------------
Console_Default: None
Network_Default: Local

Enable Authentication Method Lists
----------------------------------
Console_Default: Enable, None
Network_Default: Enable
```

```
Line                    Login Method List       Enable Method List
--------------          -----------------       ------------------
Console                 Default                 Default
Telnet                  Default                 Default
SSH                     Default                 Default

http                    : Local
https                   : Local
dot1x                   :
console#
```

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

- *password* — Password for this level (Range: 1-159 characters).
- **encrypted** — Encrypted password to be entered, copied from another device configuration.

Default Configuration

No password is defined.

Command Mode

Line Configuration mode

User Guidelines

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
```

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*]

- *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 Configuration

No enable password is defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets local level 15 password **secret** to control access to privilege levels.

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

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*

- *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 Configuration

No user is defined.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

passwords min-length

The **passwords min-length** Global Configuration mode command sets the minimum length required for passwords in the local database. To remove the minimum password length requirement, use the **no** form of this command.

Syntax

passwords min-length *length*

no passwords min-length

- *length* — The minimum length required for passwords. (Range: 8-64 characters)

Default Configuration

No minimum password length.

Command Mode

Global Configuration mode

User Guidelines

- Relevant to local user passwords, line passwords, and enable passwords.
- The software checks the password length when an unencrypted password is defined or a user enters an unencrypted password when logging in.

NOTE: The length of encrypted passwords is only checked when the user logs in. Similarly, the length of passwords that were defined before the minimum password length requirement was configured are checked only when the user logs in.

Example

The following example configures a minimum length of 8 characters required for passwords in the local database.

```
Console(config)# passwords min-length 8
```

passwords aging

The **passwords aging** Global Configuration mode command sets the expiration time of username and enable passwords. To remove the password expiration time, use the **no** form of this command.

Syntax

passwords aging username *name days*

no passwords aging username *name*

passwords aging enable-password *level days*

no passwords aging enable-password *level*

- *days*—The number of days before a password expires. (Range: 1-365)
- *name* — The name of the user (Range: 1- 20 characters).
- *level* — The level to which the password applies (Range: 1-15).

Default Configuration

No password expiration time.

Command Mode

Global Configuration mode

User Guidelines

- Relevant to local user passwords, line passwords, and enable passwords.
- The password expiration date is calculated from the day the password is defined, and not from the day aging time is defined.
- Ten days before the password expiration date, the user receives a syslog warning to change the password within "n" days. These warnings continue until the password expiration date.
- After the password expiration date, the user receives three chances to log in and change the password. If the user still does not change the password, the account is locked.
- It is recommended that local device time be updated using an external SNTP clock.

Example

The following example sets the expiration time of the level 15 enable password to 180 days.

```
Console (config)# passwords aging enable-password 15 180
```

password-aging

The **password-aging** Line Configuration mode command configures the expiration time of line passwords in the local database. To return to the default configuration, use the **no** form of this command.

Syntax

password-aging *days*

no password-aging

- *days*—The number of days before a password expires (Range: 1-365).

Default Configuration

No password expiration time.

Command Mode

Line Configuration mode

User Guidelines

- The password expiration date is calculated from the day the password is defined, and not from the day aging time is defined.
- Ten days before the password expiration date, the user receives a warning to change the password within "n" days. These warnings continue until the password expiration date.
- After the password expiration date, the user receives three chances to log in and change the password. If the user still does not change the password, the account is locked.

Example

The following example configures password aging to 120 days.

```
Console(config)# line telnet
Console(config-line)# password-aging 120
```

passwords history

The **passwords history** Global Configuration mode command sets the number of required password changes before a password in the local database can be reused. To remove this requirement, use the **no** form of this command.

Syntax

passwords history *number*

no passwords history

- *number*—Indicates the required number of password changes before a password can be reused. (Range: 1-10).

Default Configuration

No required number of password changes before reusing a password.

Command Mode

Global Configuration mode

User Guidelines

- Relevant to local user passwords, line passwords, and enable passwords.
- Password history is not checked during the configuration download.
- Password history is saved even if the feature is disabled.
- A user's password history is saved as long as the user is defined.
- If the user enters a password that is identical to the previously used one, the password is not included in the password history count. This is required to enable the user to modify privilege level or aging, without having to change passwords.

Example

The following example configures the required number of password changes before a password can be reused to 3.

```
Console(config)# passwords history 3
```

passwords history hold-time

The **passwords history hold-time** Global Configuration mode command configures the number of days a password is relevant for tracking its password history. To return to the default configuration, use the **no** form of this command.

Syntax

passwords history hold-time *days*

no passwords hold-time

- *days*—Number of days a password is relevant for tracking its password history (Range: 1-product specific).

Default Configuration

Not enabled.

Command Mode

Global Configuration mode

User Guidelines

Relevant to local user passwords, line passwords, and enable passwords.

Passwords are not deleted from the history database when they are no longer relevant for tracking purposes. Increasing the number of days a password is relevant, for tracking purposes, may make a password, that is no longer relevant for tracking purposes, relevant again.

Example

The following example configures the number of days that a password is relevant for tracking its password history to 120.

```
Console(config)# passwords history hold-time 120
```

passwords lockout

The **passwords lockout** Global Configuration mode command sets the number of failed login attempts before a user account is locked. To remove this condition, use the **no** form of this command.

Syntax

passwords lockout *number*

no passwords lockout

- *number*—Number of failed login attempts before the user account is locked (Range: 1-5).

Default Configuration

No locked user account due to failed login attempts.

Command Mode

Global Configuration mode

User Guidelines

- Relevant to local user passwords, line passwords, and enable passwords.
- The user account can still access the local console.
- A different administrator, with privilege level 15, can release a locked account by using the **set username active** command.

Example

The following example configures the number of failed login attempts before a user account is locked to 3.

```
Console(config)# passwords lockout 3
```

aaa login-history file

The **aaa login-history file** Global Configuration mode command enables writing to the login history file. To disable writing to the file, use the **no** form of this command.

Syntax

aaa login-history file

no aaa login-history file

Default Configuration

Writing to the login history file is enabled.

Command Mode

Global Configuration mode

User Guidelines

The login history is also saved in the internal buffer of the device.

Example

The following example enables writing to the login history file.

```
Console(config)# aaa login-history file
```

set username active

The **set username active** Privileged EXEC mode command reactivates a locked user account.

Syntax

set username *name* **active**

- *name*—Name of the user (Range: 1-20 characters).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- A locked user account can be reactivated from the local console.
- A different user, with privilege level 15, can reactivate a locked user account from any remote or local connection.

Example

The following example reactivates a suspended user with username **bob**.

```
Console# set username bob active
```

set line active

The **set line active** Privileged EXEC mode command reactivates a locked line.

Syntax

set line {console | telnet | ssh} active

- **console**—Console terminal line.
- **telnet**—Virtual terminal for remote console access (Telnet).
- **ssh**—Virtual terminal for secured remote console access (SSH).

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 reactivates the line for a virtual terminal for remote console access.

```
Console# set line telnet active
```

set enable-password active

The **set enable-password active** Privileged EXEC mode command reactivates a locked enable password.

Syntax

set enable-password *level* **active**

- *level*—The user level (Range: 1 -15).

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 reactivates a locked level 15 enable password.

```
Console# set enable-password 15 active
```

show passwords configuration

The **show passwords configuration** Privileged EXEC mode command displays information about password management.

Syntax

show passwords configuration

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 information about password management in the local database.

```
Console# show passwords configuration
Minimal length: 8
History: 10
History hold time: 365 days
Lock-out: Disabled

Enable Passwords
Level            Aging           Expiry date      Lockout
-----            -----           -----------      -------
1                90              Jan 18 2005      1
15               90              Jan 18 2005      0

Line Passwords
Level            Aging           Expiry date      Lockout
-----            -----           -----------      -------
Console          -               -                -
Telnet           90              Jan 18 2005      LOCKOUT
SSH              90              Jan 21 2005      0
```

The following table describes significant fields shown above.

Field	Description
Minimal length	Minimum length required for passwords in the local database.
History	Number of required passwords changes before a password in the local database can be reused.
History hold time	Period of time that a password is relevant for tracking password history.
Lockout control	Control locking a user account after a series of authentication failures.
Enable passwords	Describes the configuration and status of a local password with a specific level.
Aging	Password expiration time in days.
Expiry date	Expiration date of a 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.
Line Passwords	Describes the configuration and status of a specific line password.

show users login-history

The **show users login-history** Privileged EXEC mode command displays information about the login history of users.

Syntax

show users login-history [**username** *name*]

- *name*—Name of the user (Range: 1-20 characters).

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 login history of users.

```
Console# show users login-history


Login Time              Username     Protocol    Location
--------------          --------     --------    --------
Jan 18 2004 23:58:17    Robert       HTTP        172.16.1.8
Jan 19 2004 07:59:23    Robert       HTTP        172.16.0.8
Jan 19 2004 08:23:48    Bob          Serial
Jan 19 2004 08:29:29    Robert       HTTP        172.16.0.8
Jan 19 2004 08:42:31    John         SSH         172.16.0.1
Jan 19 2004 08:49:52    Betty        Telnet      172.16.1.7
```

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        Lockout
                       Aging      Expiry 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.

5

ACL Commands

mac access-list

The **mac access-list** Global Configuration mode command 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*

- *name*—Specifies the name of the ACL.

Default Configuration

The default for all ACLs is permit all.

Command Mode

Global Configuration mode

User Guidelines

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-1
Console(config-mac-al)#
```

deny (MAC)

The **deny** MAC-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

Syntax

deny *destination*

- destination — Specifies the MAC address of the host to which the packet is being sent.

Default Configuration

This command has no default configuration.

Command Mode

MAC-Access List Configuration mode

User Guidelines

- MAC BPDU packets cannot be denied.
- Each MAC address in the ACL is a ACE (Access Control Element) and can only be removed by deleting the ACL using the **no mac access-list** Global Configuration mode command or the Web-based interface.

Example

The following example shows how to create a MAC ACL with rules.

```
Console(config)# mac access-list macl-1
Console (config-mac-acl)# deny 66:66:66:66:66:66
Console(config-mac-acl)# exit
Console(config)#
```

service-acl

The **service-acl** Interface (VLAN) 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

- *acl-name*—Specifies the ACL to be applied to the input interface.

Default Configuration

This command has no default configuration.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example, binds (services) an ACL to VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# service-acl input macl-1
```

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*]

- *name* —Name of the ACL.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the access lists.

```
Console# show access-lists
MAC access list macl-1
deny host 66:66:66:66:66:66
```

show interfaces access-lists

The **show interfaces access-lists** Privileged EXEC mode command displays access lists applied on interfaces.

Syntax

show interfaces access-lists [**vlan** *vlan-id*]

- *vlan-id*—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.

Examples

The following example displays an ACLs applied on the device interfaces:

```
Console# show interfaces access-lists

Interface     Input ACL
---------     ----------
VLAN 2        ACL1
VLAN 10       ACL3
```

6

Address Table Commands

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*]

- *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 Configuration

No static addresses are defined. The default mode for an added address is **permanent**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- 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
```

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 Configuration

Filtering multicast addresses is disabled. All multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

User Guidelines

- If multicast routers exist on the VLAN, do not change the unregistered multicast addresses state to drop on the switch ports.
- If multicast routers exist on the VLAN and IGMP-snooping is not enabled, use the **bridge multicast forward-all** command to enable forwarding all multicast packets to the multicast switches.

Example

In this example, bridge multicast filtering is enabled.

```
Console(config)# 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* | *ip-multicast-address*}

bridge multicast address {*mac-multicast-address* | *ip-multicast-address*} [**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}

- **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.
- *ip- multicast-address* — A valid IP multicast address.
- *interface-list* — Separate non-consecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate non-consecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of ports.

Default Configuration

No multicast addresses are defined.

Command Mode

Interface configuration (VLAN) mode

User Guidelines

- 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
```

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* | *ip-multicast-address*}

- **add** — Adds ports to the group.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — A valid MAC multicast address.
- *ip- multicast-address* — A valid IP multicast address.
- *interface-list* — Separate non-consecutive Ethernet ports with a comma and no spaces; hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate non-consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

No forbidden addresses are defined.

Command Modes

Interface Configuration (VLAN) mode

User Guidelines

- 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
```

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

- **add** — Force forwarding all multicast packets.
- **remove** — Do not force forwarding all multicast packets.
- *interface-list* — Separate non-consecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate non-consecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

This setting is disabled

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

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
```

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

- **add** — Forbids forwarding all multicast packets.
- **remove** — Does not forbid forwarding all multicast packets.
- *interface-list* — Separates non-consecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separates non-consecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

This setting is disabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- IGMP snooping dynamically discovers multicast router ports. When a multicast router port is discovered, all the multicast packets are forwarded to it unconditionally.
- This command prevents a port from becoming a multicast router 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
```

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

- *seconds* — Time in seconds. (Range: 10-3825 seconds)

Default Configuration

The default setting is 300 seconds.

Command Mode

Global Configuration mode

User Guidelines

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
```

clear bridge

The **clear bridge** Privileged EXEC mode command removes any learned entries from the forwarding database.

Syntax

clear bridge

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, the bridge tables are cleared.

```
Console# clear bridge
```

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

- **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 Configuration

This setting is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command. 802.1x multiple host mode must be enabled.

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
```

port security mode

The **port security mode** Interface Configuration mode command configures the port security mode. To return to the default configuration, use the **no** form of this command.

Syntax

port security mode {**lock** | **max-addresses**}

no port security mode

- **lock** — Saves the current dynamic MAC addresses associated with the port and disables learning, relearning and aging.
- **max-addresses** — Deletes the current dynamic MAC addresses associated with the port. Learns up to the maximum addresses allowed on the port. Relearning and aging are enabled.

Default Configuration

This setting is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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 mode dynamic
```

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

- *max-addr*— Maximum number of addresses that can be learned by the port. (Range: 1-128)

Default Configuration

The default setting is 1 address.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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
```

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*

- *mac-address* — A valid MAC address.

Default Configuration

No addresses are defined.

Command Mode

Interface configuration (Ethernet, port-channel) mode; cannot be configured for a range of interfaces (range context).

User Guidelines

- 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
```

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*]

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- 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
```

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*]

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel 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

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
```

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*]

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel 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

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
```

show bridge multicast address-table

The **show bridge multicast address-table** Privileged 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**]

- *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. Can be **ip** or **mac**. If the format is unspecified, the default is **mac**.

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 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

Vlan      MAC Address           Type           Ports
----      --------------        -------        ----------
1         01:00:5e:02:02:03     static         1/e1, 2/e2
19        01:00:5e:02:02:08     static         1/e1-e8
19        00:00:5e:02:02:08     dynamic        1/e9-e11

Forbidden ports for multicast addresses:

Vlan      MAC Address           Ports
----      --------------        -----
1         01:00:5e:02:02:03     2/e8
19        01:00:5e:02:02:08     2/e8

Console# show bridge multicast address-table format ip

Vlan      IP/MAC Address        Type           Ports
----      -----------------     ------         ---------
1         224-239.130|2.2.3     static         1/e1,2/e2
19        224-239.130|2.2.8     static         1/e1-8
19        224-239.130|2.2.8     dynamic        1/e9-11

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.

show bridge multicast filtering

The **show bridge multicast filtering** Privileged EXEC mode command displays the multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

- *vlan-id* — VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

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)
```

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*]

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel 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

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

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*]

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel 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

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
```

7

Clock

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*

- *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 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 sets the system time to 13:32:00 on the 7th March 2002.

```
Console# clock set 13:32:00 7 Mar 2002
```

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

- **sntp** — SNTP servers

Default Configuration

No external clock source

Command Mode

Global Configuration mode

User Guidelines

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
```

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

- *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 Configuration

Clock set to UTC.

Command Mode

Global Configuration mode

User Guidelines

- The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Examples

The following example sets the timezone to 6 hours difference from UTC.

```
Console(config)# clock timezone -6 zone CST
```

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

- **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 Configuration

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

User Guidelines

- 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 saving time:
  - Start: First Sunday in April
  - End: Last Sunday in October
  - Time: 2 am local time
- EU rule for daylight saving time:
  - Start: Last Sunday in March
  - End: Last Sunday in October
  - Time: 1.00 am (01:00)

Examples

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
```

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*

- *number* — Key number (Range: 1-4294967295)
- *value* — Key value (Range: 1-8 characters)

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

User Guidelines

- Multiple keys can be generated.

Examples

The following example defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
```

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 Configuration

No authentication

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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*

- *key-number* — Key number of authentication key to be trusted. (Range: 1 - 4294967295)

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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

- *seconds* — Polling interval in seconds (Range: 60-86400)

Default Configuration

Polling interval is 1024 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

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
```

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 Configuration

The SNTP broadcast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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 Configuration

The SNTP anycast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

- Polling time is determined by the **sntp client poll timer** Global Configuration mode command.
- Use the **sntp client enable (Interface)** Interface Configuration mode command to enable the SNTP client on a specific interface.

Examples

The following example enables SNTP anycast clients.

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

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 Configuration

The SNTP client is disabled on an interface.

Command Mode

Interface configuration (Ethernet, port-channel, VLAN) mode

User Guidelines

- 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
```

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 Configuration

The SNTP unicast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

- Use the **sntp server** Global Configuration mode command to define SNTP servers.

Examples

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
```

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 Configuration

Polling is disabled.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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 {*ip address* | *hostname*}

- *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 Configuration

No servers are defined.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

show clock

The **show clock** User EXEC mode command displays the time and date from the system clock.

Syntax

show clock [detail]

- **detail** — Shows timezone and summertime configuration.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

- 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.
```

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 Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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
```

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 Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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
176.1.8.179  Unknown    12:17.17.987 PDT Feb 19 2002       8.98     189.19

Anycast server:
Server       Interface  Status  Last response              Offset   Delay
                                                           [mSec]   [mSec]
---------    -------    -----   ---------------------------  ------   -----
176.1.11.8   VLAN 118   Up      9:53:21.789 PDT Feb 19 2002  7.19     119.89

Broadcast:
Interface    Interface         Last response
---------    ---------         ----------------------------
176.9.1.1    VLAN 119          19:17:59.792 PDT Feb 19 2002
```

8

Configuration and Image Files

copy

The **copy** Privileged EXEC mode command copies files from a source to a destination.

Syntax

copy *source-url destination-url*

- *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 is 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.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- 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 is not corrupt.

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]
```

delete

The **delete** Privileged EXEC mode command deletes a file from a flash memory device.

Syntax

delete *url*

- *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 is the default in case a URL is specified without a prefix.
startup-config	Represents the startup configuration file.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- *.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]
```

delete startup-config

The **delete startup-config** Privileged EXEC mode command deletes the startup-config file.

Syntax

delete startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example deletes the startup-config file.

```
Console# delete startup-config
```

dir

The **dir** Privileged EXEC mode command displays a 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.

Examples

The following example displays files in the flash directory.

```
Console# dir

Directory of flash:

File Name       Permission  Size       Modification Date  Modification Time
---------       ----------  ----       -----------------  -----------------
Image-1         rw          4325376    01-Jun-2003        01:04:21
Image-2         rw          4325376    01-Jun-2003        21:28:10
aaafile.prv     --          131072     01-Jun-2003        01:01:19
sshkeys.prv     --          262144     01-Jun-2003        01:01:05
syslog1.sys     r-          262144     01-Jun-2003        02:22:48
syslog2.sys     r-          262144     01-Jun-2003        02:22:48
directry.prv    --          262144     01-Jun-2003        01:01:02
startup-config  rw          1523       08-Feb-2005        09:02:31


Total size of flash: 15597568 bytes
Free size of flash: 5759287 bytes
```

more

The **more** Privileged EXEC mode command displays a file.

Syntax

more *url*

- *url* — The location URL or reserved keyword of the file to be displayed. (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 is 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 image files, which are displayed in hexadecimal format.
- *.prv and *.sys files cannot be displayed.

Example

The following example displays the contents of file **configuration.bak**.

```
Console# more configuration.bak
interface range ethernet 1/e(1-4)
duplex half
exit
interface range ethernet 2/g(1-4)
switchport mode general
exit
vlan database
vlan 2
exit
interface range ethernet 2/g(1-4)
switchport general allowed vlan add 2
exit
interface range ethernet 1/e(1-4)
no negotiation
exit
```

rename

The **rename** Privileged EXEC mode command renames a file.

Syntax

rename *url new-url*

- *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 is 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.

Examples

The following example renames the configuration backup 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**}

- *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 Configuration

If the unit number is unspecified, the default setting is the master unit number.

Command Mode

Privileged EXEC mode

User Guidelines

- Use the **show bootvar** command to find out which image is the active image.

Examples

The following example loads system image 1 at device startup.

```
Console# boot system image-1
```

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 Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- This command displays the factory default settings at the end of the running configuration file contents.

Examples

The following example displays the contents of the running configuration file.

```
Device# 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
```

show startup-config

The **show startup-config** Privileged EXEC mode command displays the contents of the startup configuration file.

Syntax

show startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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
```

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*]

- *unit* — Specifies the unit number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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
```

9

DHCP Filtering

ip dhcp filtering vlan

Use the **ip dhcp filtering vlan** global configuration command to enable filtering of DHCP requests on a VLAN. Use the **no** form of this command to disable DHCP requests filtering on a VLAN .

Syntax

ip dhcp filtering vlan *vlan-id*

no ip dhcp filtering vlan *vlan-id*

- *vlan-id* — Specify VLAN ID.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

- Use this command to limit flooding of DHCP requests to trusted ports only.
- Use the **ip dhcp filtering trust** interface configuration command to define trusted ports.

Examples

The following example enables filtering of DHCP requests on a VLAN.

```
console(config)# ip dhcp filtering vlan 3
```

ip dhcp filtering trust

Use the **ip dhcp filtering trust** interface configuration command to configure a port as trusted for DHCP filtering purposes. Use the **no** form of this command to return to the default setting.

Syntax

ip dhcp filtering trust

no ip dhcp filtering trust

Default Configuration

The interface is untrusted.

Command Mode

Interface configuration (Ethernet, Port-channel)

User Guidelines

- Configure as “trusted”, ports that are connected to a DHCP server or to other switches or routers.
- Configure as “untrusted”, ports that are connected to DHCP clients.
- The software would flood DHCP requests to trusted ports only.

Example

The following example configures a port as trusted for DHCP filtering purposes.

```
console (config)# interface 1/e7
console (config-if)# ip dhcp filtering trust
```

show ip dhcp filtering

Use the **show ip dhcp filtering** EXEC command to display the DHCP filtering configuration.

Syntax

show ip dhcp filtering [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface* —Specify Ethernet port.
- *port-channel-number* —Specify Port-channel number.

Default Configuration

The interface is untrusted.

Command Mode

EXEC

User Guidelines

There are no user guidelines for this command .

Example

The following example displays the DHCP filtering configuration.

```
Console# show ip dhcp filtering


DHCP filtering is configured on following VLANs: 2,3



Interface Trusted
----------- ------------
1/e1 yes
1/e2 yes
```

10

Ethernet Configuration Commands

interface ethernet

The **interface ethernet** Global Configuration mode command enters the interface configuration mode to configure an Ethernet type interface.

Syntax

interface ethernet *interface*

- *interface* — Valid Ethernet port. (Full syntax: *unit*/*port*)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables configuring Ethernet port 5/e18.

```
Console(config)# interface ethernet 5/e18
```

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**}

- *port-range* — List of valid ports. Where more than one port is listed, separate non-consecutive ports with a comma and no spaces, use a hyphen to designate a range of ports.
- **all** — All Ethernet ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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)#
```

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 Configuration

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Examples

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
```

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

- *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 Configuration

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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"
```

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

- **10** — Forces 10 Mbps operation.
- **100** — Forces 100 Mbps operation.
- **1000** — Forces 1000 Mbps operation.

Default Configuration

Maximum port capability

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- 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
```

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**}

no duplex

- **half** — Forces half-duplex operation
- **full** — Forces full-duplex operation

Default Configuration

The interface is set to full duplex.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- 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
```

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

- *capability* — Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h,100f, 1000f)

Default Configuration

Auto-negotiation is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- If unspecified, the default setting is to enable all capabilities of the port.

Example

The following example enables auto-negotiation on Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# negotiation
```

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

- **auto** — Indicates auto-negotiation
- **on** — Enables flow control.
- **off** — Disables flow control.

Default Configuration

Flow control is off.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- Negotiation should be enabled for **flow control auto**.

Example

In the following example, flow control is enabled on port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# flowcontrol on
```

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

- **on** — Manual mdix
- **auto** — Automatic mdi/mdix

Default Configuration

The default setting is **on**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- **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
```

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 Configuration

Back pressure is enabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- Back pressure cannot be configured on trunks.

Example

In the following example back pressure is enabled on port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# back-pressure
```

clear counters

The **clear counters** User EXEC mode command clears statistics on an interface.

Syntax

clear counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface* — Valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — Valid 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

In the following example, the counters for interface 1/e1 are cleared.

```
Console> clear counters ethernet 1/e1
```

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*}

- *interface* — Valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- 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
```

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*]

- *interface* — Valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

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
----    -----------   -------     ------------------------------
1/e1    100M-Copper   Enabled     --
1/e2    100M-Copper   Enabled     --
1/e3    100M-Copper   Enabled     --
1/e4    100M-Copper   Enabled     --
1/e5    100M-Copper   Enabled     100f, 100h, 10f, 10h
1/e6    100M-Copper   Enabled     --
1/e7    100M-Copper   Enabled     --
1/e8    100M-Copper   Enabled     --
1/e9    100M-Copper   Enabled     --
1/e10   100M-Copper   Enabled     --
1/e11   100M-Copper   Enabled     --
1/e12   100M-Copper   Enabled     --
1/e13   100M-Copper   Enabled     --
1/e14   100M-Copper   Enabled     --
1/e15   100M-Copper   Enabled     --
1/e16   100M-Copper   Enabled     --
1/e17   100M-Copper   Enabled     --
1/e18   100M-Copper   Enabled     --
1/e19   100M-Copper   Enabled     --
1/e20   100M-Copper   Enabled     --
```

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* — Valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

- To view information on autonegotiation capabilities, use the **show interfaces advertise** Privileged EXEC mode command.

Example

The following example displays the configuration of all configured interfaces:

```
Console# show interfaces configuration

Port   Type          Duplex  Speed  Neg      Flow  Link   Back      Mdix
                                             Ctrl  State  Pressure  Mode
----   -----------   ------  -----  -------  ----  -----  --------  ----
1/e1   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e2   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e3   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e4   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e5   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e6   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e7   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e8   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e9   100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e10  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
```

```
1/e11  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e12  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e13  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e14  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e15  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e16  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e17  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e18  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
1/e19  100M-Copper   Full    100    Enabled  Off   Up     Disabled  Auto
```

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*]

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel 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 displays the status of all configured interfaces:

```
Console# show interfaces status

Port   Type          Duplex  Speed  Neg      Flow  Link   Back      Mdix
                                             Ctrl  State  Pressure  Mode
----   -----------   ------  -----  -------  ----  -----  --------  ----
1/e1   100M-Copper   --      --     --       --    Down   --        --
1/e2   100M-Copper   --      --     --       --    Down   --        --
1/e3   100M-Copper   --      --     --       --    Down   --        --
1/e4   100M-Copper   --      --     --       --    Down   --        --
1/e5   100M-Copper   Full    100    Enabled  Off   Up     Disabled  On
1/e6   100M-Copper   --      --     --       --    Down   --        --
1/e7   100M-Copper   --      --     --       --    Down   --        --
1/e8   100M-Copper   --      --     --       --    Down   --        --
1/e9   100M-Copper   --      --     --       --    Down   --        --
1/e10  100M-Copper   --      --     --       --    Down   --        --
1/e11  100M-Copper   --      --     --       --    Down   --        --
1/e12  100M-Copper   --      --     --       --    Down   --        --
1/e13  100M-Copper   --      --     --       --    Down   --        --
1/e14  100M-Copper   --      --     --       --    Down   --        --
1/e15  100M-Copper   --      --     --       --    Down   --        --
1/e16  100M-Copper   --      --     --       --    Down   --        --
1/e17  100M-Copper   --      --     --       --    Down   --        --
1/e18  100M-Copper   --      --     --       --    Down   --        --
1/e19  100M-Copper   --      --     --       --    Down   --        --
```

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*]

- *interface* — Valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

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
```

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*]

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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.

port storm-control include-multicast

The **port storm-control include-multicast** Interface Configuration (Ethernet) mode command counts multicast packets in broadcast storm control. To disable counting multicast packets, use the **no** form of this command.

Syntax

port storm-control include-multicast [unknown-unicast]

no port storm-control include-multicast

- **unknown-unicast** — Specifies also counting unknown unicast packets.

Default Configuration

Multicast packets are not counted.

Command Modes

Interface Configuration (Ethernet) mode

User Guidelines

- To control multicasts storms, use the **port storm-control broadcast enable** and **port storm-control broadcast rate** commands.

Example

The following example enables counting broadcast and multicast packets on Ethernet port 2/e3.

```
Console(config)# interface ethernet 2/e3
Console(config-if)# port storm-control include-multicast
```

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 Configuration

Broadcast storm control is disabled.

Command Modes

Interface Configuration (Ethernet) mode

User Guidelines

- Use the **port storm-control broadcast rate** Interface Configuration (Ethernet) mode command, to set the maximum allowable broadcast rate.
- Use the **port storm-control include-multicast** Interface Configuration (Ethernet) mode command to count multicast packets and optionally unknown unicast packets in the storm control calculation.

Example

The following example enables storm control on Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# port storm-control broadcast enable
```

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

- *rate* — Maximum kilobits per second of broadcast, multicast, and unknown unicast traffic on a port. (Range: 70-250,000 Kbits/Sec, where the following granularity is applied:
  - 70K - 1M in steps of at least 10K
  - 1M-10M in steps of at least 1M
  - 10M-250M in steps based on the requested rate)

Default Configuration

The default storm control broadcast rate is 100 Kbits/Sec.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- Use the **port storm-control broadcast enable** Interface Configuration mode command to enable broadcast storm control.
- Since granularity depends on the requested rate, the software displays the actual rate.

Example

The following example configures the maximum storm control broadcast rate at 900 Kbits/Sec on Ethernet port 1/e5.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# port storm-control broadcast rate 900
```

show ports storm-control

The **show ports storm-control** Privileged EXEC mode command displays the storm control configuration.

Syntax

show ports storm-control [*interface*]

- *interface* — A valid Ethernet port. (Full syntax: *unit*/*port*)

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

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       Included
                   [Kbits/
                   Sec]
----     --------  ---------  ------------------------------.
1/e1     Enabled   70         Broadcast, Multicast, Unknown
                              Unicast
2/e1     Enabled   100        Broadcast
3/e1     Disabled  100        Broadcast
```

11

GVRP Commands

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 Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables GVRP globally on the device.

```
Console(config)# gvrp enable
```

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 Configuration

GVRP is disabled on all interfaces.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- 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
```

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

- {**join** | **leave** | **leaveall**} — Indicates the type of timer.
- *timer_value* — Timer values in milliseconds in multiples of 10. (Range: 10-2147483647)

Default Configuration

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

User Guidelines

- The following relationship must be maintained between the timers:
  - 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 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
```

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 Configuration

Dynamic VLAN creation or modification is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- 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
```

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 Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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
```

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*]

- *interface* — A valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — A valid port-channel 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 clears all GVRP statistical information on Ethernet port 1/e6.

```
console# clear gvrp statistics ethernet 1/e6
```

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*]

- *interface* — A valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — A valid 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 example displays GVRP configuration information:

```
Console> show gvrp configuration

GVRP Feature is currently enabled on the device.

                                                    Timers (milliseconds)
Port(s)  Status   Registration   Dynamic VLAN    Join   Leave   Leave All
                                Creation
------   -------  ------------   -----------     ----   -----   ---------
2/e1     Enabled  Normal         Enabled         200    600     10000
4/e4     Enabled  Normal         Enabled         200    600     10000
```

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*]

- *interface* — A valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — A valid 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 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
```

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*]

- *interface* — A valid Ethernet port. (Full syntax: *unit*/*port*)
- *port-channel-number* — A valid 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 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 Type       INVEVENT:  Invalid Event
INVAVAL :  Invalid Attribute Value
 Port  INVPROT  INVATYP  INVAVAL  INVALEN  INVEVENT
```

12

IGMP Snooping Commands

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 Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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 Configuration

IGMP snooping is disabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- 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
```

ip igmp snooping mrouter learn-pim-dvmrp

The **ip igmp snooping mrouter learn-pim-dvmrp** Interface Configuration (VLAN) mode command enables automatic learning of multicast router ports in the context of a specific VLAN. To remove automatic learning of multicast router ports, use the **no** form of this command.

Syntax

ip igmp snooping mrouter learn-pim-dvmrp

no ip igmp snooping mrouter learn-pim-dvmrp

Default Configuration

Automatic learning of multicast router ports is enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- Multicast router ports can be configured statically using the **bridge multicast forward-all** Interface Configuration (VLAN) mode command.

Example

The following example enables automatic learning of multicast router ports on VLAN 2.

```
Console(config) # interface vlan 2
Console(config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```

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*

no ip igmp snooping host-time-out

- *time-out* — Host timeout in seconds. (Range: 1 - 2147483647)

Default Configuration

The default host-time-out is 260 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The timeout should be at least greater than 2*query_interval+max_response_time of the IGMP router.

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
```

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 router 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

- *time-out* — Multicast router timeout in seconds (Range: 1 - 2147483647)

Default Configuration

The default value is 300 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the multicast router timeout to 200 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping mrouter-time-out 200
```

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

- *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 Configuration

The default leave-time-out configuration is 10 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- 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
```

show ip igmp snooping mrouter

The **show ip igmp snooping mrouter** User EXEC mode command displays information on dynamically learned multicast router interfaces.

Syntax

show ip igmp snooping mrouter [**interface** *vlan-id*]

- *vlan-id* — VLAN 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 example displays multicast router interfaces in VLAN 1000.

```
Console> show ip igmp snooping mrouter interface 1000

VLAN            Ports
----            -----
1000            1/e1

Detected multicast routers that are forbidden statically:
VLAN            Ports
----            -----
1000            1/e19
```

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*

- *vlan-id* — VLAN 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 example displays IGMP snooping information on VLAN 1000.

```
Console> show ip igmp snooping interface 1000
IGMP Snooping is globaly enabled
IGMP Snooping is enabled on VLAN 1000
IGMP host timeout is 300 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 200 sec
Automatic learning of multicast router ports is enabled
```

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*]

- *vlan-id* — VLAN number.
- *ip-multicast-address* — IP multicast address.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

- 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         IP Address           Querier        Ports
----         ------------------   --------       ------------
1            224-239.130|2.2.3    Yes            1/e1, 2/e2
19           224-239.130|2.2.8    Yes            1/e9-e11

IGMP Reporters that are forbidden statically:
-------------------------------------------
Vlan         IP Address           Ports
----         ------------------   ------------
1            224-239.130|2.2.3    1/e19
```

13

IP Addressing Commands

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*]

- *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 Configuration

No IP address is defined for interfaces.

Command Mode

Interface Configuration (Ethernet, VLAN, port-channel) mode

User Guidelines

- 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
```

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

- *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 Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, VLAN, port-channel) mode

User Guidelines

- 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
```

ip default-gateway

The **ip default-gateway** Global Configuration mode command defines a default gateway (router). To return to the default configuration, use the **no** form of this command.

Syntax

ip default-gateway *ip-address*

no ip default-gateway

- *ip-address* — Valid IP address of the default gateway.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

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
```

show ip interface

The **show ip interface** User 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.*]

- *interface-number* — Valid Ethernet port.
- *vlan-id* — Valid VLAN number.
- *port-channel number.* — Valid 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 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
```

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.*}

- *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 Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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

- *seconds* — Time (in seconds) that an entry remains in the ARP cache. (Range: 1 - 40000000)

Default Configuration

The default timeout is 60000 seconds.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

clear arp-cache

The **clear arp-cache** Privileged EXEC mode command deletes all dynamic entries from the ARP cache.

Syntax

clear arp-cache

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 deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

show arp

The **show arp** Privileged EXEC mode command displays entries in the ARP table.

Syntax

show arp

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 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
```

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 Configuration

IP Domain Naming System (DNS)-based host name-to-address translation is enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables IP Domain Naming System (DNS)-based host name-to-address translation.

```
Console(config)# ip domain-lookup
```

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

- *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 Configuration

A default domain name is not defined.

Command Mode

Global Configuration mode

User Guidelines

- This command enables host name-to-address translation. The preference in name-to-address resolution is determined by the type of host name-to-address entry. Static entries are read first, followed by DHCP entries and DNS-protocol entries.

Examples

The following example defines default domain name dell.com.

```
Console(config)# ip domain-name dell.com
```

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*]

- *server-address* — Specifies IP addresses of the name server.

Default Configuration

No name server addresses are specified.

Command Mode

Global Configuration mode

User Guidelines

- 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.

Examples

The following example sets the available name server.

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

ip host

The **ip host** Global Configuration mode command defines static host name-to-address mapping in the host cache. To remove the host name-to-address mapping, use the **no** form of this command.

Syntax

ip host *name address*

no ip host *name*

- *name* — Name of the host (Range: 1-158 characters)
- *address* — Associated IP address.

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

- Up to 64 host name-to address mapping entries are permitted in the host cache.

Examples

The following example defines a static host name-to-address mapping in the host cache.

```
Console(config)# ip host accounting.dell.com 176.10.23.1
```

clear host

The **clear host** Privileged EXEC mode command deletes entries from the host name-to-address cache.

Syntax

clear host {*name* | *}

- *name* — Specifies the host entry to be removed. (Range: 1-158 characters)
- * — Removes all entries.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example deletes all entries from the host name-to-address cache.

```
Console# clear 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* | *}

- *name* — Specifies the host entry to be removed. (Range: 1-158 characters)
- * — Removes all entries.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- This command deletes the host name-to-address mapping temporarily until the next renewal of the IP address.

Examples

The following example deletes all entries from the host name-to-address mapping.

```
Console# clear host dhcp *
```

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*]

- *name* — Specifies the host name. (Range: 1-158 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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
```

14

LACP Commands

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

- *value* — Specifies system priority value. (Range: 1 - 65535)

Default Configuration

The default system priority is 1.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the system priority to 120.

```
Console(config)# lacp system-priority 120
```

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

- *value* — Specifies port priority. (Range: 1 - 65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

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
```

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

- **long** — Specifies the long timeout value.
- **short** — Specifies the short timeout value.

Default Configuration

The default port timeout value is **long**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

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
```

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**]

- *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 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 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
```

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*]

- *port_channel_number* — Valid port-channel 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 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
```

15

Line Commands

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**}

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the device as a virtual terminal for remote console access.

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

- *bps*—Baud rate in bits per second (bps). Possible values are 2400, 9600, 19200, 38400, 57600 and 115200.

Default Configuration

The default speed is 9600 bps.

Command Mode

Line Configuration (console) mode

User Guidelines

- 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
```

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 Configuration

Autobaud is disabled.

Command Mode

Line Configuration (console) mode

User Guidelines

- 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.

Examples

The following example enables autobaud.

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

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

- *minutes* — Specifies the number of minutes. (Range: 0 - 65535)
- *seconds* — Specifies additional time intervals in seconds. (Range: 0 - 59)

Default Configuration

The default configuration is 10 minutes.

Command Mode

Line Configuration mode

User Guidelines

- To specify no timeout, enter the **exec-timeout** 0 command.

Examples

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
```

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 Configuration

The command history function is enabled.

Command Mode

Line Configuration mode

User Guidelines

- 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
```

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

- *number-of-commands*—Number of commands that the system records in its history buffer. (Range: 10 - 216)

Default Configuration

The default history buffer size is 10.

Command Mode

Line Configuration mode

User Guidelines

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
```

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

no terminal history

Default Configuration

The default configuration for all terminal sessions is defined by the **history** line configuration command.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example disables the command history function for the current terminal session.

```
Console# no terminal history
```

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*

no terminal history size

- *number-of-commands*—Specifies the number of commands the system may record in its command history buffer. (Range: 10-216)

Default Configuration

The default command history buffer size is 10.

Command Mode

User EXEC mode

User Guidelines

- 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.
- The maximum number of commands in all buffers is 256.

Examples

The following example configures the command history buffer size to 20 commands for the current terminal session.

```
Console> terminal history size 20
```

show line

The **show line** User EXEC mode command displays line parameters.

Syntax

show line [**console** | **telnet** | **ssh**]

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Configuration

If the line is not specified, the default value is console.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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
```

16

LLDP Commands

lldp enable (global)

To **enable Link Layer Discovery Protocol (LLDP)**, use the **lldp enable** command in global configuration mode. To disable LLDP, use the **no** form of this command.

Syntax

lldp enable

no lldp enable

Default Configuration

The command is enabled.

Command Mode

Global configuration

User Guidlines

There are no guidelines for this command.

Example

The following example enables Link Layer Discovery Protocol (LLDP) .

```
console (config)# lldp enable
```

lldp enable (interface)

To enable Link Layer Discovery Protocol (LLDP) on an interface, use the **lldp enable** command in interface configuration mode. To disable LLDP on an interface, use the **no** form of this command.

Syntax

lldp enable [rx | tx | both]

no **lldp enable**

- *rx* — Receive only LLDP packets.
- *tx* —Transmit only LLDP packets.
- *both* — Receive and transmit LLDP packets (default)

Default Configuration

Enabled in both modes.

Command Modes

Interface configuration (Ethernet)

User Guidelines

- LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG. LLDP data received through LAG ports is stored individually per port.
- LLDP operation on a port is not dependent on STP state of a port. I.e. LLDP frames are sent and received on blocked ports. If a port is controlled by 802.1X, LLDP operates only if the port is authorized.

Examples

The following example enables Link Layer Discovery Protocol (LLDP) on an interface (g5).

```
Console(config)# interface ethernet 1/e5
Console(config-if)# lldp enable
```

lldp timer

To specify how often the software sends Link Layer Discovery Protocol (LLDP) updates, use the **lldp timer command** in global configuration mode. To revert to the default setting, use the **no** form of this command.

Syntax

lldp timer seconds

no **lldp timer**

- *seconds* — Specifies in seconds how often the software sends LLDP update. (Range: 5 - 32768 seconds).

Default Configuration

The default value is 30 seconds.

Command Modes

Global configuration

User Guidelines

There are no user guidelines for this command.

Examples

The following example specifies how often the software sends Link Layer Discovery Protocol (LLDP) updates.

```
Console (config) # lldp timer
```

lldp hold-multiplier

To specify the amount of time, the receiving device should hold a Link Layer Discovery Protocol (LLDP) packet before discarding it. Use the **lldp hold-multiplier** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

Syntax

lldp hold-multiplier number

no lldp hold-multiplier

- *number* — Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value (Range: 2-10).

Default Configuraiton

The default configuration is 4.

Command Modes

Global configuration

User Guidelines

- The actual time-to-live value used in LLDP frames can be expressed by the following formula: TTL = min(65535, LLDP-Timer * LLDP-HoldMultiplier). For example, if the value of LLDP timer is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header.

Examples

The following example specifies how often the software sends Link Layer Discovery Protocol (LLDP) updates.

```
Console (config) # lldp hold-multiplier 6
```

lldp reinit-delay

To specify the minimum time an LLDP port will wait before reinitializing LLDP transmission, use the **lldp reinit-delay** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

Syntax

lldp reinit-delay seconds

no lldp reinit-delay

- seconds — Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. (Range 1-10 seconds).

Default Configuraiton

The default value is 2 seconds.

Command Modes

Global configuration

User Guidelines

There are no user guidelines for this command.

Examples

The following example pecifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.

```
Console (config) # lldp reinit-delay 6
```

lldp tx-delay

To specify the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB, use the **lldp tx-delay** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

Syntax

lldp tx-delay seconds

no lldp tx-delay

Parameters

- *seconds* — Specifies the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Range 1-8192 second.

Default Configuration

The default value is 2 seconds.

Command Modes

Global configuration

Usage Guidelines

- It is recommended that the TxDelay would be less than 0.25 of the LLDP timer interval.

Examples

The following example specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.

```
Console (config) # lldp tx-delay 7
```

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. To revert to the default setting, use the **no** form of this command.

Syntax

lldp optional-tlv tlv1 [tlv2 … tlv5]

no **lldp optional-tlv**

- *tlv* — Specifies TLV that should be included. Available optional TLVs are: port-desc, sys-name, sys-desc and sys-cap . (Range 1-8192 seconds).

Default Configuration

No optional TLV is transmitted.

Command Modes

Interface configuration (Ethernet)

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies which optional TLV (2)s from the basic set should be transmitted.

```
Console(config)# interface ethernet g5
Console(config-if)# lldp optional-tlv sys-name
```

lldp management-address

To specify the management address that would be advertised from an interface, use the **lldp management-address** command in interface configuration mode. To stop advertising management address information, use the **no** form of this command.

Syntax

lldp management-address ip-address

no management-address ip

- *ip-address* — Specifies the management address to advertise.

Default Configuration

No IP address is advertised.

Command Modes

Interface configuration (Ethernet)

User Guidelines

- Each port can advertise one IP address.
- Only static IP addresses can be advertised.

Example

The following example specifies management address that would be advertised from an interface.

```
Console(config)# interface ethernet g5
Console(config-if)# lldp management-address 192.168.0.1
```

clear lldp rx

To restart the LLDP RX state machine and clearing the neighbors table, use the **clear lldp rx** command in privileged EXEC mode.

Syntax

clear lldp rx [ethernet interface]

- *Interface* — Ethernet port

Command Modes

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

The folowing example restarts the LLDP RX state machine and clearing the neighbors table.

```
console (config)#clear lldp rx
```

show lldp configuration

To display the Link Layer Discovery Protocol (LLDP) configuration, use the **show lldp configuration** command in privileged EXEC mode.

Syntax

show lldp configuration [ethernet interface]

- *Interface* — Ethernet port

Command Modes

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the Link Layer Discovery Protocol (LLDP) configuration.

```
Switch# show lldp configuration


Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds


Port     State      Optional TLVs      Addres
1/e1     RX, TX     PD, SN, SD, SC     172.16.1.1
1/e2     TX         PD, SN             172.16.1.1
1/e3     Disabled
```

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.

Syntax

show lldp local ethernet interface

- *Interface* — Ethernet port

Command Modes

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port.

```
Switch# show lldp local ethernet g1
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
```

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.

Syntax

show lldp neighbors [ethernet interface]

- *Interface* — Ethernet port

Command Modes

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP).

```
Switch# show lldp neighbors
```

Port	Device ID	Port ID	Hold Time	Capabilities	System Name
g1	0060.704C.73FE	1	117	B	ts-7800-2
g1	0060.704C.73FD	1	93	B	ts-7800-2
g2	0060.704C.73F C	9	1	B, R	ts-7900-1
g3	0060.704C.73FB	1	92	W	ts-7900-2

```
Switch# show lldp neighbors ethernet g1
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
```

17

Management ACL

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*

- *name* — Access list name. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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 re-enter 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 channel with an IP address or console interface. Management ACL only restricts access to the device for management configuration or viewing.

Examples

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
```

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*]

- *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 Configuration

If no permit rule is defined, the default is set to deny.

Command Mode

Management Access-list Configuration mode

User Guidelines

- 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
```

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*]

- *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 Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

- 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
```

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

- *name* — Specifies the name of the access list to be used. (Range: 1-32 characters)
- **console-only** — Indicates that the device can be managed only from the console.

Default Configuration

If no access list is specified, an empty access list is used.

Command Mode

Global Configuration mode

User Guidelines

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
```

show management access-list

The **show management access-list** Privileged EXEC mode command displays management access-lists.

Syntax

show management access-list [*name*]

- *name* — Specifies the name of a management access list. (Range: 1 - 32 characters)

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 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)
```

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 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 information about the active management access list.

```
Console# show management access-class
Management access-class is enabled, using access list mlist
```

18

PHY Diagnostics Commands

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*

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- 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.

Examples

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
```

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.

show copper-ports tdr [*interface*]

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

- 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           -                  -
```

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*]

- *interface* — A valid Ethernet port. (Full syntax: *unit/port*)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

- 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
```

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**]

Syntax Description

- *interface* — A valid Ethernet port. (Full syntax: *unit*/*port*)
- **detailed** — Detailed diagnostics.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

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    Voltage  Current  Output  Input   TX Fault  LOS
        [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
```

19

Port Channel Commands

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*

- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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**}

- *port-channel-range* — List of valid port-channels to add. Separate non-consecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels.
- **all** — All valid port-channels.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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

- *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 Configuration

The port is not assigned to a port-channel.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

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
```

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*]

- *port-channel-number* — Valid 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 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
```

20

Port Monitor Commands

port monitor

The **port monitor** Interface Configuration Ethernet 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*

- *src-interface*—Valid Ethernet port. (Full syntax: *unit/port*)
- **rx**—Monitors received packets only.
- **tx**—Monitors transmitted packets only.

Default Configuration

Monitors both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- 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.
- Up to 8 source ports can be configured.

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
```

port monitor vlan-tagging

The **port monitor vlan-tagging** Interface Configuration (Ethernet) mode command transmits tagged ingress mirrored packets. To transmit untagged ingress mirrored packets, use the **no** form of this command.

Syntax

port monitor vlan-tagging

no port monitor vlan-tagging

Default Configuration

Ingress mirrored packets are transmitted untagged.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures all ingress mirrored packets from port 1/e9 to be transmitted as tagged packets.

```
Console (config)# interface ethernet 1/e9
Console (config-if)# port monitor vlan-tagging
```

show ports monitor

The **show ports monitor** User EXEC mode command displays the port monitoring status.

Syntax

show ports monitor

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 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
```

21

Power over Ethernet Commands

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}

- **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 Configuration

The device discovery protocol is enabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

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
```

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

- *pd-type*—Specifies the type of powered device attached to the interface. (Range: 1-24 characters)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

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
```

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

- **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 Configuration

The default setting is low priority.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- An unlimited number of ports can be configured as critical, high or low.
- As power becomes unavailable, critical and high ports continue to receive power at the expense of low ports.

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
```

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

- *percentage*—Specifies the threshold as a percentage to compare measured power. (Range: 1-99)

Default Configuration

The default threshold is 95 percent.

Command Mode

Global Configuration mode

User Guidelines

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
```

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 Configuration

Inline power traps are disabled

Command Mode

Global Configuration mode

User Guidelines

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
```

show power inline

The **show power inline** User EXEC mode command displays the information about inline power.

Syntax

show power inline [**ethernet** *interface*]

- *interface* — Valid Ethernet port. (Full syntax: *unit*/*port*)

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 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 A  Auto   High      On     0.44 - 12.95
2/e1   Wireless AP Model Auto   Low       On     0.44 - 3.84
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 A  Auto   High      On     0.44 - 12.95

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.

22

QoS Commands

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

no qos

Default Configuration

QoS is disabled on the device.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables QoS on the device.

```
Console(config)# qos
```

show qos

The **show qos** User EXEC mode command displays quality of service (QoS) for the device.

Syntax

show qos

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 example displays QoS attributes when QoS is disabled on the device.

```
Console> show qos
Qos: disable
Trust: dscp
```

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

- *number-of-queues* — Specifies the number of expedite queues. The expedite queues would be the queues with higher indexes. (Range: 0 or 4)

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

- When the specified number of expedite queues is 0, the Strict Priority scheduling method is used.
- When the specified number of expedite queues is 4, weights are defined as 1, 2, 4 and 8.
- Port priority queues are used for internal purposes, such as stacking.

Example

The following example configures the number of expedite queues as 0.

```
Console(config)# priority-queue out num-of-queues 0
```

show qos interface

The **show qos interface** User EXEC mode command displays interface QoS information.

Syntax

show qos interface [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**queueing**]

- *interface-number* — Valid Ethernet port number.
- *vlan-id*— Valid VLAN ID.
- *number* — Valid port-channel number.
- **queuing** — Indicates the queue strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC mode

User Guidelines

- If no keyword is specified, port QoS information (e.g., DSCP trusted, CoS trusted, untrusted, etc.) is displayed.
- If no interface is specified, QoS information about all interfaces is displayed.

Examples

The following example displays QoS information about Ethernet port 1/e11.

```
Console> show qos interface ethernet 1/e11 queuing
Ethernet   1/e11
wrr bandwidth weights and EF priority:

qid        weights          Ef          Priority
1          25               dis         N/A
2          25               dis         N/A
3          25               dis         N/A
4          25               dis         N/A
```

```
Cos-queue map:
cos         qid
0           2
1           1
2           1
3           2
4           3
5           3
6           4
7           4
```

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*]

- *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 Configuration

Cos 0, 1, 2, and 3 are mapped to queue 1

Cos 4 and 5 are mapped to queue 2

Cos 6 and 7 are mapped to queue 3

Command Mode

Global Configuration mode

User Guidelines

- Queue 4 is reserved for stacking.

Example

The following example maps CoS 7 to queue 2.

```
Console(config)# wrr-queue cos-map 2 7
```

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

- *dscp-list* — Specifies up to 8 DSCP values separated by a space. (Range: 0 - 63)
- *queue-id* — Specifies the queue number to which the DSCP values are mapped.

Default Configuration

The following table describes the default map.

DSCP value	0-15	16-39	40-63
Queue-ID	1	2	3

Command Mode

Global Configuration mode

User Guidelines

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
```

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

- **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 Configuration

CoS is the default trust mode.

Command Mode

Global Configuration mode

User Guidelines

- 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.
- 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.

Example

The following example configures the system to the DSCP trust state.

```
Console(config)# qos trust dscp
```

qos trust (Interface)

The **qos trust** Interface Configuration (Ethernet, Port-channel) mode command enables each port trust state while the system is in the basic QoS mode. To disable the trust state on each port, use the **no** form of this command.

Syntax

qos trust

no qos trust

Default Configuration

qos trust is enabled on each port.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures Ethernet port 1/e15 to the default trust state.

```
console(config)# interface ethernet 1/e15
console(config-if) qos trust
```

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*

no qos cos

- *default-cos* — Specifies the default CoS value of the port. (Range: 0 - 7)

Default Configuration

Default CoS value of a port is 0.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

- 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
```

show qos map

The show qos map User EXEC mode command displays all QoS maps.

Syntax

show qos map [**dscp-queue**]

- **dscp-queue** — Indicates the DSCP to queue map.

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 example displays the DSCP port-queue map.

```
Console> show qos map

Dscp-queue map:
d1 : d2 0  1  2  3  4  5  6  7  8  9
-----------------------------------
0 :    01 01 01 01 01 01 01 01 01 01
1 :    01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 02 02 02 02 02 02 02
3 :    02 02 03 03 03 03 03 03 03 03
4 :    03 03 03 03 03 03 03 03 04 04
5 :    04 04 04 04 04 04 04 04 04 04
6 :    04 04 04 04
```

The following table describes the significant fields shown above.

Column	Description
d1	Decimal Bit 1 of DSCP
d2	Decimal Bit 2 of DSCP
01 - 04	Queue numbers

23

Radius Commands

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*}

- *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 key 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 Configuration

No RADIUS server host is specified.

The port number for authentication requests is 1812.

The usage type is **all**.

Command Mode

Global Configuration mode

User Guidelines

- 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.

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
```

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

- *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 key used on the RADIUS daemon. (Range: 0-128 characters)

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode

User Guidelines

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 dell-server
```

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

- *retries* — Specifies the retransmit value. (Range: 1 - 10)

Default Configuration

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

User Guidelines

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
```

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*

- *source* — Specifies a valid source IP address.

Default Configuration

The source IP address is the IP address of the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

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
```

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

- *timeout* — Specifies the timeout value in seconds. (Range: 1 - 30)

Default Configuration

The timeout value is 3 seconds.

Command Mode

Global Configuration mode

User Guidelines

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
```

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

- *deadtime* — Length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0 - 2000)

Default Configuration

The deadtime setting is 0.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the deadtime to 10 minutes.

```
Console(config)# radius-server deadtime 10
```

show radius-servers

The **show radius-servers** Privileged EXEC mode command displays the RADIUS server settings.

Syntax

show radius-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays RADIUS server settings.

```
Console# show radius-servers

IP          Port   TimeOut   Retransmit  DeadTime  Source    Priority  Usage
address     Auth                                   IP
---------   ----   -------   ----------  ------    --------  --------  -----
172.16.1.1  1645   Global    Global      Global    -         1         All
172.16.1.2  1645   11        8           Global    Global    2         All

Global values
-------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
```

24

RMON Commands

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*}

- *interface number* — Valid Ethernet port.
- *port-channel-number* — Valid 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 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 1518 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 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
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 1518 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 1518 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 1518 octets in length inclusive (excluding framing bits but including FCS octets).

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*

- *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 Configuration

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

User Guidelines

- 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
```

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*]

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)
- *port-channel-number* — Valid 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 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.

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*]

- *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 Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

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      Packets    Broadcast   Multicast   Util
----------   ---------   -------    ----------  ---------   -----
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
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
Sample Set: 1           Owner: Me
Interface: 1/e1         Interval: 1800
Requested samples: 50   Granted samples: 50

Maximum table size: 500

Time                    Dropped    Collisions
--------------------    --------   ----------
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 1518 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 1518 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 1518 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.

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 variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]

no rmon alarm *index*

- *index* — Specifies the alarm index. (Range: 1-65535)
- *variable* — Specifies the object identifier of the particular 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 Configuration

The type is **absolute**.

The startup direction is **rising-falling**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the following alarm conditions:

- Alarm index — 1000
- Variable identifier — dell
- 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 dell 360000 1000000 1000000 10 20
```

show rmon alarm-table

The **show rmon alarm-table** User EXEC mode command displays the alarms table.

Syntax

show rmon alarm-table

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 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.

show rmon alarm

The **show rmon alarm** User EXEC mode command displays alarm configuration.

Syntax

show rmon alarm *number*

- *number* — Specifies the alarm index. (Range: 1 - 65535)

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 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.

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*

- *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 Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

show rmon events

The **show rmon events** User EXEC mode command displays the RMON event table.

Syntax

show rmon events

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 example displays the RMON event table.

```
Console> show rmon events

Index  Description  Type      Community  Owner    Last time sent
-----  -----------  --------  ---------  -------  --------------
                                                  ------
1      Errors       Log                  CLI      Jan 18 2002
                                                  23:58:17
2      High         Log-Trap  device     Manager  Jan 18 2002
       Broadcast                                  23:59:48
```

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.

show rmon log

The **show rmon log** User EXEC mode command displays the RMON log table.

Syntax

show rmon log [*event*]

- *event* — Specifies the event index. (Range: 0 - 65535)

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 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.

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**}

- **history** *entries* — Maximum number of history table entries. (Range: 20 -270)
- **log** *entries* — Maximum number of log table entries. (Range: 20-100)

Default Configuration

History table size is 270.

Log table size is 200.

Command Mode

Global Configuration mode

User Guidelines

- The configured table size takes 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
```

25

SNMP Commands

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*]

- *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 Configuration

No communities are defined.

Command Mode

Global Configuration mode

User Guidelines

- 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.
- The **no snmp-server community** command is used to remove a community or a community group.

Examples

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
```

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*]

- *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. You may also identify the subtree by specifying its logical name; for example, "IfEntry.*.1".
- **included**—Indicates that the view type is included.
- **excluded**—Indicates that the view type is excluded.

Default Configuration

No view entry exists.

Command Mode

Global Configuration mode

User Guidelines

- This command can be entered multiple times for the same view record.
- The number of views is limited to 64 including pre-configured views.
- No check is made to determine that a MIB node corresponds to the "starting portion" of the OID until the first wildcard.
- Following is a list of unsupported counters in the Iftable MIB:
  - ifInDiscards
  - ifOutErrors
  - ifOutQLen
  - ifHCInOctets
  - ifHCInUcastPkts
  - ifHCInMulticastPkts
  - ifHCInBroadcastPkts
  - ifHCOutOctets
  - ifHCOutUcastPkts
  - ifHCOutMulticastPkts
  - ifHCOutBroadcastPkts
- The following counters are also not supported
  - Alignment errors
  - Multiple Collision Frames
  - SQE Test Errors
  - Carrier Sense Errors
  - Symbol Errors

Examples

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
```

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**]}

- *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 Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

The index of the group name table is comprised of Group Name, Security Model, and Security Level. Different views for the same group can be defined with different security levels. For example, after having created the appropriate views, a group can be created for which "no authentication" is required, while allowing only notification view for "interfaces". A group of the same name can be created for which "priv" authentication is required. Read views can, for example, be configured for this group for mib2, and write views for interfaces. In this case, users in this group who send "priv" packets can modify all "interfaces" MIBs and view all mib2.

Examples

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
```

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*]

- *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 Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

- 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.

Examples

The following example configures an SNMPv3 user **John** in group **user-group**.

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

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

- *engineid-string*—Specifies a character string that identifies the engine ID. (Range: 9-64 hexa characters)
- **default**—The engine ID is created automatically based on the device MAC address.

Default Configuration

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

User Guidelines

- 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 to be used for the entire stack, and verify that the stack engine ID is unique throughout the entire management network.

- 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** Global Configuration mode command.

Examples

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
```

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 Configuration

SNMP traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables SNMP traps.

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

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*]

- *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. You may also identify the subtree by specifying its logical name; for example, "IfEntry.*.1".
- **included**—Indicates that the filter type is included.
- **excluded**—Indicates that the filter type is excluded.

Default Configuration

No filter entry exists.

Command Mode

Global Configuration mode

User Guidelines

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.

Examples

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
```

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**]

- *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: 0-65535)
- *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: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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 host {*ip-address* | *hostname*} *username* [**traps** | **informs**]

- *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: 0-65535)
- *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, when a response is not received for a generated message. If unspecified, the default maximum number of retries is 3. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

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
```

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 Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables SNMP failed authentication traps.

```
Console(config)# snmp-server trap authentication
```

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

- *text* — Specifies the string that describes system contact information. (Range: 0-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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 **Dell_Technical_Support**.

```
console(config)# snmp-server contact Dell_Technical_Support
```

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

- *text* — Specifies a string that describes system location information. (Range: 0-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

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
```

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* …]

- *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 Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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.

Examples

The following example configures the scalar MIB sysName with the value **dell**.

```
Console(config)# snmp-server set sysName sysname dell
```

show snmp

The **show snmp** Privileged EXEC mode command displays the SNMP status.

Syntax

show snmp

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 SNMP communications status.

```
Console# show snmp

Community-  Community-    View name     IP
String      Access                     address
----------  ----------    ---------     -------
                                        -
public      read only     user-view     All
private     read write    Default       172.16.1.1
private     su            DefaultSuper  172.17.1.1
```

```
Community-string         Group name    IP address
-----------------        ----------    ----------
public                   user-group    all

Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications
Target Address    Type   Community     Version  UDP    Filter  TO   Retries
                                                Port   Name    Sec
--------------    -----  ---------     -------  ----   ------  ---  -------
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   Retries
                                       Level    Port   Name    Sec
--------------    -----  ---------     -------  ----   ------  ---  -------
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.

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 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 SNMP engine ID.

```
Console# show snmp engineID

Local SNMP engineID: 08009009020C0B099C075878
```

show snmp views

The **show snmp views** Privileged EXEC mode command displays the configuration of views.

Syntax

show snmp views [*viewname*]

- *viewname*—Specifies the name of the view. (Range: 1-30)

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 configuration of views.

```
Console# show snmp views


Name                 OID Tree          Type
-----------  ------------------------  ---------
user-view    1.3.6.1.2.1.1             Included
user-view    1.3.6.1.2.1.1.7           Excluded
user-view    1.3.6.1.2.1.2.2.1.*.1     Included
```

show snmp groups

The **show snmp groups** Privileged EXEC mode command displays the configuration of groups.

Syntax

show snmp groups [*groupname*]

- *groupname*—Specifies the name of the group. (Range: 1-30)

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 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.

show snmp filters

The **show snmp filters** Privileged EXEC mode command displays the configuration of filters.

Syntax

show snmp filters [*filtername*]

- *filtername*—Specifies the name of the filter. (Range: 1-30)

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 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
```

show snmp users

The **show snmp users** Privileged EXEC mode command displays the configuration of users.

Syntax

show snmp users [*username*]

- *username*—Specifies the name of the user. (Range: 1-30)

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 configuration of users.

```
Console# show snmp users

Name      Group name    Auth Method    Remote
------    ------------  ---------      -------------------------
John      user-group    md5
John      user-group    md5            08009009020C0B099C075879
```

26

Spanning-Tree Commands

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 Configuration

Spanning-tree is enabled.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables spanning-tree functionality.

```
Console(config)# 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

- **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 Configuration

STP is enabled.

Command Modes

Global Configuration mode

User Guidelines

- 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
```

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

- *seconds* — Time in seconds. (Range: 4 - 30)

Default Configuration

The default forwarding time for the IEEE Spanning Tree Protocol (STP) is 15 seconds.

Command Modes

Global Configuration mode

User Guidelines

- 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
```

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 Spanning Tree BPDUs to other devices.To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree hello-time

- *seconds* — Time in seconds. (Range: 1 - 10)

Default Configuration

The default hello time for IEEE Spanning Tree Protocol (STP) is 2 seconds.

Command Modes

Global Configuration mode

User Guidelines

- 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
```

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

- *seconds* — Time in seconds. (Range: 6 - 40)

Default Configuration

The default maximum age for IEEE Spanning Tree Protocol (STP) is 20 seconds.

Command Modes

Global Configuration mode

User Guidelines

- 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
```

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

- *priority* — Priority of the bridge. (Range: 0 - 61440 in steps of 4096)

Default Configuration

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

Command Modes

Global Configuration mode

User Guidelines

- 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
```

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 Configuration

Spanning tree is enabled on all ports.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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
```

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

- *cost* — Path cost of the port (Range: 1 - 200,000,000)

Default Configuration

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

User Guidelines

- 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
```

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

- *priority* — The priority of the port. (Range: 0 - 240 in multiples of 16)

Default Configuration

The default port priority for IEEE Spanning TreeProtocol (STP) is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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
```

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

no spanning-tree portfast

Default Configuration

PortFast mode is disabled.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- 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.

Example

The following example enables PortFast on Ethernet port 1/e15.

```
Console(config)# interface ethernet 1/e15
Console(config-if)# spanning-tree portfast
```

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 link-type

- **point-to-point** —Indicates that the port link type is point-to-point.
- **shared** — Indicates that the port link type is shared.

Default Configuration

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

User Guidelines

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
```

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

- *long* — Specifies port path costs with a range of 1-200,000,000 .
- *short* — Specifies port path costs with a range of 0-65,535.

Default Configuration

Short path cost method.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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**}

- **filtering** — Filter BPDU packets when the spanning tree is disabled on an interface.
- **flooding** — Flood BPDU packets when the spanning tree is disabled on an interface.

Default Configuration

The default setting is flooding.

Command Modes

Global Configuration mode

User Guidelines

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
```

clear spanning-tree detected-protocols

The **clear spanning-tree detected-protocols** Privileged EXEC mode command enables the user to set the switches back to RSTP mode without rebooting the device.

Syntax

clear spanning-tree detected-protocols [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

- 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
```

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**

- *instance-id*—ID of the spanning -tree instance (Range: 1-15).
- *priority*—Device priority for the specified spanning-tree instance (Range: 0-61440 in multiples of 4096).

Default Configuration

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

spanning-tree mst max-hops

The **spanning-tree mst max-hops** Global Configuration mode command configures the number of hops in an MST region before the BDPU 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

- *hop-count*—Number of hops in an MST region before the BDPU is discarded . (Range: 1-40)

Default Configuration

The default number of hops is 20.

Command Mode

Global Configuration mode

User Guidelines

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
```

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**

- *instance-ID*—ID of the spanning tree instance. (Range: 1-15)
- *priority*—The port priority. (Range: 0 - 240 in multiples of 16)

Default Configuration

The default port priority for IEEE Multiple Spanning Tree Protocol (MSTP) is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the port priority of port 1/e1 for instance 1 to 142.

```
Console(config)# interface ethernet 1/e1
Console(config-if)# spanning-tree mst 1 port-priority 142
```

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**

- *instance-ID*—ID of the spanning -tree instance (Range: 1-15).
- *cost*—The port path cost. (Range: 1 - 200,000,000)

Default Configuration

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

User Guidelines

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
```

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 Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

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
```

instance (mst)

The **instance** MST Configuration mode command maps VLANS to an MST instance.

Syntax

instance *instance-id* {**add** | **remove**} **vlan** *vlan-range*

- *instance-ID*—ID of the MST instance (Range: 1-15).
- *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: 1-4093).

Default Configuration

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Modes

MST Configuration mode

User Guidelines

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
```

name (mst)

The **name** MST Configuration mode command defines the MST region name. To return to the default setting, use the **no** form of this command.

Syntax

name *string*

no name

- *string*—MST configuration name. Case-sensitive (Range: 1-32 characters).

Default Configuration

The default name is a bridge ID.

Command Mode

MST Configuration mode

User Guidelines

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
```

revision (mst)

The **revision** MST configuration command defines the MST region revision number. To return to the default configuration, use the **no** form of this command.

Syntax

revision *value*

no revision

- *value*—Configuration revision number (Range: 0-65535).

Default Configuration

The default configuration revision number is 0.

Command Mode

MST Configuration mode

User Guidelines

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
```

show (mst)

The **show** MST Configuration mode command displays the current or pending MST region configuration.

Syntax

show {**current** | **pending**}

- **current**—Indicates the current region configuration.
- **pending**—Indicates the pending region configuration.

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

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
```

exit (mst)

The **exit** MST Configuration mode command exits the MST configuration mode and applies all configuration changes.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

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
```

abort (mst)

The **abort** MST Configuration mode command exits the MST configuration mode without applying the configuration changes.

Syntax

abort

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

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
```

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

- *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 ID of the spanning tree instance.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays spanning-tree information.

```
Console# show spanning-tree


Spanning tree enabled mode RSTP
Default port cost method: long


Root ID    Priority             32768
           Address              00:01:42:97:e0:00
           Path Cost            20000
           Root Port            1 (1/e1)
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec


Bridge ID  Priority             36864
           Address              00:02:4b:29:7a:00
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 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 ID    Priority             36864
           Address              00:02:4b:29:7a:00
           This switch is the root.
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 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 ID    Priority             N/A
           Address              N/A
           Path Cost            N/A
           Root Port            N/A
           Hello Time N/A       Max Age N/A        Forward Delay N/A

Bridge ID  Priority             36864
           Address              00:02:4b:29:7a:00
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 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 ID    Priority             32768
           Address              00:01:42:97:e0:00
           Path Cost            20000
           Root Port            1 (1/e1)
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec

Bridge ID  Priority             36864
           Address              00:02:4b:29:7a:00
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 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 ID    Priority             32768
           Address              00:01:42:97:e0:00
           Path Cost            20000
           Root Port            1 (1/1)
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec

Bridge ID  Priority             36864
           Address              00:02:4b:29:7a:00
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 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 ID    Priority             32768
           Address              00:01:42:97:e0:00
           Path Cost            20000
           Root Port            1 (1/e1)
```

```
          Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec

Bridge ID  Priority   36864
          Address              00:02:4b:29:7a:00
          Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec

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) 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          Enabled
1                    10-20                 Enabled

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 Cost  20000
                     Root Port  1 (1/e1)
```

```
                    Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 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 sec    Forward Delay 15 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 Cost 20000
                    Root Port 4 (1/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 Cost 20000
                     Root Port 1 (1/e1)
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 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 sec    Forward Delay 15 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 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) 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 Cost 20000
                     Port Cost 4 (1/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 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: 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 Cost 20000
                     Root Port 1 (1/e1)
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec

IST Master ID        Priority  32768
                     Address   00:02:4b:19:7a:00
                     Path Cost 10000
                     Rem hops  19

Bridge ID            Priority  32768
                     Address   00:02:4b:29:7a:00
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 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 Port  1 (1/e1)
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec
                     Max hops  20
```

spanning-tree guard root

Use the **spanning-tree guard root** interface configuration command to enable root guard on all the spanning tree instances on that interface. Root guard restricts the interface to be the root port for the switch. Use the **no** form of this command to disable root guard on the interface.

Syntax

spanning-tree guard root

no spanning-tree guard root

Default Configuration

Root guard is disabled.

Command Modes

Interface configuration (Ethernet, port-channel).

User Guidelines

Root guard can be enabled when the switch works in STP, RSTP and MSTP.

When root guard is enabled, if spanning-tree calculations cause a port to be selected as the root port, the port transitions to the alternate state.

Example

The following example enable root guard on port e8.

```
Console(config)# interface ethernet 1/e8
Console(config-if)# spanning-tree guard root
```

27

SSH Commands

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

- *port-number* — Port number for use by the SSH server (Range: 1 - 65535).

Default Configuration

The default port number is 22.

Command Mode

Global Configuration mode

User Guidelines

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
```

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 Configuration

Device configuration from a SSH server is enabled.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

crypto key generate dsa

The **crypto key generate dsa** Global Configuration mode command generates DSA key pairs.

Syntax

crypto key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

crypto key generate rsa

The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs.

Syntax

crypto key generate rsa

Default Configuration

RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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 Configuration

Public Key authentication for incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

AAA authentication is independent

Example

The following example enables public key authentication for incoming SSH sessions.

```
Console(config)# ip ssh pubkey-auth
```

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 Configuration

No keys are specified.

Command Mode

Global Configuration mode

User Guidelines

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
Console(config-pubkey-key)# key-string rsa
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
```

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*

- *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 Configuration

No SSH public keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

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
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

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*

- **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 Configuration

No keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

- 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
```

show ip ssh

The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

Syntax

show ip ssh

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 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)

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**]

- **rsa** — Indicates the RSA key.
- **dsa** — Indicates the DSA key.

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 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
```

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**}]

- *username* — Specifies the remote SSH client username.
- **bubble-babble** — Fingerprint in Bubble Babble format.
- **hex** — Fingerprint in Hex format.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

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
```

crypto slogin key generate dsa

The **crypto slogin key generate dsa** Global Configuration mode command generates DSA key pairs for secure login to remote access servers.

Syntax

crypto slogin key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

- Use this command to generate DSA key pairs Secure Copy.
- DSA keys are generated in pairs: one public DSA key and one private DSA key. If the device already has Slogin 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.
- This command may take a considerable period of time to execute.

Example

This example generates DSA key pairs for secure login to remote access servers.

```
Console# config
Console(config)# crypto slogin key generate dsa
```

crypto slogin key generate rsa

The **crypto slogin key generate rsa** Global Configuration mode command generates RSA key pairs for secure login to remote access servers.

Syntax

crypto slogin key generate rsa

Default Configuration

RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

- Use this command to generate RSA key pairs Secure Copy.
- RSA keys are generated in pairs: one public RSA key and one private RSA key. If the device already has Slogin 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.
- This command may take a considerable period of time to execute.

Example

This example generates RSA key pairs for secure login to remote access servers.

```
Console# config
Console(config)# crypto slogin key generate rsa
```

show crypto slogin key mypubkey

The **show crypto slogin key mypubkey** Privileged EXEC mode command displays the secure login public keys of the device.

Syntax

show crypto slogin key mypubkey [**rsa** | **dsa**]

- **rsa** — Indicates the RSA key.
- **dsa** — Indicates the DSA key.

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 secure login public RSA keys of the device

```
Console# show crypto slogin 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
```

28

Syslog Commands

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 Configuration

Logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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*}

- *ip-address* — IP address or URL 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, local**7.
- *text* — Syslog server description. (Range: 1-64 characters)

Default Configuration

The default port number is 514.

The default logging message level is **informational**.

The default facility is local7.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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

- *level* — Specifies the severity level of logged messages displayed on the console. Possible values: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational, debugging.**

Default Configuration

The default severity level is **informational**.

Command Mode

Global Configuration mode

User Guidelines

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
```

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

- *level* — Specifies the severity level of messages logged in the buffer. Possible values: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational, debugging.**

Default Configuration

The default severity level is **informational**.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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

- *number* — Specifies the maximum number of messages stored in the history table. (Range: 20 - 400)

Default Configuration

The default number of messages is 200.

Command Mode

Global Configuration mode

User Guidelines

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
```

clear logging

The **clear logging** Privileged EXEC mode command clears messages from the internal logging buffer.

Syntax

clear logging

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 clears messages from the internal logging buffer.

```
Console# clear logging

Clear logging buffer [yes/no]?
```

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

- *level* — Specifies the severity level of syslog messages sent to the logging file. Possible values: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational** and **debugging.**

Default Configuration

The default severity level is **errors**.

Command Mode

Global Configuration mode

User Guidelines

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
```

clear logging file

The **clear logging file** Privileged EXEC mode command clears messages from the logging file.

Syntax

clear logging file

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 clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [yes/no]?
```

aaa logging

The **aaa logging** Global Configuration mode command enables logging AAA login events in the syslog. To disable logging AAA login events, use the **no** form of this command.

Syntax

aaa logging login

no aaa logging login

- **login** — Indicates logging messages related to successful login events, unsuccessful login events and other login-related events.

Default Configuration

Logging AAA login events is enabled.

Command Mode

Global Configuration mode

User Guidelines

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
```

file-system logging

The **file-system logging** Global Configuration mode command enables logging file system events in the syslog. 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

- **copy** — Indicates logging messages related to file copy operations.
- **delete-rename** — Indicates logging messages related to file deletion and renaming operations.

Default Configuration

Logging file system events is enabled.

Command Mode

Global Configuration mode

User Guidelines

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
```

management logging

The **management logging** global configuration command enables logging management access list (ACL) events in the syslog. To disable logging management access list events, use the **no** form of this command.

Syntax

management logging deny

no management logging deny

- **deny** — Indicates logging messages related to deny actions of management ACLs.

Default Configuration

Logging management ACL events is enabled.

Command Mode

Global Configuration mode

User Guidelines

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
```

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 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 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 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
```

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 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 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
```

show syslog-servers

The **show syslog-servers** Privileged EXEC mode command displays the settings of the syslog servers.

Syntax

show syslog-servers

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 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
```

29

System Management

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*]

- *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 Configuration

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

User Guidelines

- 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
```

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*]

- *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 Configuration

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

User Guidelines

- The **traceroute** command takes advantage of the error messages generated by the routers 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 router 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 router 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.

telnet

The **telnet** User EXEC mode command enables logging on to a host that supports Telnet.

Syntax

telnet {*ip-address* | *hostname*} [*port*] [*keyword1*.....]

- *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 User Guidelines.
- *keyword* — One or more keywords listed in the Keywords table in the User Guidelines.

Default Configuration

The default port is the Telnet port (decimal23) on the host.

Command Mode

User EXEC mode

User Guidelines

- 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
```

  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.

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
```

resume

The **resume** User EXEC mode command enables switching to another open Telnet session.

Syntax

resume [*connection*]

- *connection* — The connection number. (Range: 1 - 4 connections)

Default Configuration

The default connection number is that of the most recent connection.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following command switches to open Telnet session number 1.

```
Console> resume 1
```

reload

The **reload** Privileged EXEC mode command reloads the operating system.

Syntax

reload

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- 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]?
```

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

- *name* — The host name of the device. (Range: 1-158 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the device host name.

```
Console(config)# hostname Dell
Dell(config)#
```

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

- *unit*— Unit number of the new master (Range: 1-2)

Default Configuration

Disables forcing the selection of a stack master.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

stack reload

The **stack reload** Privileged EXEC mode command reloads stack members.

Syntax

stack reload [**unit** *unit*]

- *unit*— Number of the unit to be reloaded (Range: 1-6)

Default Configuration

All units are reloaded.

Command Modes

Privileged EXEC mode

User Guidelines

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
```

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

- **top** *unit*— Specifies the number of the unit displayed at the top. (Range: 1-6)
- **bottom** *unit*— Specifies the number of the unit displayed at the bottom. (Range: 1-6)

Default Configuration

The master unit is displayed at the top.

Command Modes

Global Configuration mode

User Guidelines

- 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 6 at the top of the display and unit 1 at the bottom.

```
Console# config
Console(config)# stack display-order top 6 bottom 1
```

show stack

The **show stack** User EXEC mode command displays information about the status of a stack.

Syntax

show stack [**unit** *unit*]

- *unit*— Specifies the number of the unit. (Range: 1-6)

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 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       6        Slave
2     00:00:b0:87:12:13  1.0.0.0 Enabled   5       1        Master
4     00:00:b0:87:12:14  1.0.0.0           5       6        Slave
5     00:00:b0:87:12:15  1.0.0.0           2       4        Slave
6     00:00:b0:87:12:16  1.0.0.0           4       1        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: PowerCOnnect34xx. Software: 1.0.0.0
Status: Master
Active image: image-1.
Selected for next boot: image-2.
```

show users

The **show users** User EXEC mode command displays information about the active users.

Syntax

show users

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 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
```

show sessions

The **show sessions** User EXEC mode command lists open Telnet sessions.

Syntax

show sessions

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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.

show system

The **show system** User EXEC mode command displays system information.

Syntax

show system [**unit** *unit*]

- *unit*— Specifies the number of the unit. (Range: 1-6)

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 example displays the system information.

```
Console> show system

Unit       Type
----       -----------------
1          PowerConnect 3424

Unit       Main Power Supply    Redundant Power Supply
----       -----------------    ----------------------
1          OK

Unit       Fan1       Fan2       Fan3       Fan4       Fan5
----       ----       ----       ----       ----       ----
1          OK         OK

Unit       Temperature           Temperature Sensor Status
           (Celsius)
----       --------------------  -------------------------
1          30                    OK
```

show version

The **show version** User EXEC mode command displays system version information.

Syntax

show version [**unit** *unit*]

- *unit*— Specifies the number of the unit. (Range: 1-6)

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 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
```

asset-tag

The **asset-tag** Global Configuration mode command specifies the asset tag of the device. To return to the default configuration, use the **no** form of the command.

Syntax

asset-tag [**unit** *unit*] *tag*

no asset-tag [**unit** *unit*]

- *unit*— Specifies the number of the unit. (Range: 1-6)
- *tag* — Specifies the asset tag of the device. (Range: 1- 16 characters)

Default Configuration

No asset tag is defined.

The default unit number is that of the master unit

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the asset tag of the master unit as "1qwepot".

```
Console(config)# asset-tag 1qwepot
```

show system id

The **show system id** User EXEC mode command displays system ID information.

Syntax

show system id [**unit** *unit*]

- *unit*— Specifies the number of the unit. (Range: 1-6)

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 example displays system service and asset tag information.

```
Console> show system id

Service Tag: 89788978

Serial number: 8936589782

Asset tag: 7843678957


Unit           Service tag    Serial number      Asset tag

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

1              89788978       893659782          7843678957

2              34254675       3216523877         5621987728
```

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 Configuration

Disabled.

Command Mode

Global Configuration mode

User Guidelines

- Use the **show cpu utilization** privileged EXEC command to view information on CPU utilization.

Example

This example enables measuring CPU utilization.

```
Console# config

Console(config)# service cpu-utilization
```

show cpu utilization

The **show cpu utilization** Privileged EXEC mode command displays display information about CPU utilization.

Syntax

show cpu utilization

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

- Use the **service cpu-utilization** Global Configuration mode command to enable measuring CPU utilization.

Example

The following example displays CPU utilization.

```
Console# show cpu utilization

CPU utilization service is on.

CPU utilization

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

five seconds: 5%; one minute: 3%; five minutes: 3%
```

30

TACACS+ Commands

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*}

- *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 key 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 Configuration

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

User Guidelines

- 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
```

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

- *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 key used on the TACACS+ daemon. (Range: 0-128 characters)

Default Configuration

Empty string.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the authentication encryption key.

```
Console(config)# tacacs-server key dell-s
```

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

- *timeout* — Specifies the timeout value in seconds. (Range: 1 - 30)

Default Configuration

5 seconds

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the timeout value to 30.

```
Console(config)# tacacs-server timeout 30
```

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*

- *source* — Specifies the source IP address.

Default Configuration

The source IP address is the address of the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example specifies the source IP address.

```
Console(config)# tacacs-server source-ip 172.16.8.1
```

show tacacs

The **show tacacs** Privileged EXEC mode command displays configuration and statistical information about a TACACS+ server.

Syntax

show tacacs [*ip-address*]

- *ip-address* — Name or IP address of the TACACS+ server.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays configuration and statistical information about a TACACS+ server.

```
Console# show tacacs

Device Configuration
--------------------

IP address  Status     Port  Single      TimeOut  Source   Priority
                           Connection           IP
----------  --------   ----  ---------   -------  ------   --------
172.16.1.1  Connected  49    No          Global   Global   1
```

```
Global values
-------------
TimeOut: 3
Device Configuration
--------------------
Source IP: 172.16.8.1
```

31

User Interface

enable

The **enable** User EXEC mode command enters the Privileged EXEC mode.

Syntax

enable [*privilege-level*]

- *privilege-level* — Privilege level to enter the system. (Range: 1 - 15)

Default Configuration

The default privilege level is 15.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters Privileged EXEC mode:

```
Console> enable
enter password:
Console#
```

disable

The **disable** Privileged EXEC mode command returns to the User EXEC mode.

Syntax

disable [*privilege-level*]

- *privilege-level* — Privilege level to enter the system. (Range: 1 - 15)

Default Configuration

The default privilege level is 1.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example returns to Users EXEC mode.

```
Console# disable
Console>
```

login

The **login** User EXEC mode command changes a login username.

Syntax

login

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 example enters Privileged EXEC mode and logs in with username **admin**.

```
Console> login
User Name:admin
Password:*****
Console#
```

configure

The **configure** Privileged EXEC mode command enters the Global Configuration mode.

Syntax

configure

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 enters Global Configuration mode.

```
Console# configure

Console(config)#
```

exit (Configuration)

The **exit** command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

All configuration modes

User Guidelines

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#
```

exit

The **exit** Privileged/User EXEC mode command closes an active terminal session by logging off the device.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

Privileged and User EXEC modes

User Guidelines

There are no user guidelines for this command.

Example

The following example closes an active terminal session.

```
Console> exit
```

end

The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

Syntax

end

Default Configuration

This command has no default configuration.

Command Mode

All configuration modes.

User Guidelines

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#
```

help

The **help** command displays a brief description of the help system.

Syntax

help

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

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?').
```

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 Configuration

Dumping is disabled.

Command Mode

User EXEC mode

User Guidelines

- 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 data-dump 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
```

show history

The **show history** User EXEC mode command lists the commands entered in the current session.

Syntax

show history

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

- 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)
```

show privilege

The **show privilege** Privileged/User EXEC mode command displays the current privilege level.

Syntax

show privilege

Default Configuration

This command has no default configuration.

Command Mode

Privileged and User EXEC modes

User Guidelines

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
```

32

VLAN Commands

vlan database

The **vlan database** Global Configuration mode command enters the VLAN Configuration mode.

Syntax

vlan database

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the VLAN database mode.

```
Console(config)# vlan database
Console(config-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*

- *vlan-range* — Specifies a list of VLAN IDs to be added. Separate non-consecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

VLAN Configuration mode

User Guidelines

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
```

interface vlan

The **interface vlan** Global Configuration mode command enters the Interface Configuration (VLAN) mode.

Syntax

interface vlan *vlan-id*

- *vlan-id* — Specifies an existing VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters Interface Configuration mode for VLAN 1.

```
Console(config)# interface vlan 1
Console(config-if)#
```

interface range vlan

The **interface range vlan** Global Configuration mode command enables simultaneously configuring multiple VLANs.

Syntax

interface range vlan {*vlan-range* | **all**}

- *vlan-range* — Specifies a list of VLAN IDs to be added. Separate non-consecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.
- **all** — All existing static VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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.
- The following commands are not supported with the **interface range vlan** command: **private-vlan primary**, **private-vlan community**, **private-vlan isolated** and **ip internal-usage-vlan**.

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)#
```

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

- *string* — Unique name to be associated with this VLAN. (Range: 1-32 characters)

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) mode. Cannot be configured for a range of interfaces (range context).

User Guidelines

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
```

private-vlan primary

The **private-vlan primary** Interface Configuration mode command configures the primary PVLAN. To return to the default configuration, use the **no** form of this command.

Syntax

private-vlan primary

no private-vlan primary

Default Configuration

No PVLANs are configured.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- An IP interface cannot be defined on a primary VLAN.
- A primary VLAN cannot be defined if an IP interface has been configured on it.
- The command is not supported under the command **interface range vlan**.

Example

This example configures VLAN 200 as the primary private VLAN.

```
Console# config
Console(config)# vlan database
Console(config-vlan)# vlan 200
Console(config-vlan)# exit
Console(config)# interface vlan 200
Console(config-if)# private-vlan primary
```

private-vlan isolated

The **private-vlan isolated** Interface Configuration mode command configures the isolated VLAN of the PVLAN. To return to the default configuration, use the **no** form of this command.

Syntax

private-vlan isolated *vlan-id*

no private-vlan isolated

- *vlan-id* — Specifies the ID of the isolated VLAN.

Default Configuration

No VLAN is configured.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- This command creates an isolated VLAN and associates it with the primary VLAN.
- The command is executed in the context of the primary VLAN.
- An isolated VLAN can only be associated with one primary VLAN.
- A VLAN that has been configured as an isolated VLAN cannot be configured as a primary or community VLAN.
- The command is not supported under the command **interface range vlan**.

Example

This example configures VLAN 20 as the isolated VLAN of primary private VLAN 200.

```
Console# config
Console(config)# vlan database
Console(config-vlan)# vlan 200
Console(config-vlan)# exit
Console(config)# interface vlan 200
Console(config-if)# private-vlan primary
Console(config-if)# private-vlan isolated 20
```

private-vlan community

The **private-vlan community** Interface Configuration mode command associates the primary VLAN with the community VLANs.

Syntax

private-vlan community {**add** *community-vlan-list* | **remove** *community-vlan-list* }

- **add** *community-vlan-list*— Specifies a list of community VLAN IDs to be associated. Separate non-consecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.
- **remove** *community-vlan-list*— Specifies a list of community VLAN IDs to be removed. Separate non-consecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.

Default Configuration

No association is configured.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- This command creates a community VLAN and associates it with the primary VLAN.
- The command is executed in the context of the primary VLAN.
- A community VLAN can only be associated with one primary VLAN.
- A VLAN that has been configured as a community VLAN cannot be configured as a primary or isolated VLAN.
- The command is not supported under the command **interface range vlan**.

Example

This example associates primary private VLAN 200 with community private VLAN 2.

```
Console# config
Console(config)# vlan database
Console(config-vlan)# vlan 200
Console(config-vlan)# exit
Console(config)# interface vlan 200
Console(config-if)# private-vlan community add 2
```

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}

switchport mode private-vlan {promiscuous | community | isolated}

no switchport mode

- **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.
- **promiscuous** — Indicates a promiscuous private-vlan port.
- **community** — Indicates a community private-vlan port.
- **isolated** — Indicates an isolated private-vlan port.

Default Configuration

All ports are in access mode, and belong to the default VLAN (whose VID=1).

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- A port cannot be defined as promiscuous or isolated if it is a member of a VLAN.
- If a port is defined as promiscuous or isolated, it is no longer a member of the default VLAN.

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
```

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

- *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 Configuration

All ports belong to VLAN 1.

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

- 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
```

switchport private-vlan

The **switchport private-vlan** Interface Configuration command configures private-vlan port VLANs. To return to the default configuration, use the **no** form of this command.

Syntax

switchport private-vlan promiscuous *pvlan*

no switchport private-vlan promiscuous

switchport private-vlan isolated *pvlan*

no switchport private-vlan isolated

switchport private-vlan community *cvlan*

no switchport private-vlan community

- *pvlan*— Specifies the ID of the primary VLAN.
- *cvlan*— Specifies the ID of the community VLAN.

Default Configuration

The port is not a member of a PVLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- The community VLAN should be associated with the primary VLAN by using the **private-vlan community** Interface Configuration mode command.
- The VLAN number must be one that has not been created in the VLAN database.
- As the command is used to add a port to a Private VLAN, prior to adding the port, the port must be added to the Private Isolated Mode.

Example

This example configures private VLAN 200 as the primary private VLAN and associates it with promiscuous private VLAN Ethernet port 1/e10.

```
Console# config
Console(config)# vlan database
Console(config-vlan)# vlan 200
Console(config-vlan)# exit
Console(config)# interface vlan 200
Console(config-if)# private-vlan primary
Console(config-if)# exit
Console(config)# interface ethernet 1/e10
Console(config-if)# switchport private-vlan promiscuous 200
```

show vlan private-vlan

The **show vlan private-vlan** Privileged EXEC mode command displays information about private VLANs.

Syntax

show vlan private-vlan [**primary** *vlan-id*]

- *vlan-id*— Specifies the ID of the primary VLAN.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about specific private VLANs.

```
Console# show vlan private-vlan

Primary               Isolated              Community
-------               --------              ---------
100                   101                   102, 103
200                   201                   202, 203

Console# show vlan private-vlan primary 100

Primary VLAN: 100
Isolated VLAN: 101
Community VLANs: 102, 103

Promiscuous ports: 1/e19, 2/e19
Isolated ports: 1/e1-e8, 2/e1-e8

Community             Ports
---------             -----
102                   1/e21, 1/e22
103                   2/e21, 2/e22
```

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* }

- **add** *vlan-list* — List of VLAN IDs to be added. Separate non-consecutive 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 non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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
```

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

- *vlan-id*— Specifies the ID of the native VLAN.

Default Configuration

VID=1.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- 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
```

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*

- **add** *vlan-list* — Specifies the list of VLAN IDs to be added. Separate non-consecutive 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 non-consecutive 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 Configuration

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

User Guidelines

- 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
```

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

- *vlan-id* — Specifies the PVID (Port VLAN ID).

Default Configuration

If the default VLAN is enabled, PVID = 1. Otherwise, PVID=4095.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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
```

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 Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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
```

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 Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

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
```

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*}

- **add** *vlan-list* — Specifies the list of VLAN IDs to be added. Separate non-consecutive 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 non-consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- 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
```

switchport customer vlan

Use the **switchport customer vlan** interface configuration command set the port's VLAN when the interface is in customer mode. Use the **no** form of this command to revert to default.

Syntax

switchport customer vlan *vlan-id*

no switchport customer vlan

vlan-id — VLAN ID of the customer

Default Configuration

No VLAN is configured

Command Mode

Interface configuration (Ethernet, port-channel)

User Guidelines

There are no user Guidelines for this command

Example

The following example sets the port's VLAN when the interface is in customer mode.

```
Console(config)# interface ethernet 1/e5
Console(config-if)# switchport customer vlan vlan-id
```

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

- *vlan-id* — Specifies the ID of the internal usage VLAN.

Default Configuration

The software reserves an unused VLAN as the internal usage VLAN of an interface.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- 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.
- This command is not supported under the command **interface range vlan**.

Example

The following example reserves VLAN 15 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 15
```

mac-to-vlan

The **mac-to-vlan** VLAN Configuration mode command adds MAC addresses to the MAC-to-VLAN database. To remove MAC addresses from the database, use the **no** form of this command.

Syntax

mac-to-vlan *mac-address vlan-id*

no mac-to-vlan *mac-address*

- *mac-address*— Specifies the MAC address to be added to the list.
- *vlan-id* — Specifies the VLAN ID.

Default Configuration

No MAC address entry in the database.

Command Mode

VLAN Configuration mode

User Guidelines

- The associated VLAN cannot be the default VLAN.
- Up to 256 MAC addresses can be mapped to a VLAN.
- A MAC can be mapped to only one VLAN. If the same MAC is mapped to more than one VLAN, it is effectively mapped only according to the last mapping.

Example

This example maps MAC address 0060.704c.73ff to VLAN 123.

```
Console# config
Console(config)# vlan database
Console(config-if)# mac-to-vlan 0060.704c.73ff 123
```

show vlan mac-to-vlan

The **show vlan mac-to-vlan** Privileged EXEC mode command displays the MAC-to-VLAN database.

Syntax

show mac-to-vlan [*mac-address*]

- *mac-address*— Specifies the MAC address to be viewed.

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 MAC-to-VLAN database.

```
Console# show vlan mac-to-vlan


MAC Address          VLAN
-----------          ----
```

```
0060.704c.73ff       123
0060.708c.73ff       deny
```

show vlan

The **show vlan** Privileged EXEC mode command displays VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- *vlan-id* — specifies a VLAN ID
- *vlan-name* — Specifies a VLAN name string. (Range: 1 - 32 characters)

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 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    -
```

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 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 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
```

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*}

- *interface* — A valid Ethernet port number.
- *port-channel-number* — A valid port-channel 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 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 is member in:
Vlan        Name                Egress rule    Type
----        -------             -----------    -------
1           default             untagged       System
8           VLAN008             tagged         Dynamic
11          VLAN011             tagged         Static
19          IPv6 VLAN           untagged       Static
72          VLAN0072            untagged       Static

Static configuration:
PVID: 1 (default)
Ingress Filtering: Enabled
Acceptable Frame Type: All
```

```
Port is statically configured to:
Vlan        Name                Egress rule
----        -------             -----------
1           default             untagged
11          VLAN011             tagged
19          IPv6 VLAN           untagged
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 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 is statically configured to:
Vlan        Name                Egress rule
----        ------------        -----------
8           VLAN0072            untagged
91          IP Telephony        tagged

Forbidden VLANS:
VLAN        Name
----        ----
73          out

Port 2/e19
VLAN Membership mode: Private-VLAN Community
Primary VLAN: 2921
Community VLAN: 2922

Console# show interfaces switchport ethernet 2/e19
Port 2/e19:
VLAN Membership mode: Private-VLAN Community

Operating parameters:
PVID: 2922
Ingress Filtering: Enabled
Acceptable Frame Type: Untagged
GVRP status: Disabled
```

```
Port is member in:
Vlan        Name                Egress rule    Type
----        ------------        -----------    ------
2921        Primary A           untagged       Static
2922        Community A1        untagged       Static

Static configuration:
PVID: 2922
Ingress Filtering: Enabled
Acceptable Frame Type: Untagged
GVRP status: Disabled
```

33

Web Server

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 Configuration

HTTP server is enabled.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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

- *port-number* — Port number for use by the HTTP server. (Range: 1-65534)

Default Configuration

The default port number is 80.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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 Configuration

HTTPS server is disabled.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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

- *port-number* — Port number to be used by the HTTPS server. (Range: 1-65534)

Default Configuration

The default port number is 443.

Command Mode

Global Configuration mode

User Guidelines

- Specifying 0 as the port number effectively disables HTTPS access to the device.

Example

The following example configures the https port number to 100.

```
Console(config)# ip https port 100
```

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*]

- *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 Configuration

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

User Guidelines

- 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
```

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*]

- *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 Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

- 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.

Examples

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
```

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**

- *number* — Specifies the certificate number. (Range: 1 - 2)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

- 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: Jan 1 02:44:50 2003 GMT
Valid to: Dec 31 02:44:50 2004 GMT
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

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

- *number* — Specifies the certificate number. (Range: 1 - 2)

Default Configuration

Certificate number 1.

Command Mode

Global Configuration mode

User Guidelines

- 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
```

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*]

- *number* — Specifies the certificate number. (Range: 1- 2)

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 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: Jan 1 02:44:50 2003 GMT
Valid to: Dec 31 02:44:50 2004 GMT
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

show ip http

The **show ip http** Privileged EXEC mode command displays the HTTP server configuration.

Syntax

show ip http

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 HTTP server configuration.

```
Console# show ip http
HTTP server enabled. Port: 80
```

show ip https

The **show ip https** Privileged EXEC mode command displays the HTTPS server configuration.

Syntax

show ip https

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 HTTP server configuration.

```
Console# show ip https
HTTPS server enabled. Port: 443


Certificate 1 is active
Issued by: www.verisign.com
Valid from: Jan 1 02:44:50 2004 GMT
Valid to: Dec 31 02:44:50 2005 GMT
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

```
Certificate 2 is inactive
Valid From: Jan 1 02:44:50 2004 GMT
Valid to: Dec 31 02:44:50 2005 GMT
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```

34

802.1x Commands

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

- *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 Configuration

No authentication method is defined.

Command Mode

Global Configuration mode

User Guidelines

- 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.
- The device accepts EAP frames with a priority tag and also accepts EAP packets with VLAN tags.

Examples

The following example uses the **aaa authentication dot1x default** command with no authentication.

```
Console(config)# aaa authentication dot1x default none
```

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

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables 802.1x globally.

```
Console(config)# dot1x system-auth-control
```

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

- **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)

User Guidelines

- 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.

Examples

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
```

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 Configuration

Periodic re-authentication is disabled.

Command Mode

Interface Configuration (Ethernet)

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables periodic re-authentication of the client.

```
Console(config)# interface ethernet 1/e16
Console(config-if)# dot1x re-authentication
```

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

- *seconds* — Number of seconds between re-authentication attempts. (Range: 300 - 4294967295)

Default Configuration

Re-authentication period is 3600 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Examples

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
```

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*]

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following command manually initiates a re-authentication of 802.1X-enabled Ethernet port 1/e16.

```
Console# dot1x re-authenticate ethernet 1/e16
```

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

- *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 Configuration

Quiet period is 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- 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.

Examples

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
```

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

- *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

User Guidelines

- 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

Examples

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
```

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

- *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

User Guidelines

- 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

Examples

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
```

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

- *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

User Guidelines

- 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

Examples

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
```

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

- *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

User Guidelines

- 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.

Examples

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
```

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*]

- *interface* — Valid Ethernet port. (Full syntax: *unit*/*port*)

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 status of 802.1X-enabled Ethernet ports.

```
Console# show dot1x

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

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
```

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.

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*]

- *username* — Supplicant username (Range: 1-160 characters)

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 802.1X users.

```
Console# show dot1x users

Port   Username    Session Time   Auth Method    MAC Address
-----  --------    ------------   -----------   --------------
1/e1   Bob         1d:03:08.58    Remote        0008:3b79:8787
1/e2   John        08:19:17       None          0008:3b89:3127
```

```
Console# show dot1x users username Bob

Username: Bob
Port   Username    Session Time   Auth Method    MAC Address
-----  --------    ------------   -----------   --------------
1/e1   Bob         1d:03:08.58    Remote        0008:3b79:8787
```

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.

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*

- *interface* — Valid Ethernet port. (Full syntax: *unit/port*)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

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.

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

User Guidelines

- 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
```

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

no dot1x multiple-hosts

Default Configuration

Multiple hosts are disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- This command enables the attachment of multiple clients to a single 802.1X-enabled port. In this mode, 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.
- For unauthenticated VLANs, multiple hosts are always enabled.
- Multiple-hosts must be enabled to enable port security on the port.

Examples

The following command enables multiple hosts (clients) on an 802.1X-authorized port.

```
Console(config-if)# dot1x multiple-hosts
```

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

- **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 Configuration

Frames with source addresses that are not the supplicant address are discarded.

No traps are sent.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- 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
```

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 Configuration

No VLAN is defined as a guest VLAN.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- 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.

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
```

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 Configuration

Disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

- 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
```

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*]

- *interface* — Valid Ethernet port. (Full syntax: *unit*/*port*)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays 802.1X advanced features for the device.

```
Console# show dot1x advanced

Guest VLAN: 2
Unauthenticated VLANs: 91,92

Interface             Multiple Hosts        Guest VLAN
---------             --------------        ----------
1/e1                  Disabled              Enabled
1/e2                  Enabled               Disabled
```

```
Console# show dot1x advanced ethernet 1/e1

Interface             Multiple Hosts        Guest VLAN
---------             --------------        ----------
1/e1                  Disabled              Enabled

Single host parameters
Violation action: Discard
Trap: Enabled
Trap frequency: 100
Status: Single-host locked
Violations since last trap: 9
```