Cisco Small Business 200 Series Advanced Smart Switch Command Line Reference

Chapter 1: Using the Command Line Interface 14

Chapter 2: Administration 22

Chapter 5: Spanning Tree Protocol 257

Chapter 6: MAC Address Tables 285

Using the Command Line Interface

The command-line interface (CLI) provides a text-based way to manage and monitor the system. You can access the CLI using a physical serial connection or a remote logical connection with telnet.

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

- **Command Syntax**
- **Command Conventions**
- **Interface Naming Convention**
- **Using the No Form of a Command**
- **Command Modes**
- **Command Completion and Abbreviation**
- **CLI Error Messages**
- **Command Organization in this Document**

Command Syntax

A command is one or more words that might include one or more parameters. Parameters might be required or optional values.

Some commands, such as **show network** or **clear vlan**, do not require parameters. Other commands, such as **network parms**, require that you supply a value after the command. You must type the parameter values in a specific order. Optional parameters follow required parameters. The following example describes the **network parms** command syntax:

network parms ***ip-address netmask*** [***gateway***]

- **network parms** is the command name.
- ***ip-address*** and ***netmask*** are mandatory parameters that you must replace with the actual value.
- ***gateway*** is an optional parameter that you can replace with text.

This reference lists each command by the command name and provides the following information where applicable:

- Syntax Descriptions—describes each keyword and parameter.
- Defaults—describe any default values for the command parameters.
- Command Modes—identifies the CLI command modes in which you can execute the command.
- Examples—one or more examples of the command string, the output, and descriptions of the output fields, if applicable.
- Related Commands—other commands you can use in conjunction with the primary command.

Command Conventions

In this document the command elements include command key words and parameters. Key words are entered as shown in the command. Parameters are shown in italics and represent variable text. You must replace the parameter name with an appropriate value, which might be an alphabetic, numeric, or alphanumeric value. Parameters are order-dependent.

Keywords and parameters could be mandatory or optional, and might be one of several choices. The following table describes the conventions this document uses to distinguish command elements.

Symbol	Examples	Description
No brackets	**spanning-tree**	Mandatory parameter that is not in italics. The command element is a keyword. Enter it as shown. When in italics, the command element is a variable (placeholder text). Enter your own text to replace it.
	ip-address	A parameter in italics is a variable (placeholder text). Enter the command, replacing the variable in the command with a value. For example, the ***ip-address*** variable might be replaced by 192.168.10.254.
[ ] square brackets	**[encrypted]**	Optional parameter entered as show.
	[***ip-address***]	Optional variable that can be replaced by a value.
	[**level** ***0-100***]	Optional parameter with a range of values.

Symbol	Examples	Description
{} curly braces	**{drop | forward}**	A list of parameter choices, each separated by a vertical bar, to be entered as shown.
	{***ip-address*** | ***hostname***}	A list of parameter choices, each separated by a vertical bar. The chosen variable is replaced by the appropriate value.
[{}] Braces within square brackets	{**source interface** ***interface*** [{**rx** | **tx**}]	A required choice within an optional element. In the example, if you chose to enter **source interface**, you must enter a value for the ***interface*** parameter, and you can optionally chose the **rx** or the **tx** parameter.

Interface Naming Convention

Fast Ethernet switch ports are represented in the CLI as *e1* for port 1, *e2* for port 2, *e3* for port 3, and so forth.

The gigabit Ethernet switch ports are represented as *g1* and *g2*.

Link aggregation groups (LAGs) are configurable as logical interfaces and are represented in the CLI as *ch1*, *ch2*, *ch3*, and so forth.

Using the No Form of a Command

The **no** keyword is a specific form of an existing configuration command and does not represent a new or distinct command. Almost every configuration command has a **no** form. In general, use the **no** form of the command to reverse the action of a command or reset it to the default value. Example:

```
#no shutdown
```

Reverses the **shutdown** command to bring up the interface.

Using a Space in a Command

To include a space in a string, enclose the string in quotes, such as "*string space*". Example:

```
#set contact "Thom Dobro"
```

Command Modes

Modes group commands according to the function of each command. The commands in a particular mode are not available until you change to that mode.

The command prompt changes in each command mode to identify the current mode. The following table describes the command modes and the prompts for that mode.

NOTE In the following table, the word *switch* in the prompt represents the switch hostname. By default, the hostname is **switch***<last three bytes of the MAC address>*. You can use the **set hostname** command to configure a different hostname that will display in the CLI prompt.

Command Mode	Prompt	Description
Privileged EXEC	switch#	**The show commands that display** status and statistics, some configuration commands, and access to the Global Config and VLAN Config modes.
Global Config	switch (Config)#	General setup commands and modifications to the running configuration.
VLAN Config	switch (Vlan)#	VLAN configuration commands.
Interface Config	(switch) (Interface *interface*)#	Manage the interfaces.
Access List Config	switch(config-macal)#	Switch management access list configuration commands.

Command Mode	Prompt	Description
Line Console Config	switch (config-line)#	Outbound telnet settings and console interface settings, including console login and authentication information.
Line SSH Config	switch (config-ssh)#	SSH login and authentication information.
Line Telnet Config	switch (config-telnet)#	Telnet login and authentication information.

The following table explains how to enter and exit each mode.

Mode	To Enter	To Exit
Privileged EXEC	Users enter this mode when they log in.	To log out of the CLI session, enter **quit**.
Global Config	From the Privileged EXEC mode, enter **configure** or **config**.	To exit to the Privileged EXEC mode, enter **exit**, or press **Ctrl-Z**.
VLAN Config	From the Privileged EXEC mode, enter **vlan database**.	To exit to the Privileged EXEC mode, enter **exit** or press **Ctrl-Z**.
Interface Config	From the Global Config mode, enter **interface** *interface*	To exit to the Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter **Ctrl-Z**.
Access List Config	From the Global Config mode, enter **management access-list** *listname*	To exit to the Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter **Ctrl-Z**.
Line Console	From the Global Config mode, enter **line console**.	To exit to the Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter **Ctrl-Z**.
Line SSH	From the Global Config mode, enter **line ssh**.	To exit to the Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter **Ctrl-Z**.

Mode	To Enter	To Exit
Line telnet	From the Global Config mode, enter **line telnet**.	To exit to the Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter **Ctrl-Z**.

Command Completion and Abbreviation

The command completion feature finishes spelling the keyword when you type enough letters of a command to uniquely identify the command keyword. After you have entered enough letters, press the spacebar or **Tab** key to complete the keyword.

The command abbreviation feature allows you to execute a command when you have entered enough letters to uniquely identify the command. You must enter all of the required keywords and parameters, however.

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. The most common CLI error messages are:

- `% Invalid input detected at '^' marker`—You entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.
- `Command not found / Incomplete command. Use ? to list commands`—You did not enter the required keywords or values.
- `Ambiguous command`—You did not enter enough letters to uniquely identify the command.

Using CLI Help

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

Command Organization in this Document

This document is divided into chapters, such as Administration and Port Management chapters, based on general CLI functions. Chapters are divided into sections, such as the Port Mirroring and Cable Diagnostics sections, where all commands related to those features are listed. Commands that configure the feature are listed first in each section, in alphabetical order, followed by commands that display status and statistics information (**show** commands), in alphabetical order.

2

Administration

This chapter describes how to configure global system settings and perform diagnostics.

It contains the following topics:

- **Control Packet Handling**
- **Auto Configuration**
- **Bonjour**
- **Port Mirroring**
- **Cable Diagnostics**
- **PoE**
- **Switch Management Access Control**
- **SNTP and Time Settings**
- **System Software and Configuration Management**
- **Syslog**
- **RMON**

Control Packet Handling

You can use the commands described in this section to control how the switch handles packets of the Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), or 802.1X protocol.

protocol cdp

Use this command to drop or forward Cisco Discovery Protocol (CDP) packets. CDP enables directly connected devices to share information such as their IP addresses, capabilities, and software versions. Although the switch does not use CDP to share its own information, by default it forwards CDP packets on behalf of connected devices within a VLAN.

protocol cdp {**drop** | **forward**}

Syntax Descriptions

Parameter	Description
drop	The switch drops all CDP packets.
forward	The switch forwards all CDP packets.

Default

CDP packets are forwarded.

Command Modes

Global Config

protocol {lldp | dot1x}

Use this command to drop, forward, or terminate Link Layer Discovery Protocol (LLDP) or IEEE 802.1X Extensible Authentication Protocol over LAN (EAPOL) packets.

protocol {**lldp** | **dot1x**} {**drop** | **forward** | **terminate**}

Syntax Descriptions

Parameter	Description
lldp	Specifies that the command applies to LLDP packets.
dot1x	Specifies that the command applies to IEEE 802.1X packets.
drop	Drop all packets of the specified type.
forward	Forwards all packets of the specified type to the VLAN.
terminate	Process the packets.

Default

LLDP and 802.1X packets are terminated.

Command Modes

Global Config

Usage Guidelines

LLDP or 802.1X must be disabled globally before you can use this command to configure the drop, forward, or terminate action for each protocol.

Related Commands

Command	Description
[no] lldp med	Enables and disables LLDP MED.
[no] dot1x port-control	Enables and disables the 802.1X operation on all ports.
show protocol	Displays the drop, forward, or terminate state for the CPD, LLDP, and Dot1X protocols.

show protocol

Use this command to display the drop, forward, or terminate state for the CPD, LLDP, and Dot1X protocols.

```
show protocol
```

Command Modes

Privileged Exec

Examples

The following shows sample output for the command:

```
(Switch) #show protocol

Protocol  Mode
--------  ----
cdp         forward
dot1x       terminate
lldp        terminate
```

Related Commands

Command	Description
protocol cpd	Configures the switch to drop or forward CDP packets.
protocol {lldp | dot1x}	Configures the switch to drop, forward, or terminate LLDP or 802.1X packets.

Auto Configuration

The following commands configure the Auto Configuration file download feature. When enabled, the switch automatically downloads a network configuration file if no file is found in flash memory when the switch reboots. The switch uses information obtained through DHCP to identify the TFTP server and file name to use in the download.

boot autoinstall

Use this command to enable DHCP Auto Configuration on the switch. Use the **no** form of the command to disable this feature.

boot autoinstall

no boot autoinstall

Default

DHCP Auto Configuration is enabled.

Command Modes

Privileged Exec

Usage Guidelines

The Auto Configuration feature depends upon the proper configuration of other devices in the network, including a DHCP or BOOTP server, a TFTP server, and, if necessary, a DNS server.

Related Commands

Command	Description
boot autoinstall default-config	Enables the switch to look for and download a default network configuration file upon startup when no host-specific configuration file is found.
show autoinstall	Displays Auto Configuration status information.
boot autoinstall backup-tftp	Configures the address of a backup TFTP server to be used when the Auto Configuration process cannot locate the primary server or network configuration file name provided by the DHCP server at startup.
boot autoinstall backup-bootfile	Configures a backup configuration file name to be used when the Auto Configuration process cannot locate the primary server or network configuration file name provided by the DHCP server at startup.

boot autoinstall backup-bootfile

Use this command to configure a backup configuration file name to be used when the Auto Configuration process cannot locate the primary server or configuration file name provided by a DHCP server at startup.

boot autoinstall backup-bootfile *filename*

no boot autoinstall backup-bootfile

Syntax Descriptions

Parameter	Description
filename	The name of the network configuration file on the backup TFTP server.

Default

No backup file name is configured.

Command Modes

Privileged Exec

Related Commands

Command	Description
boot autoinstall	Enables or disables the Auto Configuration feature.
boot autoinstall backup-tftp	Configures the address of a backup TFTP server to be used when the Auto Configuration process cannot locate the server or network configuration file name provided by the DHCP server at startup.
show autoinstall	Displays Auto Configuration status information.

boot autoinstall backup-tftp

Use this command to configure the address of a backup TFTP server to be used when the Auto Configuration process cannot locate the primary server or configuration file name provided by the DHCP server at startup. Use the **no** form of this command to delete the backup server address.

boot autoinstall backup-tftp {*server-ip* | *hostname***}**

no boot autoinstall backup-tftp

Syntax Descriptions

Parameter	Description
server ip	The IP address of a TFTP server.
hostname	The hostname of the backup TFTP server. The switch must be configured to use a DNS server if a hostname is specified.

Default

No backup TFTP server address is configured.

Command Modes

Privileged Exec

Related Commands

Command	Description
boot autoinstall	Enables and disables the Auto Configuration feature.
boot autoinstall backup-bootfile	Configures a backup configuration file name to be used when the Auto Configuration process cannot locate the server or network configuration file name provided by the DHCP server at startup.
show autoinstall	Displays Auto Configuration status information.

boot autoinstall default-config

Use this command to enable the switch to attempt to download a default network configuration file when no host-specific configuration file is found during bootup. Use the `no` form of this command to disable it.

boot autoinstall default-config

no boot autoinstall default-config

Default

This feature is enabled.

Command Modes

Privileged Exec

Usage Guidelines

The Auto Configuration feature must be enabled on the switch for this feature to be operational. See the **boot autoinstall** command.

Related Commands

Command	Description
boot autoinstall	Enables and disables the Auto Configuration feature.
show autoinstall	Displays Auto Configuration status information.

show autoinstall

Use this command to display the status of the Auto Configuration feature.

show autoinstall

Command Modes

Privileged Exec

Examples

The following shows sample output for the command:

```
(Switch) #show autoinstall

AutoInstall Mode............................... Started
AutoInstall default-config Mode................ Disabled
AutoInstall Backup TFTP Server Address......... Not configured
AutoInstall Backup Boot Filename............... Not configured
AutoInstall State.............................. Waiting for boot options
```

Related Commands

Command	Description
boot autoinstall	Enables and disables the autoinstall feature.

Command	Description
boot autoinstall default-config	Enables the switch to look for and download a default network configuration file upon startup when no host-specific configuration file is found.
boot autoinstall backup-tftp	Configures the address of a backup TFTP server to be used when the Auto Configuration process cannot locate the server or network configuration file name provided by the DHCP server at startup.
boot autoinstall backup-bootfile	Configures a backup configuration file name to be used when the Auto Configuration process cannot locate the server or network configuration file name provided by the DHCP server at startup.

Bonjour

Bonjour enables the switch and its services to be discovered by using multicast DNS (mDNS). Bonjour advertises switch services to the network and answers queries for service types it supports, simplifying network configuration in small business environments.

bonjour run

Use this command to enable Bonjour on the switch. Use the `no` form of the command to disable it.

bonjour run

no bonjour run

Default

Bonjour is enabled.

Command Modes

Global Config

Usage Guidelines

When bonjour is enabled, the switch advertises the following service types:

- Cisco-specific device description (csco-sb)—This service enables clients to discover Cisco switches and other products deployed in small business networks.
- Management user interfaces—This service identifies the management interfaces available on the switch (HTTP, Telnet, or SSH).

When a Bonjour-enabled switch is attached to a network, any Bonjour client can discover and get access to the management interface without prior configuration.

A system administrator can use an installed Internet Explorer plug-in to discover the switch. The web-based interface for this switch shows up as a tab in the browser.

Bonjour works in both IPv4 and IPv6 networks.

Related Commands

Command	Description
show bonjour	Displays Bonjour configuration details.

show bonjour

Use this command to show all the info related to Bonjour like on/off Bonjour, RR TTL, and all the available service types.

show bonjour

Command Modes

Privileged Exec

Examples

The following example shows the output of the **show bonjour** command.

```
User:cisco
Password:**********
(Switch) #show bonjour

Bonjour Administration Mode: Enabled

Published Services:
```

```
#   Service Name       Type             Domain        Port    TXT    data
 --- -----------------  ---------------  ------------  ------  ------------------------
  1  switchEC38FE    _csco-sb._tcp.  local.         80              deviceType=Switch
                                                                       deviceDescr=Emulation,
                                                     0.0.0.0, Linux 2.6.23.17-
                                                                            88.fc7
                                                                            fmVersion=0.0.0.0
                                                                            hdVersion=1.0
                                                                            hostname=switchEC38FE
                                                               MACAddress=00:02:BC:EC:38:
                                                                            FE
                                                                            model=Emulation
                                                                            serialNo=none
```

Related Commands

Command	Description
bonjour run	Enables Bonjour on the switch.

Port Mirroring

Port Mirroring enables you to monitor and analyze network traffic on a port or VLAN by using a network analyzer.

A mirroring session consist of a destination probe port and at least one source port or VLAN. The external network analyzer can use any of the Ethernet ports as a probe port. The probe port transmits a mirror copy of the probed traffic to the network analyzer.

A port configured as a destination port acts as a mirroring port when the session is operationally active. When the session is not active, the port acts as a normal port with respect to transmitting traffic.

monitor session

This command adds a mirrored port (source port) or probe port (destination port) to a mirroring session. This command can also be used to disable the administrative mode of the session. The no form of this command removes all the configuration of this session, including the source and destinations interfaces and VLAN.

monitor session *1-4* {**source interface** *interface* [{**rx** | **tx**}] | **vlan** *vlan-id* |
destination interface *interface* | **mode**}

no monitor session *session-id* {**source interface** *interface* | **vlan** *vlan-id* |
destination interface *interface* | **mode**}

Syntax Descriptions

Parameter	Description
1-4	Four port mirroring sessions can be configured, numbered 1 to 4.
source interface	The port or LAG to be mirrored.
rx | tx	If the **source interface** parameter is specified, option **rx** can be used to monitor only ingress packets. Option **tx** can be used to monitor only egress packets. If no option is specified, both ingress and egress packets are monitored.
vlan-id	The VLAN ID of the traffic to be monitored.
destination interface	The port where data from the monitored port will be copied to.
mode	Enables the mirroring session. Use the `no` form of the command with the **mode** keyword to disable the session while leaving all other configured values intact.

Default

No port is configured to perform mirroring.

Command Modes

Global Config

Usage Guidelines

VLAN mirroring mirrors only the ingress (Rx) traffic only.

Examples

The following commands configure a mirroring session that copies VLAN 30 traffic received on port e7 to port e8:

```
(Switch) (Config)#monitor session 1 source interface e7 rx
(Switch) (Config)#monitor session 1 vlan 30
(Switch) (Config)#monitor session 1 destination interface e8
```

The following command administratively enables mirroring session 1:

```
(Switch) (Config)#monitor session 1 mode
```

Related Commands

Command	Description
show monitor session	Displays the port monitoring information for a particular mirroring session.

show monitor session

This command displays the port and vlan mirroring information for a particular mirroring session.

show monitor session *session-id*

Syntax Descriptions

Parameter	Description
session-id	A unique number assigned to the mirroring session when it was configured.

Command Modes

Privileged EXEC

Examples

The following example shows the output of this command when no VLAN is specified.

```
(Switch) #show monitor session 1

Port Mirroring is enabled on Following VLAN: None

Session ID   Admin Mode   Probe Port    Mirrored Port   Type
----------   -----------  -----------   --------------  -------
1            Enable       e1            e2              Rx,Tx
                                        e3              Rx,Tx
```

The following example shows the output of this command when a VLAN is specified.

```
(Switch) #show monitor session 2

Port Mirroring is enabled on Following VLAN: 10

Session ID   Admin Mode   Probe Port   Mirrored Port   Type
----------   ----------   ----------   -------------   -------
1            Enable       e4           e5              Rx
```

Related Commands

Command	Description
monitor session	Adds a mirrored port (source port) or probe port (destination port) to a mirroring session and enables the administrative mode of the session.

Cable Diagnostics

The commands in this section enable you to run hardware diagnostic tests on ports and view the results.

show cablestatus

Use this command to display the cable connection status on a selected port.

show cablestatus *interface*

Syntax Descriptions

Parameter	Description
interface	The port number.

Command Modes

Privileged Exec

Examples

The following example shows sample command output.

```
(switch) #show cablestatus e1

Cable Status.................................. Normal
Cable Length.................................. 0m - 10m

(switch) #show cablestatus e2

Cable Status.................................. Open
Failure Location.............................. 1m
```

Cable Status	One of the following states is returned: ▪ Normal—The cable is working correctly. ▪ Open—The cable is disconnected or there is a faulty connector. ▪ Short—There is an electrical short in the cable. ▪ Cable Test Failed—The cable status could not be determined. The cable might be working.
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, the cable status might display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

Failure Location	The estimated distance in meters from end of the cable to the failure location. The failure location is valid only if the cable status is Open or Short.

Related Commands

Command	Description
show fiber-ports optical transceiver	Displays diagnostic information for optical transceivers.

show fiber-ports optical-transceiver

Use this command to display diagnostics for optical transceivers.

show fiber-ports optical-transceiver [*interface*]

Syntax Descriptions

Parameter	Description
interface	The port number.

Command Modes

Privileged Exec

Examples

The following example shows output for the command when no port is specified.

```
Output    Input
Port     Temp  Voltage  Current     Power    Power   TX     LOS
          [C]   [Volt]     [mA]     [dBm]    [dBm]   Fault
-------  ----  -------   -------   -------  -------  -----  ---
g1        0.4    0.000  3081249.3   54.887   50.502   Yes    No
g2        0.9    0.000  3081249.3   54.887   50.502   Yes    No

 Temp - Internally measured transceiver temperatures.
 Voltage - Internally measured supply voltage.
 Current - Measured TX bias current.
 Output Power - Measured optical output power relative to 1mW.
 Input Power - Measured optical power received relative to 1mW.
 TX Fault - Transmitter fault.
 LOS - Loss of signal.
```

TEMP	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured TX output power in milliwatts.
Input Power	Measured RX received power in milliwatts.
TX Fault	Transmitter fault.
LOS	Loss of signal.

Related Commands

Command	Description
show cablestatus	Displays the cable connection status on a selected port.

PoE

The following commands configure the Power-over-Ethernet functionality on the switch.

NOTE These commands are valid only for the SF 200E-24P and SF 200E-48P switches.

lldp med transmit-tlv

Use this command to specify the optional Type Length Values (TLVs) in the LLDP MED set transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) on a specific port. Use the `no` form of the command to exclude the specified TLV for the specified port.

lldp med transmit-tlv [**capabilities**] [**ex-pse**] [**inventory**] [**location**] [**network-policy**]

no lldp med transmit-tlv [**capabilities**] [**ex-pse**] [**inventory**] [**location**] [**network-policy**]

Syntax Descriptions

Parameter	Description
capabilities	Includes the switch capabilities TLV in LLDP advertisements.
ex-pse	Includes the extended power sourcing equipment TLV in LLDP advertisements. This keyword is available only on switches that support PoE.
inventory	Includes the switch inventory TLV in LLDP advertisements.
location	Includes the switch location TLV in LLDP advertisements.
network-policy	Includes the switch network policy TLV in LLDP advertisements.

Default

No LLDP capabilities are advertised.

Command Modes

Interface Config

Examples

The following example includes the network policy TLV in LLDP advertisements on port e7.

```
(Switch) (Interface e7)#lldp med transmit-tlv network-policy
```

Related Commands

Command	Description
lldp med transmit-tlv	Specifies the optional Type Length Values (TLVs) in the LLDP MED set that are transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) on all ports.

lldp med transmit-tlv all

Use this command to specify the optional Type Length Values (TLVs) in the LLDP MED set transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) for all ports. Use the `no` form of the command to exclude the specified TLV for all the ports.

lldp med transmit-tlv all [**capabilities**] [**ex-pse**] [**inventory**] [**location**] [**network-policy**]

no lldp med transmit-tlv all [**capabilities**] [**ex-pse**] [**inventory**] [**location**] [**network-policy**]

Syntax Descriptions

Parameter	Description
capabilities	Includes the switch capabilities TLV in LLDP advertisements.
ex-pse	Includes the extended power sourcing equipment TLV in LLDP advertisements. This keyword is available only on switches that support PoE.
inventory	Includes the switch inventory TLV in LLDP advertisements.
location	Includes the switch location TLV in LLDP advertisements.
network-policy	Includes the switch network policy TLV in LLDP advertisements.

Default

No LLDP capabilities are advertised.

Command Modes

Global Config

Examples

The following example includes the network policy TLV in LLDP advertisements on all ports.

```
(Switch) (Config)#lldp med transmit-tlv all network-policy
```

Related Commands

Command	Description
lldp med transmit-tlv	Specifies the optional TLVs in the LLDP MED set transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) on a specific port.
show lldp med	Displays a summary of the current LLDP-MED configuration.

poe

Use this command to configure the port as a Power-Sourcing Equipment (PSE)-capable interface. Use the `no` form of the command to configure as a non-PSE interface.

poe

no poe

Default

PoE is enabled on PoE-capable ports (not applicable to non-PoE ports).

Command Modes

Global Config

Interface Config

Usage Guidelines

Use the command in Global Config mode to enable PSE functionality on all PSE-capable ports. Use the command in Interface Config mode to configure PSE functionality on a specific port.

Related Commands

Command	Description
lldp med transmit-tlv **lldp med transmit-tlv all**	Specifies the TLVs in the LLDP MED set transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) on a specific port or on all ports.
poe power management	Sets the power management as dynamic or static.
poe power limit	Sets the method for power management.
poe priority	Configures the port priority level for the delivery of power to an attached device.
poe usagethreshold	Configures the system power usage threshold level at which a trap is generated and a message is logged.
poe reset	Configures the PoE functionality to reinitialize automatically on encountering a fault condition.
poe powered-device describe	Adds a comment or description of the powered device type to enable the operator to remember what is attached to the interface.
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port configuration	Displays per-port PoE configuration.
show poe port	Displays per-port PoE status.

poe power limit

Use this command to set the power management method. Use the `no` form of the command to reset the method to the default.

poe power limit {{**dot3af** | **user-def** *3000-16200*}} | [**lldp-med**]}

no poe power limit

Syntax Descriptions

Parameter	Description
dot3af	The maximum power that can be delivered by the PSE port is limited by the detected IEEE 802.3af class.
user-def	The maximum power that can be delivered by the PSE port is specified by the user. The value can be in the range of 3W (*3000*) to 16.2W (*16200*).
lldp-med	The maximum power that can be delivered by the PSE port is limited by the value in LLDP-MED TLVs received from a powered device. The value specified by the powered device should be in the range of 3–16.2 watts. If it is not in the range, then the default value of 16.2 watts is configured, unless the **dot3af** is specified or a different user-defined value is configured.

Modes

Global Config

Interface Config

Default

PoE power is limit by the port. The value is 16.2 watts.

Usage Guidelines

The keywords **lldp-med** and **dot3af**, and the keywords **lldp-med** and **user-def**, can be enabled simultaneously. If an LLDP-MED TLV is received from the powered device, that value is given priority over a dot3af or user-defined value.

If only **lldp-med** is enabled, and no LLDP-MED TLV is received from the powered device, then the default value of 16.2 watts is configured.

Related Commands

Command	Description
poe power management	Sets the power management as dynamic or static.

Command	Description
poe power limit	Sets the method for power management.
poe priority	Configures the port priority level for the delivery of power to an attached device.
poe usagethreshold	Configures the system power usage threshold level at which a trap is generated and a message is logged.
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port configuration	Displays per-port PoE configuration.
show poe port	Displays per-port PoE status.

poe power management

Use this command to set the power management as dynamic or static. Use the **no** form of the command to reset it to its default value.

poe power management {**dynamic-with-priority** | **static- with-priority**}

no poe power management

Syntax Descriptions

Parameter	Description
dynamic-with-priority	Power management is done by the PoE controller. Power is supplied to devices as long as the consumption is within the configured limit and priority. There is no pre-allocation of power. A port with a higher port priority is given preference when the switch supplies power to multiple ports. If two or more port priorities are equal, the port with the lower port number is given preference.

Parameter	Description
static-with-priority	Power management is done by the PoE controller. The switch pre-allocates power based on the configured power limit and the priority of the port. A port with a higher port priority is given preference when the switch supplies power to multiple ports. If two or more port priorities are equal, the port with the lower port number is given preference.

Default

Dynamic-with-priority power management is enabled.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
poe power limit	Sets the method for power management.
poe priority	Configures the port priority level for the delivery of power to an attached device.
poe usagethreshold	Configures the system power usage threshold level at which a trap is generated and a message is logged.
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port configuration	Displays per-port PoE configuration.
show poe port	Displays per-port PoE status.

poe powered-device describe

Use this command to add a comment or description of the powered device type to enable the operator to remember what is attached to the interface. To remove the description, use the `no` form of this command. This is applicable to powered devices attached to the PSE ports on the switch.

NOTE The command can be used in Global Config mode to configure all ports and can be used in Interface mode to configure a specific port.

poe powered-device describe *pd-type*

no poe powered-device describe

Syntax Descriptions

Parameter	Description
pd-type	The type of powered device attached to the interface. The range is 1–24 characters.

Modes

Global Config

Interface Config

Examples

The following example shows entering into Interface Config mode and adding a description for port e1.

```
switch(config)#interface ethernet e1
switch(interface e1)#poe powered-device describe IP-phone
```

Command	Description
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port configuration	Displays per-port PoE configuration.

poe priority

The switch might not be able to supply power to all connected PoE devices. Port priority determines which ports supply power when adequate power capacity is not available for all enabled ports. Use this command to configure the port priority level for the delivery of power to an attached device. Use the `no` form of the command to reset the priority value to the default.

NOTE The command can be used in Global Config mode to configure all ports and can be used in Interface mode to configure a specific port.

poe priority {**critical** | **high** | **low**}

no poe priority

Syntax Descriptions

Parameter	Description
critical	The port is assigned the highest prioritized when PoE power requests exceed the available supply.
high	The port is assigned a high priority when PoE power requests exceed the available supply.
low	The port is assigned a low priority when PoE power requests exceed the available supply.

Command Modes

Global Config

Interface Config

Usage Guidelines

For ports that have the same priority level, the lower-numbered port is given higher priority. For a system delivering peak power to a certain number of devices, if a new device is attached on a higher-priority port, power to a device on a lower-priority port is shut down.

Default

All ports are configured with low priority.

Command	Description
poe power management	Sets the power management as dynamic or static.
poe power limit	Sets the method for power management.
poe priority	Configures the port priority level for the delivery of power to an attached device.
poe usagethreshold	Configures the system power usage threshold level at which a trap is generated and a message is logged.
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port configuration	Displays per-port PoE configuration.
show poe port	Displays per-port PoE status.

poe reset

Use this command to enable PoE to reinitialize automatically upon encountering a fault condition. If this is disabled, then administrator intervention is required to reinitialize the port. A fault condition is reported by the PoE controller in PSE Port Detection Status parameter. The possible fault conditions are Fault and Other Fault. Use the `no` form of the command to remove automatic reinitialization on a port.

NOTE The command can be used in Global Config mode to configure all ports and can be used in Interface mode to configure a specific port.

```
poe reset

no poe reset
```

Modes

Global Config

Interface Config

Default

PoE auto-reset is enabled.

Command	Description
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port configuration	Displays per-port PoE configuration.
show poe port	Displays per-port PoE status.

poe usagethreshold

Use this command to configure the system power usage threshold level at which a trap is generated and a message is logged.

poe usagethreshold ***1-100***

no poe usagethreshold

Syntax Descriptions

Parameter	Description
1-100	The power threshold percentage of total available system power.

Default

- PoE usage threshold level is 95%

Command Modes

Global Config

Related Commands

Command	Description
poe power management	Sets the power management as dynamic or static.
poe power limit	Sets the method for power management.

Command	Description
poe threshold	Configures the system power usage threshold level at which a trap is generated and a message is logged.
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port configuration	Displays per-port PoE configuration.
show poe port	Displays per-port PoE status.

show poe

Use this command to display the global configuration of the switch, and information about each device connected to the PSE port(s).

show poe

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show poe

Nominal Power................................. 180
Threshold Power............................... 162
Total Power Consumed.......................... 0
Usage Threshold............................... 90
Power Management Mode......................... dynamic-with-priority

Port Configuration

Intf   Description
------ ------------------------
e1     IP Phone
e2
e3
e4
e5
e6
e13
e14    Wireless AP
e15
e16
e17
e18
```

Related Commands

Command	Description
show poe port configuration	Displays PoE configuration for a port or all ports.
show poe port info	Displays PoE status for a port or all ports.
show poe port statistics	Displays PoE statistics for a port or all ports.

show poe port configuration

Use this command to display PoE configuration for a port or all ports.

show poe port configuration {**all** | *interface*}

Syntax Descriptions

Parameter	Description
all	Displays PoE configuration for all ports.
interface	Displays PoE configuration for the specified port.

Command Modes

Privileged Exec

Examples

The following shows sample output for all ports on which PoE operation is available.

```
(switch1) #show poe port configuration all

     Admin    Priority  Power     Power               Port  Detection
Intf Mode               Limit     Limit               pair  Type
                        (W)       Type
---- ------- --------- -------- ----------------- ----- -----------------
e1   Enable   low       15.400    class               alt-a 4ptdot3af
e2   Enable   low       15.400    class               alt-a 4ptdot3af
e3   Enable   low       15.400    class               alt-a 4ptdot3af
```

```
e4   Enable  low      15.400  class              alt-a 4ptdot3af
e5   Enable  low      15.400  class              alt-a 4ptdot3af
e6   Enable  low      15.400  class              alt-a 4ptdot3af
e13  Enable  low      15.400  class              alt-a 4ptdot3af
e14  Enable  low      15.400  class              alt-a 4ptdot3af
e15  Enable  low      15.400  class              alt-a 4ptdot3af
e16  Enable  low      15.400  class              alt-a 4ptdot3af
e17  Enable  low      15.400  class              alt-a 4ptdot3af
e18  Enable  low      15.400  class              alt-a 4ptdot3af
```

The following shows sample output for a specific port.

```
(switch1) #show poe port configuration e1

Interface.................................... e1
Description..................................
Admin Mode................................... Enable
Priority..................................... low
Power Limit(W)............................... 15.400
Power Limit Type............................. class
Port Pair.................................... alt-a
Detection Type............................... 4ptdot3af
```

Related Commands

Command	Description
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port info	Displays PoE status for a port or all ports.
show poe port statistics	Displays PoE statistics for a port or all ports.

show poe port info

Use this command to display PoE status for a port or all ports.

show poe port info {**all** | *interface*}

Syntax Descriptions

Parameter	Description
all	Displays PoE status for all ports.
interface	Displays PoE status for the specified port.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show poe port info all

                       Output   Output
Intf   Class   Power   Current  Voltage   Temperature     Status
               (mW)     (mA)     (volt)       (C)
------ ------ -------- -------- -------- ------------- ------------
e1        0    00000    0000      00          0          Searching
e2        0    00000    0000      00          0          Searching
e3        0    00000    0000      00          0          Searching
e4        0    00000    0000      00          0          Searching
e5        0    00000    0000      00          0          Searching
e6        0    00000    0000      00          0          Searching
e13       0    00000    0000      00          0          Searching
e14       0    00000    0000      00          0          Searching
e15       0    00000    0000      00          0          Searching
e16       0    00000    0000      00          0          Searching
e17       0    00000    0000      00          0          Searching
e18       0    00000    0000      00          0          Searching
```

Related Commands

Command	Description
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).
show poe port configuration	Displays PoE configuration for a port or all ports.
show poe port statistics	Displays PoE statistics for a port or all ports.

show poe port statistics

Use this command to display PoE statistics for an interface or all interfaces.

show poe port statistics {**all** | *interface*}

Syntax Descriptions

Parameter	Description
all	Displays PoE statistics for all ports.
interface	Displays PoE statistics for the specified port.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show poe port statistics all

         MPS      Power     Over              Invalid
 Intf   Absent   Denied    Load     Short   Signature
------ -------- -------- -------- -------- ------------
e1         0        0        0        0       1583117
e2         0        0        0        0       1583110
e3         0        0        0        0       1572025
e4         0        0        0        0       1572172
e5         0        0        0        0       1541835
e6         0        0        0        0       1541945
e13        0        0        0        0       1583102
e14        0        0        0        0       1583067
e15        0        0        0        0       1572154
e16        0        0        0        0       1572088
e17        0        0        0        0       1541959
e18        0        0        0        0       1541924
```

Related Commands

Command	Description
show poe	Displays the global configuration, and information about each device connected to the PSE port(s).

Command	Description
show poe port configuration	Displays PoE configuration for a specific port or all ports.
show poe port info	Displays PoE status for a specific port or all ports.

Switch Management Access Control

The following commands configure user login information and access settings for the switch management interfaces. Switch management can be performed through the web-based interface, a command line interface (CLI), or SNMP.

This section contains the following subsections:

- **Authentication Methods**
- **User Logins and Passwords**
- **Management Access—General**
- **HTTP Access**
- **Telnet Access**
- **SSH Access**
- **Console Access**
- **Management Access Lists**

Authentication Methods

ip http authentication

Use this command to specify authentication methods for HTTP server users. To return to the default, use the `no` form of this command. The supported methods are `local` or `RADIUS`.

ip http authentication *method1* [*method2*]

no ip http authentication

Syntax Descriptions

Parameter	Description
method1	The primary authentication method to use, **`local`** or **`RADIUS`**.
method2	The secondary authentication method to use if the primary method returns an error, **`local`** or **`RADIUS`**.

Default

method1—**`local`** authentication

Command Modes

Global Config

Examples

The following example configures HTTP authentication using a RADIUS server and, if the RADIUS server is not available, using a locally administered user names and passwords.

```
(switch) (Config)#ip http authentication radius
```

Related Commands

Command	Description
radius server host	Configures the IP address or DNS for a RADIUS server.
show authentication methods	Displays information about the authentication methods.

login authentication

Use this command to specify the login authentication method for a line (console and Telnet) access mode. To return to the default list configuration, use the **no** form of this command. The supported methods are **local**, **RADIUS**, or **none**.

If two methods of authentication are defined, then the second method is used only if the first method returns an error—not if there is an authentication denial from the first method.

login authentication ***method1*** **[*method2*]**

no login authentication

Syntax Descriptions

Parameter	Description
method1	The primary authentication method to use, which can be **local**, **RADIUS**, or **none**.
method2	The secondary authentication method to use if the primary method returns an error.

Default

method1—**local** authentication

Command Modes

Line Console Config

Line Telnet Config

Examples

The following example specifies the default authentication method for console access.

```
(Switch) (config)#line console
(Switch) (config-line)#login authentication radius
```

The following example specifies the default authentication method for Telnet access.

```
(Switch) (config)#line telnet
(Switch) (config-telnet)#login authentication radius
```

Related Commands

Command	Description
ip http authentication	Specifies authentication methods for HTTP server users.
radius server host	Configures the IP address or DNS for a RADIUS server.
show authentication methods	Displays information about the authentication methods.

show authentication methods

Use this command to display information about the authentication methods.

show authentication methods

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
(switch)#show authentication methods

Line          Method
-------      -----------------
Console      :local        radius     none
Telnet       :radius

HTTP         :local
DOT1X        :
```

Related Commands

Command	Description
ip http authentication	Specifies authentication methods for HTTP server users.
login authentication	Specifies the login authentication method list for a line (console and Telnet) access mode.

User Logins and Passwords

password

The currently logged-in user can use this command to change the password. This command can be used after the password has aged-out or at any time to change the user's password. The user is prompted to enter the old password and the new password. The change is effective upon the next log-in.

```
password
```

Command Modes

Privileged Exec

Related Commands

Command	Description
passwords min-length	Enforces a minimum password length for local users.
passwords aging	Implement aging on passwords for local users.
show passwords configuration	Displays the configured password management settings.

passwords aging

Use this command to implement aging on passwords for local users. When a user's password expires, the user is prompted to change it before logging in again. Use the `no` form of the command to reset it to the default value (180 days). If it is set to 0, password aging is disabled.

```
passwords aging 0-365

no passwords aging
```

Syntax Descriptions

Parameter	Description
0-365	The number of days. The range is 0–365.

Default

aging—180 days

Command Modes

Global Config

Related Commands

Command	Description
passwords min-length	Enforces a minimum password length for local users.
password	Allows a user to change their password after it has expired.
show passwords configuration	Displays the configured password management settings.

passwords min-length

Use this command to enforce a minimum password length for local users. Use the `no` form of the command to reset it to its default value.

passwords min-length ***min-length***

no passwords min-length

Syntax Descriptions

Parameter	Description
min-length	The minimum number of characters that a password must have. The range is 8-64.

Default

min length—8 characters

Command Modes

Global Config

Related Commands

Command	Description
passwords aging	Implement aging on passwords for local users.
password	Allows a user to change their password after it has expired.
show passwords configuration	Displays the configured password management settings.

passwords strength-check

Use this command to enable the switch to perform the configured password strength checks when users log in. The strength checks are configured separately (see **Related Commands**). Use the `no` form of this command to disable password strength checking.

```
passwords strength-check
no passwords strength-check
```

Default

This feature is enabled.

Command Modes

Global Config

Related Commands

Command	Description
passwords strength check-username	Configures the switch to prevent users from including their user names in their passwords when they create or change their password.
passwords strength exclude-keyword	Configures the switch to check whether preconfigured keywords are used in a password when a user attempts to create or change the password.

Command	Description
passwords strength maximum repeated-characters	Configures the switch to check whether any character in the password is repeated more that three consecutive times.

passwords strength check-username

Use this command to prevent users from including their user names in their passwords when they create or change them.

This security check is enforced only when the passwords strength check feature is enabled (see the **passwords strength-check** command).

Use the `no` form of this command to disable checking for user names in passwords.

passwords strength check-username

no password strength check-username

Default

This feature is enabled.

Command Modes

Global Config

Usage Guidelines

When you enable this feature, the following warning displays if one or more currently configured users violates the user name condition.

```
Warning: Not all user(s) passwords comply with the current password strength
restriction(s).
```

Related Commands

Command	Description
passwords strength exclude-keyword	Configures the switch to check whether preconfigured keywords `cisco` and `ocsic` are used in a password when a user attempts to create or change the password.

Command	Description
passwords strength maximum repeated-characters	Configures the switch to check whether any character in the password is repeated consecutively more than three times.
passwords strength-check	Enables the switch to perform the configured password strength checks when users log in.

passwords strength exclude-keyword

Configures the switch to check whether preconfigured keywords are used in a password when a user attempts to create or change the password. The preconfigured keywords are **`cisco`** and **`ocsic`**.

This security check is enforced only when the passwords strength check feature is enabled (see the **passwords strength-check** command).

Use the **`no`** form of this command to disable checking for keyword usage in passwords.

password strength exclude-keyword

no password strength exclude-keyword

Default

This feature is disabled.

Command Modes

Global Config

Usage Guidelines

When you enable this feature, the following warning displays if one or more currently configured users violates the keyword strength setting.

```
Warning: Not all user(s) passwords comply with the current password strength
restriction(s).
```

Related Commands

Command	Description
passwords strength check-username	Configures the switch to prevent users from including their user names in their passwords when they create or change them.
passwords strength maximum repeated-characters	Configures the switch to check whether any character in the password is repeated consecutively more than three times.
passwords strength-check	Enables the switch to perform the configured password strength checks when users log in.

passwords strength maximum repeated-characters

Use this command to configure the switch to check whether any character in the password is repeated consecutively more than three times.

This security check is enforced only when the passwords strength check feature is enabled (see the **passwords strength-check** command).

Use the `no` form of this command to disable checking for repeated characters in passwords.

password strength maximum repeated-characters

no password strength maximum repeated-characters

Default

This feature is disabled.

Command Modes

Global Config

Usage Guidelines

When you enable this feature, the following warning displays if one or more currently configured users violates the maximum repeated characters setting.

```
Warning: Not all user(s) passwords comply with the current password strength
restriction(s).
```

Related Commands

Command	Description
passwords strength check-username	Configures the switch to prevent users from including their user names in their passwords when they create or change them.
passwords strength exclude-keyword	Configures the switch to check whether preconfigured keywords are used in a password when a user attempts to create or change the password.
passwords strength-check	Enables the switch to perform the configured password strength checks when users log in.

show loginsession

Use this command to display the current login sessions to the to the switch.

show loginsession {**long**}

Syntax Descriptions

Parameter	Description
long	Use the `long` parameter to display full-length usernames. Without this keyword, the usernames are truncated in the output.

Command Modes

Global Config

Examples

In version 1.0.1.nn:

```
(switch121D4E)  #show loginsession
ID     User Name      Connection From            Idle Time   Session Time Session Type
--    --------------  ---------------------      ----------- ------------ ------------
00    cisco           EIA-232                    00:00:00    00:03:49     Serial Port
```

In version 1.0.2.nn and higher:

```
(switch122D4E) #
```

```
(switch122D4E) #show loginsession

ID User Name      Connection From Idle Time Session Time Session Type Auth Method
-- ------------- --------------- --------- ------------ ------------ -----------
00 cisco          EIA-232         00:00:00  00:02:39     Serial Port  Local
```

ID	Login session ID.
System Name	A name used to identify the switch. The factory default is blank.
Username	The name the user entered to log on to the system.
Connection From	Time this session has been idle.
Idle Time	Total time this session has been connected.
Session Type	Type of session, such as HTTP, HTTPS, telnet, serial, or SSH.
Authentication Method	The authentication method can be **`Local`** or **`RADIUS`**.

Related Commands

Command	Description
passwords min-length	Enforces a minimum password length for local users.
passwords aging	Implement aging on passwords for local users.
password	Allows a user to change their password after it has expired.
show users	Displays the configured user names and their settings.

show passwords configuration

Use this command to display the configured password management settings.

show passwords configuration

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
Switch) #show passwords configuration

Passwords Configuration
-----------------------
Password Strength Check Disabled
Minimum Password Length........................ 8
Maximum Password Repeated Characters........... Disabled
Minimum Password Character Classes............. Disabled
Password Exclude User Name..................... Disabled
Password Exclude Keywords...................... Disabled
Password History............................... 0
Password Aging (days).......................... 0
```

Related Commands

Command	Description
passwords min-length	Enforces a minimum password length for local users.
passwords aging	Implements aging on passwords for local users.

show user accounts

This command displays the local user status with respect to user account lockout and password aging.

show user accounts [**long**]

Syntax Descriptions

Parameter	Description
long	Displays the complete user names. Without this keyword, the long user names are truncated in the output.

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
(switch) #show users accounts

 UserName                 Privilege   Password          Password          Lockout
                                       Aging          Expiry date
--------------------     ---------  ----------   ---------------------   -------
cisco                    15         180          Jun 30 1970 00:00:43    False
jonstew                  15         180          Jul 07 1970 08:32:36    False
```

User Name	The local user account user name.
Privilege	The privilege level of the users. All users are assigned the highest privilege level (15) by default.
Password Aging	The number of days before the password expires.
Password Expiry date	The date when the password is scheduled to expire.
Lockout	Indicates `True` if the user is currently locked out due to an aged-out password or `False` if not locked out.

Related Commands

Command	Description
show users	Displays the configured user names and their settings.

show users

Use this command to display the management users that are currently accessing the switch through one of the user interfaces (serial console, Telnet, web, or SNMP).

show users [long]

Syntax Descriptions

Parameter	Description
long	Displays the complete user names. Without this keyword, the long user names are truncated in the output.

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
Switch) #show users

User Name              Protocol    Location
--------------------   ----------  -----------------------
cisco                  Serial      EIA-232
```

User Name	The name the user enters to login using serial, port, Telnet, web and SNMP.
Protocol	Shows the protocol the user is using to access the switch.
Location	Shows the IP address of the user system.

Related Commands

Command	Description
show user accounts	Displays the local user status with respect to user account lockout and password aging.

show users login-history

Use this command to display information about the login history of users.

show users login-history

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
(switch)#show users login-history

Login Time           Username  Protocol  Location
-------------------- --------- --------- ---------------
Jan 19 2005 08:23:48 Bob       Serial
Jan 19 2005 08:29:29 Robert    HTTP      172.16.0.8
Jan 19 2005 08:49:52 Betty     Telnet    172.16.1.7
```

Login Time	The date and time the user logged into switch.
Username	User name.
Protocol	Serial/Telnet/HTTP.
Location	IP address for Telnet and HTTP.

Related Commands

Command	Description
show users	Displays the configured user names and their settings.

username

Use this command to add a new user to the local user database. Use the **no** form of the command to remove the user.

username *name* {**password** *password* [**encrypted**] | **no password**} [**override-complexity check**]

no username *name*

Syntax Descriptions

Parameter	Description
name	The name of the user. The range is 1-32 characters.
password	The authentication password for the user. The range is 8–64 characters. This value can be zero if the **no passwords min-length** command has been executed.

Parameter	Description
encrypted	The password as entered is an encrypted value, which has been copied from another switch where it was encrypted.
nopassword	Specifies that the user has no passwords.
override-complexity check	Specifies that the password will not be checked to meet any password criteria configured using the **passwords strength-check** commands.

Defaults

- Default user: **cisco**
- Default password for **cisco** user: **cisco**

Command Modes

Global Config

Usage Guidelines

The **cisco** user can not be deleted.

Users created using this command have full administrative privileges.

Examples

The following example configures a user name and password with encryption.

```
Switch(config)#username "user1" password fb3604df5a109405b2d79ecb06c47ab5
encrypted
```

Related Commands

Command	Description
passwords min-length	Enforces a minimum password length for local users.
passwords aging	Implement aging on passwords for local users.
password	Allows a user to change their password after it has expired.
show users	Displays the configured user names and their settings.

Management Access—General

network mgmt_vlan

Use this command to the configure management VLAN ID. Use the `no` form of the command to reset it to the default value (VLAN 1).

network mgmt_vlan *1-4094*

no network mgmt_vlan

Syntax Descriptions

Parameter	Description
1-4094	The VLAN ID. Access to the management interfaces is restricted to the specified VLAN.

Default

The default VLAN ID for management access is 1.

Command Modes

Privileged EXEC

Related Commands

Command	Description
show network	Displays configuration settings associated with the switch's management interface.

show network

Use this command to display configuration settings associated with the switch management interface.

show network

Command Modes

Privileged Exec

Usage Guidelines

The management interface is the logical interface used for in-band connectivity with the switch via any of the front panel ports. The configuration parameters associated with the switch management interface do not affect the configuration of the front panel ports through which traffic is switched. The management interface is always considered to be up, whether or not any member ports are up; therefore, the show network command will always show Interface Status as Up.

Examples

The following shows sample output for the command

```
(switch) #show network

Interface Status............................... Always Up
IP Address..................................... 10.131.12.78
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.131.12.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................ fe80::205:5ff:fe0a:201/64
Burned In MAC Address.......................... 00:05:05:0A:02:01
Configured IPv4 Protocol....................... DHCP
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Management VLAN ID............................. 1
```

HTTP Access

The following commands configure user access to the management interface through HTTP.

ip http port

Use this command to specify the TCP port for use by a web browser to configure the switch. To use the default TCP port, use the `no` form of this command.

ip http port ***1025-65535***

no ip http port

Syntax Descriptions

Parameter	Description
1025-65535	The HTTP protocol port number.

Default

port—80

Command Modes

Privileged Exec

Related Commands

Command	Description
show ip http	Displays the HTTP server configuration.
show network	Displays configuration settings associated with the switch's management interface.

ip http server

Use this command to enable the switch to be configured, monitored, or modified from a browser. To disable this function use the `no` form of this command.

ip http server

no ip http server

Default

HTTP access is enabled.

Command Modes

Privileged Exec

Related Commands

Command	Description
show ip http	Displays the HTTP server configuration.
show network	Displays configuration settings associated with the switch's management interface.

ip http session soft-timeout

Use this command to configure the soft timeout for HTTP sessions. When this timeout expires the user will be forced to reauthenticate. This timer begins on initiation of the web session and is restarted with each access to the switch. Use the `no` form of this command to reset the timeout to the defaults.

ip http session soft-timeout ***1-60***

no ip http session soft-timeout

Syntax Descriptions

Parameter	Description
1-60	The timeout in minutes.

Default

timeout—10 minutes

Command Modes

Privileged Exec

Related Commands

Command	Description
ip http server	Enables the switch to be configured, monitored, or modified from a browser.
show ip http	Displays the HTTP server configuration.

show ip http

Use this command to display the HTTP server configuration.

show ip http

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show ip http
HTTP Mode (Unsecure)................................. Enabled
HTTP Server Port....................................... 80
Maximum Allowable HTTP Sessions................ 5
HTTP Session Soft Timeout.......................... 10 minutes
```

Related Commands

Command	Description
ip http server	Enables the switch to be configured, monitored, or modified from a browser.
ip http session soft-timeout	Configures the soft timeout for HTTP sessions.

Telnet Access

The following commands configure user access to the management interface and outbound connections through Telnet.

ip telnet server enable

Use this command to enable the Telnet Server Admin Mode, in which the **telnet** command can be used to establish a telnet connection to a remote host.

Use the `no` form of command to disable the Telnet Server Admin Mode and close any existing telnet connections to remote hosts.

ip telnet server enable

no ip telnet server enable

Default

Telnet Server Admin Mode is disabled.

Command Modes

Privileged Exec

Related Commands

Command	Description
telnet	Establishes a new outbound Telnet connection to a remote host.
show network	Displays configuration settings associated with the switch's management interface.
show telnetcon	Displays Telnet configuration and status information.

telnet

Use this command to establish a new outbound Telnet connection to a remote host.

telnet {*ip-address* | *hostname*} *port* [**debug**] [**line**] [**localecho**]

Syntax Descriptions

Parameter	Description
ip address	The IP address of the Telnet server.
hostname	The hostname of the Telnet server. Ensure that a DNS server is configured if a hostname is specified.
port	The logical port number for Telnet communications in the range of 1025 to 65535.
debug	Displays the currently enabled Telnet options.
line	Sets the outbound Telnet operational mode as line mode. By default, the operational mode is character mode.
localecho	Enables keystrokes entered on the local device to be echoed back to the screen immediately.

Defaults

- No *ip address* or *hostname*.
- *Port*—23

- **line**—Character mode
- **noecho**—Disabled

Command Modes

Privileged Exec

Related Commands

Command	Description
ip telnet server enable	Enables Telnet connections to the system and enables the Telnet Server Admin Mode.
show network	Displays configuration settings associated with the switch's management interface.
show telnetcon	Displays Telnet configuration and status information.

telnetcon timeout

Use this command to set the Telnet connection session timeout value in minutes. A session is active as long as the session has not been idle for the value set. Use the `no` form of this command to reset the timeout to the default.

telnetcon timeout *1-160*

no telnetcon timeout

Syntax Descriptions

Parameter	Description
1-160	The timeout value in minutes.

Default

timeout—5 minutes

Command Modes

Privileged Exec

Usage Guidelines

When the timeout value is changed, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Related Commands

Command	Description
ip telnet server enable	Enables Telnet connections to the system and enables the Telnet Server Admin Mode.
telnet	Establishes a new outbound Telnet connection to a remote host.
show network	Displays configuration settings associated with the switch's management interface.
show telnetcon	Displays Telnet configuration and status information.

show telnetcon

Use this command to display Telnet configuration and status information, such as the configured timeout, the number of allowed sessions, and the administrative mode for making outbound Telnet connections from the switch.

show telnetcon

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show telnetcon

Remote Connection Login Timeout (minutes)...... 5
Maximum Number of Remote Connection Sessions... 2
Allow New Telnet Sessions...................... Yes
Telnet Server Admin Mode....................... Disable
```

Related Commands

Command	Description
ip telnet server enable	Enables Telnet connections to the system and enables the Telnet Server Admin Mode.
telnet	Establishes a new outbound Telnet connection to a remote host.
show network	Displays configuration settings associated with the switch's management interface.

SSH Access

The following commands configure user access to the management interface through SSH.

copy nvram:sshkey-dsa

Use this command to download a DSA SSH host key. A key cannot be downloaded while SSH is enabled or sessions are active.

copy *url* **nvram:sshkey-dsa**

Command Modes

Privileged EXEC

Related Commands

Command	Description
crypto key generate dsa	Generates a DSA key pair for SSH.

copy nvram:sshkey-rsa1

Use this command to download an RSA1 SSH host key. A key cannot be downloaded while SSH is enabled or sessions are active.

copy *url* **nvram:sshkey-rsa1**

Command Modes

Privileged EXEC

Related Commands

Command	Description
copy nvram:sshkey-rsa2	Downloads an RSA2 SSH host key.
crypto key generate rsa	Generates an RSA key pair for SSH.

copy nvram:sshkey-rsa2

Use this command to download an RSA2 SSH host key. A key cannot be downloaded while SSH is enabled or sessions are active.

```
copy url nvram:sshkey-rsa2
```

Command Modes

Privileged EXEC

Related Commands

Command	Description
copy nvram:sshkey-rsa1	Downloads an RSA1 SSH host key.
crypto key generate rsa	Generates an RSA key pair for SSH.

crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files overwrite any existing generated or downloaded DSA key files. Use the `no` form of this command to delete the DSA key files from the device.

```
crypto key generate dsa
```

no crypto key generate dsa

Command Modes

Global Config

Related Commands

Command	Description
copy nvram:sshkey-dsa	Downloads a DSA SSH host key.

crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files overwrite any existing generated or downloaded RSA key files. Use the `no` form of the command to delete the RSA key files from the device.

crypto key generate rsa

no crypto key generate rsa

Command Modes

Global Config

Related Commands

Command	Description
copy nvram:sshkey-rsa1	Downloads an RSA1 SSH host key.
copy nvram:sshkey-rsa2	Downloads an RSA2 SSH host key.

ip ssh protocol

Use this command to set the available protocol levels (versions) for SSH. SSH version 1, version 2, or both can be set. The specified level(s) are enabled and any unspecified level is disabled.

ssh protocol {{1 | 2} | {1 2}}

Default

Version 1 and 2 are set.

Command Modes

Privileged EXEC

Examples

The following example sets protocol level 1 (and unsets level 2 if it was previously set).

```
(switch) #ip ssh protocol 1
```

The following example sets both levels:

```
(switch) #ip ssh protocol 1 2
```

Related Commands

Command	Description
ip ssh server enable	Enables management access through SSH.
sshcon maxsessions	Configures the number of remote SSH connections allowed.
sshcon timeout	Configures the SSH Login Inactivity Timeout in minutes.
show ip ssh	Shows SSH configuration information.

ip ssh server enable

Use this command to enable management access through SSH. Use the `no` form of this command to disable access through SSH.

ip ssh server enable

no ip ssh server enable

Default

SSH access is disabled.

Command Modes

Privileged EXEC

Related Commands

Command	Description
ip ssh protocol	Sets or removes protocol levels (versions) for SSH.
sshcon maxsessions	Configures the number of remote SSH connections allowed.
sshcon timeout	Configures the SSH Login Inactivity Timeout in minutes.
show ip ssh	Shows SSH configuration information.

sshcon maxsessions

Use this command to configure the number of remote SSH connections allowed. Use the `no` form of the command to return the maximum to the default (2 sessions).

sshcon maxsessions *0-2*

no sshcon maxsessions

Default

maxsessions—2

Command Modes

Privileged EXEC

Related Commands

Command	Description
ip ssh server enable	Enables management access through SSH.
ip ssh protocol	Sets or removes protocol levels (versions) for SSH.

Command	Description
sshcon timeout	Configures the SSH Login Inactivity Timeout in minutes.
show ip ssh	Shows SSH configuration information.

sshcon timeout

Use this command to set the SSH connection timeout value in minutes. A session is active as long as the session has not been idle for the value set. Use the `no` form of this command to reset the timeout to the default.

sshcon timeout *1-160*

no sshcon timeout

Syntax Descriptions

Parameter	Description
1-160	The timeout value in minutes.

Default

timeout—10 minutes

Command Modes

Privileged Exec

Usage Guidelines

When the timeout value is changed, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Related Commands

Command	Description
ip ssh server enable	Enables management access through SSH.
ip ssh protocol	Sets or removes protocol levels (versions) for SSH.

Command	Description
sshcon maxsessions	Configures the number of remote SSH connections allowed.
show ip ssh	Shows SSH configuration information.

show ip ssh

Use this command to display SSH settings.

show ip ssh

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show ip ssh
SSH Configuration
Administrative Mode: .......................... Enabled
Protocol Levels: .............................. Versions 1 and 2
SSH Sessions Currently Active: ................ 0
Max SSH Sessions Allowed: ..................... 2
SSH Timeout: .................................. 5
Keys Present: ................................. DSA RSA
Key Generation In Progress: ................... None
```

Console Access

This section describes the commands you use to configure properties for the console connection to the switch CLI.

line console

Use this command in Global Config mode to enter the Line (Console) Config Mode, where you set properties of the console port.

line console

Command Modes

Global Mode

Related Commands

Command	Description
serial baudrate	Specifies the communication rate of the console port.
serial databits	Specifies the number of data bits per character for the console connection.
serial parity	Sets the parity for the console connection.
serial stopbits	Sets the number of stop bits for the console connection.
show serial	Displays serial port communication settings.

serial baudrate

Use this command to specify the communication rate of the console port. The supported rates are 9600, 38400, and 115200. Use the `no` form of the command to reset it to the default value.

serial baudrate {**9600** | **38400** | **115200**}

no serial baudrate

Default

baud rate—115200

Command Modes

Line (Console) Config Mode

Related Commands

Command	Description
serial databits	Specifies the number of data bits per character for the console connection.
serial parity	Sets the parity for the console connection.
serial stopbits	Sets the number of stop bits for the console connection.
show serial	Displays serial port communication settings.

serial databits

Use this command to specify the number of data bits per character for the console connection. Use the `no` form of the command to reset it to the default value.

serial databits {**7** | **8**}

no serial databits

Default

Eight data bits per character

Command Modes

Line (Console) Config Mode

Related Commands

Command	Description
serial baudrate	Specifies the communication rate of the console port.
serial parity	Sets the parity for the console connection.
serial stopbits	Sets the number of stop bits for the console connection.
show serial	Displays serial port communication settings.

serial parity

Use this command to set the parity for the console connection. Use the `no` form of the command to remove the parity setting.

serial parity {**even** | **odd** | **none**}

no serial parity

Default

parity bits—none

Command Modes

Line (Console) Config Mode

Related Commands

Command	Description
serial databits	Specifies the number of data bits per character for the console connection.
serial baudrate	Specifies the communication rate of the console port.
serial stopbits	Sets the number of stop bits for the console connection.
show serial	Displays serial port communication settings.

serial stopbits

Use this command to set the number of stop bits for the console connection. Use the `no` form of the command to reset it to its default value (1).

serial stopbits {**1** | **2**}

no serial stopbits

Default

stop bits—1

Command Modes

Line (Console) Config Mode

Related Commands

Command	Description
serial databits	Specifies the number of data bits per character for the console connection.
serial baudrate	Specifies the communication rate of the console port.
serial parity	Sets the parity for the console connection.
show serial	Displays serial port communication settings.

serial timeout

Use this command to specify the maximum time (in minutes) the system waits for without console activity. A value of `0` indicates that a console can be connected indefinitely. Use the `no` form of this command to reset the timeout to the default.

serial timeout ***0-160***

no serial timeout

Syntax Descriptions

Parameter	Description
1-160	The timeout in minutes.

Default

timeout—5 minutes

Command Modes

Line Config

Related Commands

Command	Description
show network	Displays configuration settings associated with the switch management interface.
show serial	Displays serial port communication settings.

show serial

Use this command to display serial port communication settings.

show serial

Command Modes

Privileged Exec

Examples

The following shows sample output for the command:

```
switch#show serial

Serial Port Login Timeout (minutes)............ 5
Baud Rate (bps)................................ 115200
Character Size (bits).......................... 8
Stop Bits...................................... 1
Parity......................................... none
```

Related Commands

Command	Description
show network	Displays configuration settings associated with the switch's management interface.
show serial	Displays configuration settings associated with the switch's serial console interface.

Management Access Lists

deny

Use this command in Management Access-List Config mode to set conditions for the management access list. This command can take the following forms:

deny interface *interface* [**service** *service*] [**priority** *priority*]

deny ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**service** *service*] [**priority** *priority*]

deny user *username* [**priority** *priority*]

Syntax Descriptions

Parameter	Description
interface	A port number.
service	The service type: **telnet**, **http**, **tftp**, **ssh**, or **snmp**.
priority	Priority for the rule. The range is 1–16.

Parameter	Description
ip-address	The source IP address to deny.
mask	The network mask of the source IP address.
prefix-length	The number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). The range is 0–32 bits.
username	The name of a management user.

Default

No users are denied access.

Command Modes

Access List Config

User Guidelines

Management access must be retained on at least one interface; i.e., if you deny management access to all but one interface, you cannot deny access on the last interface.

Examples

The following example uses the command to allow management access on all the interfaces except for e1 and e2:

```
switch(config)#management access-list mlist
switch(config-macal)#deny interface e1 priority <1-16>
switch(config-macal)#deny interface e2 priority <1-16>
switch(config-macal)#exit
switch(config)#management access-class mlist
```

Related Commands

Command	Description
management access-class	Restrict management connections.
management access-list	Defines an access list for management and enters the access-list configuration mode.

Command	Description
permit	Sets conditions for the management access list.
show management access-list	Displays information about the configured management access list.

management access-class

Use this command in Global Config mode to restrict management connections. To disable restriction, use the `no` form of this command.

NOTE Console access cannot be disabled.

management access-class {**console-only** | *access-list-name*}

no management access-class

Syntax Descriptions

Parameter	Description
console-only	Restricts management access to the serial (console) interface.
access-list-name	Restricts management access to the specified access list name.

Default

Management access is not restricted.

Command Modes

Global Config

Examples

The following example uses the **management access-class** command to restrict access to an access list named *mlist* after the access list has been defined:

```
switch(config)#management access-list mlist
switch(config-macal)#deny interface e1 priority <1-16
switch(config-macal)#deny interface e2 priority <1-16>
switch(config-macal)#permit priority <1-16>
switch(config-macal)#exit
switch(config) #management access-class mlist
```

Related Commands

Command	Description
management access-list	Defines an access list for management and enters the access-list configuration mode.
deny **permit**	Sets conditions for the management access list.
show management access-list	Displays information about the configured management access list.

management access-list

Use this command to define an access list for management and to enter the Access List Config mode. In Access List Config mode, you can configure the denied or permitted access conditions using the **deny** and **permit** commands. To remove an access list, use the `no` form of this command.

management access-list *access-list-name*

no management access-list

Syntax Descriptions

Parameter	Description
access-list-name	The user-defined name of the access list.

Default

No access list.

Command Modes

Global Config

Usage Guidelines

This command enters the access-list configuration mode, where the denied or permitted access conditions with the **deny** and **permit** commands must be defined. If no match criteria are defined, the default is to permit access. If re-entering to 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.

Related Commands

Command	Description
management access-class	Restrict management connections.
deny **permit**	Sets conditions for the management access list.

permit

Use this command in Management Access-List Configuration mode to set conditions for the management access list.

permit interface *interface* [**service** *service*] [**priority** *priority*]

permit ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**service** *service*] [**priority** *priority*]

permit user *username* [**priority** *priority*]

Syntax Descriptions

Parameter	Description
interface	A port number.
service	The service type: telnet, http, tftp, ssh, or snmp.
priority	Priority for the rule. The range is 1–16.
ip-address	The source IP address to deny.
mask	The network mask of the source IP address.

Parameter	Description
prefix-length	The number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). The range is 0–32 bits.
username	The name of a management user.

Default

All users are permitted management access.

Command Modes

Management Access-list Configuration mode

Examples

The following example uses the **permit** command to allow access only to two management interfaces, e1 and e2:

```
switch(config)#management access-list mlist
switch(config-macal)#permit interface e1 priority <1-16>
switch(config-macal)#permit interface e2 priority <1-16>
switch(config-macal)#deny priority <1-16>
switch(config-macal)#exit
switch(config)#management access-class mlist
```

Related Commands

Command	Description
management access-class	Restrict management connections.
management access-list	Defines an access list for management and enters the access-list configuration mode.
deny	Sets conditions for the management access list.

show management access-list

Use this command to display information about the configured management access list.

show management access-list

Command Modes

Privileged Exec

Examples

The following example displays the active management access list.

```
switch#show management access-list a1
--deny interface e5 priority 1
! (Note: all other access implicitly permitted)
```

Related Commands

Command	Description
management access-list	Defines an access list for management and enters the access-list configuration mode.

show management access-class

Use this command to display information about the active management access list.

show management access-class

Command Modes

Privileged Exec

Examples

The following example displays the management access-list information.

```
switch#show management access-class

Management access-class is enabled, using access list mlist
```

Related Commands

Command	Description
management access-class	Restrict management connections.

SNTP and Time Settings

A system clock is used to provide a network-synchronized time-stamping service for switch software events such as message logs. You can configure the system clock manually or configure the switch as an SNTP client that obtains the clock from a server. This section describes the SNTP and time commands.

This section contains the following subsections:

- **Clock Commands**
- **SNTP Commands**

Clock Commands

Use the commands described in this section to view and configure clock settings when the SNTP feature is not used.

clock date

Use this command to set the date and time manually.

clock date *dd/mm/yyyy* **time** *hh:mm:ss*

Syntax Descriptions

Parameter	Description
dd/mm/yyyy	The current date in day:month:year format.
hh:mm:ss	The time in hours:minutes:seconds format.

Defaults

The switch clock initiates with the following values:

- **date**—01/01/1970
- **time**—00:00:00

Command Modes

Global Config

Related Commands

Command	Description
clock timezone	Sets the offset to Coordinated Universal Time (UTC).
show clock	Displays the time and date from the system clock.

clock summer-time

Use this command to enable daylight savings time (DST). Use the `no` form of the command to remove the DST configuration.

clock summer-time

no clock summer-time

Default

DST is not configured by default.

Command Modes

Global Config

Related Commands

Command	Description
clock summertime date	Sets the summertime offset from the universal coordinated time (UTC).
show clock	Displays the time and date from the system clock.

clock summertime date

Use this command to set the summertime offset to the UTC. Use the `no` form of the command to delete the summertime configuration.

clock summer-time date *start-date start-month start-year start-minutes end-date end-month*} *end-year end-minutes* [**offset** *offset*] [**zone** *acronym*]

no clock summer-time

Syntax Descriptions

Parameter	Description
date	The day of the month when DST begins. The range is 1–31.
month	The month when DST begins, specified as the first three letters by name. For example, enter **jan** for January.
year	The current year. The range is 2000–2097.
hh:mm	The time in hours and minutes. The range for *hh* is 0–23 and the range for *mm* is 0–59.
offset	Number of minutes to add during the summertime. The range is 1–1440 minutes.
zone *acronym*	An acronym for the local timezone during DST, up to four characters. The acronym is for display purposes only.

Default

No summertime offset is configured.

Command Modes

Global Config

Examples

The following example configures a summertime date starting on March 14, 2010 at 2:00 A.M, with an offset of 1 hour, ending on November 7, 2010 at 2:00 A.M. This example also names this timezone EDT.

```
(Switch) (Config)#clock summer-time date 14 mar 2010 02:00 7 nov 2010 02:00
offset 60 zone EDT
```

Related Commands

Command	Description
clock summertime recurring	Sets the summertime offset to UTC recursively every year.
show clock	Displays the time and date from the system clock.

Command	Description
clock timezone config dhcp	Sets the clock operational data with the time zone details received from DHCP server.

clock summertime recurring

Use this command to set the summertime (daylight savings time) offset to UTC recursively every year. If the optional parameters are not specified, they are read as either '0' or '\0', as appropriate. Use the `no` form of this command to remove the summertime configuration.

clock summer-time recurring {**usa** | **eu** | {*start-week day month hh:mm week day month hh:mm*}} [**offset** *offset*] [**zone** *acronym*]

no clock summertime

Syntax Descriptions

Parameter	Description
usa	The recurring daylight savings time offset is configured to the U.S. standard.
eu	The recurring summertime offset is configured to the European standard.
week	Week of the month. The range is 1–5, from first to last week.
day	Day of the week, identified by a three-letter abbreviation (for example *sun*, for Sunday).
month	Month, identified by a three-letter abbreviation (for example *Jan*, for January).
hh:mm	Time in 24-hour format in hours and minutes. The range for *hh* is 0–23 and the range for *mm* is 0–59.
offset	The number of minutes to add during the summertime. The range is 1–1440 minutes.
acronym	The acronym, up to four characters, for the time zone to be displayed when summertime is in effect.

Default

No summertime recurring offset is configured.

Command Modes

Global Config

Examples

The following example configures a recurring summertime date starting on the Sunday in the fourth week of March, at 2:00 A.M, with an offset of 1 hour, ending on Sunday in the fourth week of November at 2:00 A.M. This example also names this timezone EDT.

```
(Switch) (Config)#clock summer-time recurring 4 sun mar 02:00 4 sun nov 02:00 offset 60
zone EDT
```

Related Commands

Command	Description
clock summer-time	Enables daylight savings time (DST).
clock summertime date	Sets the summertime offset to UTC.
show clock	Displays the time and date from the system clock.

clock timezone

Use this command to set the offset to Coordinated Universal Time (UTC). Use the `no` form of the command to reset the time zone offset to `0`.

clock timezone hours *hours-offset* [**minutes** *minutes-offset*] [**zone** *acronym*]

no clock timezone

Syntax Descriptions

Parameter	Description
hours-offset	The number of hours earlier or later Greenwich Mean Time. The range is –12 to +13.

Parameter	Description
minutes-offset	The number of minutes to append to the hours offset. The range is 0–59.
acronym	An acronym for the local timezone, up to four characters. The acronym is for display purposes only.

Defaults

- *hours-offset*—0
- *minutes-offset*—0
- *zone acronym*—none

Command Modes

Global Config

Examples

The following example configures a timezone offset of –5 hours and a timezone acronym of EDT.

```
Switch) (Config)#clock timezone hours -5 zone EDT
```

Related Commands

Command	Description
clock date	Sets the date and time manually.
show clock	Displays the time and date from the system clock.

clock timezone config dhcp

This command sets the clock operational data to use the time zone details received from a DHCP server. Use the `no` form of the command to use manually configured time zone details in operational data.

clock timezone config dhcp

no clock timezone config dhcp

Default

The switch does not use DHCP to obtain the timezone.

Command Modes

Global Config

Related Commands

Command	Description
clock timezone	Statically sets the offset to Coordinated Universal Time (UTC), when the DHCP option is not used.
show dhcp client timezone-option	Shows whether the switch has received its timezone information from a DHCP server and the timezone option format in which it was provided.
show clock	Displays the time and date from the system clock.

show clock

Use this command to display the time and date from the system clock. Use the **detail** keyword to show the time zone and summertime configuration.

show clock [detail]

Syntax Descriptions

Parameter	Description
detail	Shows additional timezone and daylight savings time information.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show clock

14:49:56 IST(UTC+5:30) Sep 23 2009
Time source is SNTP
Timezone configuration: static
```

The following shows sample output for the command when the **detail** keyword is specified.

```
(Switch) #show clock detail

14:49:56 IST(UTC+5:30) Sep 23 2009
Time source is SNTP
Timezone configuration: static

 Time zone:
 Acronym is IST
 Offset is UTC+5:30

 Summertime:
 Summer time is disabled
```

Related Commands

Command	Description
sntp server	Configures SNTP unicast servers.
sntp client mode	Enables SNTP client mode and sets the mode to either broadcast or unicast.
clock date	Sets the date and time manually.
clock timezone	Statically sets the offset to UTC, when the DHCP option is not used.
show sntp	Displays SNTP settings and status.

SNTP Commands

You can use the following commands to configure the switch to obtain its time settings from an SNTP server.

sntp authenticate

Use this command to require server authentication for received Network Time Protocol (NTP) traffic. To disable the feature, use the **no** form of this command.

sntp authenticate

no sntp authenticate

Default

SNTP authentication is disabled.

Command Modes

Global Config

Related Commands

Command	Description
sntp server	Configures SNTP unicast servers.
sntp authentication-key	Defines an SNTP authentication key.

sntp authentication-key

Use this command to define an authentication key for SNTP. To remove the authentication key, use the `no` form of this command.

sntp authentication-key [*key-number*] [**md5** *md5*]

no sntp authentication-key [*key-number*]

Syntax Descriptions

Parameter	Description
key number	The value is used to encrypt and decrypt SNTP messages to and from the server
md5	Specifies that the MD5 algorithm is used for encrypting the authentication key.

Default

No authentication key is configured.

Command Modes

Global Config

Related Commands

Command	Description
sntp authentication-key	Defines an SNTP authentication key.

sntp broadcast client poll interval

If the switch is configured as an SNTP broadcast client, it polls the SNTP broadcast servers to synchronize time settings at a specified interval. Use this command to set the poll interval. Use the `no` form of the command to reset it to the default value.

sntp broadcast client poll-interval ***poll-interval***

no sntp broadcast client poll-interval

Syntax Descriptions

Parameter	Description
poll-interval	A value from 3 to 16. This value is used as an exponent of 2 to calculate the poll interval in seconds.

Default

poll-interval—3

Command Modes

Global Config

Related Commands

Command	Description
sntp client mode	Enables Simple SNTP client mode and sets the mode to either broadcast or unicast.
show sntp	Displays SNTP settings and status.

Command	Description
show sntp client	Displays SNTP client settings.

sntp client mode

Use this command to enable Simple Network Time Protocol (SNTP) client mode and set the mode to either broadcast or unicast. Use the `no` form of the command to disable SNTP client functionality.

sntp client mode {**broadcast** | **unicast**}

no sntp client mode

Syntax Descriptions

Parameter	Description
broadcast	Configures the switch to obtain its time settings from SNTP broadcast servers.
unicast	Configures the switch to obtain its time settings from SNTP unicast servers.

Default

The switch is not configured as an SNTP broadcast or unicast client.

Command Modes

Global Config

Usage Guidelines

Use the command without the optional keywords **broadcast** or **unicast** to enable the SNTP client without specifying a mode.

Related Commands

Command	Description
sntp server	Configures SNTP unicast servers.
show sntp	Displays SNTP settings and status.

Command	Description
show sntp client	Displays SNTP client settings.
show sntp server	Displays settings for configured SNTP unicast servers.

sntp client port

Use this command to configure the logical port number that the switch uses as an SNTP client. Use the `no` form of the command to reset the SNTP client port to the default value.

sntp client port *port-id*

no sntp client port

Syntax Descriptions

Parameter	Description
port-id	The logical port ID.

Default

port-id—123

Command Modes

Global Config

Related Commands

Command	Description
sntp client mode	Displays SNTP client settings.
show sntp client	Displays SNTP client settings.

sntp server

Use this command to configure and enable SNTP unicast servers. Three servers are configured by default. The switch can have up to six SNTP servers total. Use the `no` form of the command to set an SNTP server configuration to the default values, to disable the server, or to delete the server.

NOTE The three default servers cannot be removed using `no` form of the command.

sntp server {*ip-address* | *hostname*} [**version** *1-4*] [**port** *port-id*] [**key** *1–4294967295*] [**enable**]

no sntp server {*ip-address* | *hostname*} [**version**] [**port**] [**key**] [**enable**]

Syntax Descriptions

Parameter	Description
ip address	The IP address of the SNTP server.
hostname	The hostname of the SNTP server. Ensure that a DNS server is configured if a hostname is specified.
version	The SNTP version to use. The range is 1–4.
port	The logical UDP port number to use for SNTP messages.
key	The authentication key to use when sending packets to this server. The range is 1–4294967295.
enable	Enables the SNTP server for polling by the switch.

Default

The following SNTP unicast servers are configured by default, but are not enabled:

- time-a.timefreq.bldrdoc.gov
- time-b.timefreq.bldrdoc.gov
- time-c.timefreq.bldrdoc.gov

Unless the **enable** parameter is specified, a configured server is disabled by default.

The parameter defaults are as follows:

- **version**—4
- **port**—123
- **key**—0

Command Modes

Global Config

Examples

The following command enables one of the build in SNTP servers.

```
(switch) (Config)#sntp server time-a.timefreq.bldrdoc.gov enable
```

The following command disables the same server.

```
(switch) (Config)#no sntp server time-a.timefreq.bldrdoc.gov enable
```

The following command configures a new SNTP server, but does not enable it.

```
(switch) (Config)#sntp server 10.25.67.2 version 3 port 2123 key 432523
```

The following command configures a new SNTP server and enables it.

```
(switch) (Config)#sntp server 10.25.67.2 version 3 port 2123 key 432523
enable
```

Related Commands

Command	Description
show sntp	Displays SNTP settings and status.
show sntp server	Displays settings for configured SNTP unicast servers.

sntp trusted-key

Use this command to authenticate the identity of a system to which SNTP will synchronize. To disable authentication of the identity of the system, use the **no** form of this command.

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

Syntax Descriptions

Parameter	Description
key-number	The key number of the trusted SNTP server.

Default

No keys are trusted.

Command Modes

Global Config

Related Commands

Command	Description
sntp server	Configures SNTP unicast servers.

sntp unicast client poll-interval

If the switch is configured as an SNTP unicast client, it polls the specified SNTP servers to synchronize time settings at a regular interval. Use this command to set the poll interval. Use the `no` form of the command to reset it to the default value.

sntp unicast client poll-interval *poll-interval*

no sntp unicast client poll-interval

Syntax Descriptions

Parameter	Description
poll-interval	A value from 3 to 16. This value is used as an exponent of 2 to calculate the poll interval in seconds.

Default

poll-interval—3

Command Modes

Global Config

Related Commands

Command	Description
sntp client mode	Enables Simple SNTP client mode and sets the mode to either broadcast or unicast.
show sntp	Displays SNTP settings and status.
show sntp client	Displays SNTP client settings.

show sntp

Use this command to display SNTP status.

show sntp

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show sntp

Last Update Time:                  Jan  1 05:30:00 1970
Last Unicast Attempt Time:         Jan  1 05:30:00 1970
Last Attempt Status:               Other

Broadcast Count:                   0
```

Related Commands

Command	Description
sntp client mode	Enables Simple Network Time Protocol (SNTP) client mode and sets the mode to either broadcast or unicast.
sntp server	Configures SNTP unicast servers.
show sntp client	Displays SNTP client settings.
show sntp configuration	Displays SNTP settings.

Command	Description
show clock	Displays the time and date from the system clock.

show sntp client

Use this command to display settings for the switch when it acts as an SNTP client.

show sntp client

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show sntp client

Client Supported Modes:             unicast broadcast
SNTP Version:                       4
Port:                               123
Client Mode:                        broadcast
Broadcast Poll Interval:            3
```

Client Supported Modes	Indicates whether the switch serves as a unicast client, where it sends unicast SNTP requests to the configured servers only, or as a broadcast client, where it accepts time information broadcasted from SNTP servers.
SNTP Version	The SNTP version the switch uses as a client.
Port	The logical port number the switch uses as an SNTP client. The default is the well-known IANA port number for this service, 123.
Client Mode	Indicates whether the switch is enabled or disabled as an SNTP client.
Broadcast/ Unicast Poll Interval	The number of seconds between SNTP polling messages to broadcast or unicast SNTP servers, depending on the client mode configuration.

Related Commands

Command	Description
show sntp	Displays SNTP settings and status.
sntp client mode	Enables Simple Network Time Protocol (SNTP) client mode and sets the mode to either broadcast or unicast.
show clock	Displays the time and date from the system clock.

show sntp configuration

Use this command to show SNTP settings.

show sntp configuration

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show sntp configuration

Polling interval: 8 seconds
MD5 Authentication keys:
Authentication is not required for synchronization.
Trusted keys:
No trusted keys.
Unicast clients: Disable

Unicast servers:
Server           Auth-Key         Polling
---------        -----------      --------
time-a.timefreq Disabled          Disabled
.bldrdoc.gov
time-b.timefreq Disabled          Disabled
.bldrdoc.gov
time-c.timefreq Disabled          Disabled
.bldrdoc.gov
```

Related Commands

Command	Description
show sntp	Displays SNTP settings and status.
sntp server	Configures SNTP unicast servers.

show sntp server

Use this command to display SNTP server settings and configured servers.

show sntp server

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show sntp server

Server Host Address:
Server Type:                       unknown
Server Stratum:                    0
Server Reference Id:
Server Mode:                       Reserved
Server Maximum Entries:            3
Server Current Entries:            1

SNTP Servers
------------

Host Address: 10.131.11.75
Address Type: IPV4
Polling: Disabled
Version: 4
Port: 123
Last Attempt Time: Jan  1 05:30:00 1970
Last Update Status: Other
Total Unicast Requests: 0
Failed Unicast Requests: 0
```

Related Commands

Command	Description
sntp server	Configures SNTP unicast servers.
sntp client mode	Enables SNTP client mode and sets the mode to either broadcast or unicast.
show sntp	Displays SNTP settings and status.
show clock	Displays the time and date from the system clock.

System Software and Configuration Management

You can use the commands described in this section to download, backup, delete, save, and view files that the switch maintains in memory. File types include image, configuration, bootcode, and interface language files. This section also describes the commands for writing configuration changes to memory, setting system location and contact information, and rebooting the switch.

copy

Use this command to upload and download files to and from the switch and to manage the firmware image on the file system. You can perform the following tasks using this command:

- Download a boot code file from the network to the switch.
- Download an updated image file from the network to the switch and back up (upload) the switch image to the network
- Download a configuration file from the network to the startup configuration, backup configuration, or running configuration on the switch. Or, you can back up (upload) these file types (and the mirror configuration file type) to the network.
- Download a new language file for displaying the command line. Or, you can download an upgrade to the default language.
- Download Secure Shell (SSH) keys for use in establishing a secure connection to the management interface (see the **copy nvram:sshkey-rsa1**, **copy nvram:sshkey-rsa2**, and **copy nvram:sshkey-dsa** commands.

- Copy configuration files on the switch among the following file types: running configuration, startup configuration, backup configuration, and mirror configuration.

Uploads and downloads use the TFTP or XMODEM protocols.

copy *source destination*

Syntax Descriptions

Parameter	Description
source	The file type to be copied. See *Usage Guidelines* for further information.
destination	The file type to be copied to. See *Usage Guidelines* for further information.

Command Modes

Privileged Exec

Usage Guidelines

Replace the *source* and *destination* parameters with the options in the following table. For the *url* source or destination, use one of the following values:

{**xmodem** | **tftp**}**://**{*ip-address* | *hostname*}*/filepath/filename*}.

For TFTP, the {*ip-address* | *hostname*} parameter is the IP address or hostname of the server, *filepath* is the path to the file, and *filename* is the name of the file you want to upload or download.

Source	Destination Keywords and Parameters	Action
nvram:backup-config	**nvram:startup-config**	Copies the backup configuration to the startup configuration.
nvram:startup-config	**nvram:backup-config**	Copies the startup configuration to the backup configuration.

Source	Destination Keywords and Parameters	Action
system:running-config	**nvram:startup-config**	Saves the running configuration as the startup configuration file type.
system:running-config	**nvram:backup-config**	Saves the running configuration as the backup configuration file type.
nvram:mirror-config	**nvram:startup-config**	Saves the mirror configuration as the startup configuration file type.
nvram:mirror-config	**nvram:backup-config**	Saves the mirror configuration as the backup configuration file type.
nvram:*script scriptname*, where scriptname can be **startup-config**, **backup-config**, **mirror-config**, or **running-config**	*url*	Copies the specified configuration script file to a server.
url	**nvram:***script destfilename*, where *destfilename* can be **startup-config**, **backup-config**, or **running-config. (**Note that mirror-config can not be used as the destination file name.)	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. If errors are found, the command lists the lines where the errors occurred at the end of the validation process and prompts you to confirm the copy process before continuing.
url	**image**	Downloads an image from the remote server to the switch.
Image	*url*	Uploads an image to the remote server.

Source	Destination Keywords and Parameters	Action
url	**bootcode**	Downloads the boot code from the remote server to the switch.
url	**nvram:langpack**	Downloads the language pack file from the remote server to the switch.
url	**nvram:sshkey-dsa** **nvram:sshkey-rsa1** **nvram:sshkey-rsa2**	Downloads an SSH key of the specified type from the remote server to the switch.

NOTE All configuration files (startup, running, backup, and mirror) are text-based and user-readable.

Examples

The following example copies the current running configuration to the startup configuration file type (i.e., this copied configuration is applied the next time the switch reboots).

```
(Switch) #copy system:running-config nvram:backup-config
Are you sure you want to save? (y/n) y

Config file 'backup-config' created successfully.
Configuration Saved!
```

The following example downloads a new language from a TFTP server:

```
(Switch) #copy tftp://xyztftp.com/languages/de-AT/AustrianGerman.lf
nvram:langpack
Are you sure you want to save? (y/n) y
```

NOTE The switch has a built-in default language pack and can store a second language pack. Either the built-in or the stored language pack can be the active language. If a language pack exists on the switch, and you download another language pack, the new language pack overwrites the stored language pack, provided the language is not currently active.

The following example downloads a boot code file from a TFTP server to the switch.

```
(Switch) #copy tftp://xyztftp.com/bootcode/bootfile.bf bootcode
```

The following example saves a copy of the startup configuration file to a TFTP server. A file name is specified for the saved file.

```
(Switch) #copy nvram:startup-config tftp://xyzhttp.com/savedconfigs/
config_10-12-2010.cfg
```

Related Commands

Command	Description
show config-file-list	Lists all configuration files present in the flash file system on the switch.

delete

Use this command to delete a specified startup-config file, backup-config file, or both. The switch prompts you to confirm this action before it deletes the file(s).

NOTE The mirror-config file cannot be deleted.

delete {*config-file-name* | **all**}

Syntax Descriptions

Parameter	Description
config-file-name	The name of the configuration file.
all	Deletes the startup and backup configuration files.

Command Modes

Privileged Exec

Related Commands

Command	Description
show config-file-list	Lists all configuration files present in the flash file system on the switch.
show config-file	Displays the contents of a configuration file.

set contact

Use this command to set a string that identifies a contact for switch. Use the `no` form of the command to remove the contact information.

set contact *contact*

no set contact

Syntax Descriptions

Parameter	Description
contact	A name or other entity that serves as the contact for switch administration, from 1–160 characters.

Default

No contact string.

Command Modes

Global Config

Related Commands

Command	Description
set hostname	Sets the hostname for the switch.
set location	Sets the switch location string.

set hostname

Use this command to set the hostname for the switch. The hostname displays in the CLI prompt. Use the `no` form of the command to set the hostname to the default.

set hostname *hostname*

no set hostname

Syntax Descriptions

Parameter	Description
hostname	The hostname of the switch, from 1–64 characters.

Default

The default hostname is: **`switch`***<last three bytes of switch MAC>*. For example, **`switch142E4E`**.

Command Modes

Global Config

Related Commands

Command	Description
set location	Sets the switch location string.
set contact	Sets the name of a contact for the switch.

set location

Use this command to set a string that identifies the location of the switch. Use the **`no`** form of the command to remove the contact information.

set location *location*

no set location

Syntax Descriptions

Parameter	Description
location	A description of the location of the switch, from 1–160 characters.

Default

No location string is configured.

Command Modes

Global Config

Related Commands

Command	Description
set hostname	Sets the hostname for the switch.
set contact	Sets the name of a contact for the switch.

reload

This command reboots the switch without powering it off. Reboot means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. On a reboot, the switch tries to start with the startup configuration file. If problems are found in the startup configuration file, then the backup configuration file is used. If the backup file also fails, then the default configuration is applied.

When you enter this command, a prompted displays to confirm that the reboot should proceed. The switch LEDs indicate a successful reboot.

```
reload
```

Command Modes

Privileged Exec

Related Commands

Command	Description
reset factory default	Resets the configuration to the factory defaults, and reboots the switch.

reset factory default

This command resets the configuration to the factory defaults and reboots the switch. When you enter this command, a prompt appears to enable you to confirm the reset. When you enter **y**, you automatically reset the current configuration on the switch to the default values. The switch LEDs indicate a successful reboot.

```
reset factory default
```

Command Modes

Privileged Exec

Related Commands

Command	Description
reload	Reboots the switch without powering it off.

write memory

Use this command to save changes in the running configuration to NVRAM so that the changes persist across a reboot. This command is the same as **copy system:running config nvram:startup-config**. A log message is generated when the configuration is saved.

```
write memory
```

Command Modes

Privileged Exec

Related Commands

Command	Description
copy	Uploads and downloads files to and from the switch and copies files to different switch file types.
show running-config	Displays or captures the current switch settings.

show config-file

Use this command to display the contents of a configuration file.

show config-file ***config-file-name***

Syntax Descriptions

Parameter	Description
config-file-name	The name of the configuration file which can be: ▪ startup-config ▪ backup-config ▪ mirror-config

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch443322) #show config-file backup-config
telnetcon timeout 50
configure
exit
vlan database
vlan 1000
exit
network mgmt_vlan 1000
ip http session soft-timeout 50
configure
logging console enable
logging persistent size 200
logging host ipv4 10.131.17.31 514 debug
logging syslog enable
username "cisco" password e9fdde45468372340d4bd849dda25f08c8b6099a4b66d32b31afb4
7750f98cb8648e53d50678a956d4d54930be63f3aa0af756f7194e9d4324e231b8bb7bd2e9 encrypted override-
complexity-check
username "okk" password c6fee9c4982b125bac5ee0a356e22f0b74702a0a64d82db20a4ae2c0
e9de84aa1c3976ab79382344135da1a5ba33c70f091bd224fe9a107c1cf701cd2619b6f9 encrypted override-
complexity-check
line console
serial timeout 50
exit
spanning-tree configuration name "00-66-55-44-33-22"
snmp-server enable
```

```
snmp-server host 10.131.17.31 public traps v2

--More-- or (q)uit
```

Related Commands

Command	Description
show running-config	Displays or captures the current switch settings.

show config-file list

Use this command to list all configuration files present in the flash file system on the switch, such as the startup-config, backup config, and mirror config scripts.

show config-file list

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch443322) #show config-file list

Configuration Script Name        Size(Bytes)
-------------------------------- -----------
backup-config                           1692
startup-config                          1202

2 configuration file(s) found.
2045 Kbytes free.
```

Related Commands

Command	Description
copy	Uploads and downloads files to and from the switch and copies files to different switch file types.
delete config-file-name	Deletes a specified startup-config file, backup-config file, or both.

show running-config

Use this command to display or capture the current switch settings. By default, this command displays or captures only commands whose settings and configurations are different from the default value.

NOTE This command does not display the User Password, even if it is different than the default.

The output is displayed in script format that can be used to configure another switch with the same configuration.

show running-config [**all** | *filename*]

Syntax Descriptions

Parameter	Description
all	Displays the commands with settings and configurations that are equal to the default value.
file-name	Captures the output of the command to a file with the specified file name. This file can be copied the startup-configuration file type to be used when the system reboots, or can be applied to another switch.

Default

Displays commands with settings that differ from the default values.

Command Modes

Privileged Exec

Usage Guidelines

This command displays configured physical interfaces only; i.e., if an interface contains only the default configuration, that interface is omitted from the output. This is true for any configuration mode that contains nothing but the default configuration. That is, the command to enter a particular configuration mode, followed immediately by its exit command, are both omitted from the command output (and also from the startup-config file when the system configuration is saved).

Examples

The following shows sample output for the command.

```
(switch) #show running-config
!Current Configuration:
!
!System Description “24 FE, 2 GE, C.6.24.2, eCos-2.0"
!System Software Version "C.6.24.2"
!System Up Time          "0 days 5 hrs 42 mins 44 secs"
!Additional Packages     QOS
!Current SNTP Synchronized Time: Not Synchronized
!
telnetcon timeout 160
configure
exit
vlan database
exit
ip telnet server enable
configure
clock timezone -12 minutes 0
logging persistent severity 0
logging persistent enable
logging persistent size 200
logging host dns yahoo.com
username "cisco" password
e9fdde45468372340d4bd849dda25f08c8b6099a4b66d32b31afb4
7750f98cb8648e53d50678a956d4d54930be63f3aa0af756f7194e9d4324e231b8bb7bd2e9
encry
pted override-complexity-check
username "thomas" password
e9fdde45468372340d4bd849dda25f08c8b6099a4b66d32b31afb477
50f98cb8648e53d50678a956d4d54930be63f3aa0af756f7194e9d4324e231b8bb7bd2e9
encrypt
ed override-complexity-check
spanning-tree configuration name "00-66-55-44-33-22"
set hostname "switch123"

--More-- or (q)uit

set contact "Tom Doby"
!
exit
```

Related Commands

Command	Description
show config-file	Displays the contents of a configuration file.
copy	Uploads and downloads files to and from the switch and copies files to different switch file types.

show language-packs detail

Use this command to show details on the available and active language packs on the switch.

show language-packs detail {**all** | **tag** *language-tag*}

Syntax Descriptions

Parameter	Description
all	Displays details for all language packs on the system.
language-tag	Displays details for the specified language tag only. Language tags are specified in ISO format, with a 2 digit language and a 2-digit country code, separated by a hyphen (e.g., en-US).

Command Modes

Privileged Exec

Examples

The following example shows details for the Austrian German language pack.

```
(Switch) #show language-packs detail tag de-at
Language.......................... Austrian German
Tag............................... de-AT
Version........................... 1.8.1.1
MD5 Checksum...................... e1d2f2ed1644f3e9aeb7bb31e803efb6
File Size (KB).................... 29
File Type......................... External
Default........................... No
Status............................ Inactive
Number of Users................... 0
```

The following example shows information on all installed languages.

```
(Switch) #show language-packs detail all
Language.......................... English
Tag............................... en-US
Version........................... 1.8.1.0
MD5 Checksum...................... -----
File Size (KB).................... -----
File Type......................... Built-in
Default........................... Yes
Status............................ Inactive
Number of Users................... 0
Language.......................... Austrian German
```

```
Tag.............................. de-AT
Version.......................... 1.8.1.1
MD5 Checksum..................... e1d2f2ed1644f3e9aeb7bb31e803efb6
File Size (KB)................... 29
File Type........................ External
Default.......................... No
Status........................... Inactive
```

Related Commands

Command	Description
copy	Uploads and downloads files to and from the switch and manages the firmware image on the file system.
show language-packs summary	Shows the available and active language packs on the switch.

show language-packs summary

Use this command to show the available and active language packs on the switch.

show language-packs summary

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show language-packs summary

Language                        Tag                               Default
------------------------------- --------------------------------- -------
Austrian German                 de-AT                             No
English                         en-US                             Yes
```

Language	The language name.
Tag	The ISO standard abbreviation for the language and country.

Default	*Yes* indicates that the language is the built-in language, which displays as the default choice when logging in to the web interface. *No* indicates that the language is a secondary language that has been downloaded to the switch. The secondary language is selectable at log-in.

Related Commands

Command	Description
copy	Uploads and downloads files to and from the switch and manages the firmware image on the file system.
show language-packs detail	Shows details on the available and active language packs on the switch.

show sysinfo

Use this command to display system information.

show sysinfo

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch443322) #show sysinfo

System Description............................ 24 FE, 2 GE, C.6.24.2, eCos-
2.
System Name................................... switch443322
System Location...............................
System Contact................................
System Object ID.............................. 1.3.6.1.4.1.9.6.1.84.24.1
System Up Time................................ 0 days 4 hrs 27 mins 39 secs
Current SNTP Synchronized Time................. Not Synchronized
Software MD5 Sum..............................
2d9ef52bdb6245d872041827ff3ae9f5
Bootcode MD5 Sum..............................
dc5a73e5b2d4b88df66cc069b29c8d5d
```

```
Languages Supported:

           Language                                 Tag                Default
------------------------------- --------------------------------- -------
English                         en-US                             Yes

MIBs Supported:

RFC 1907 - SNMPv2-MIB              The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB                Remote Network Monitoring Management
                                   Information Base

--More-- or (q)uit
```

System Description	Text used to identify this switch.
System Name	A name used to identify the switch. The factory default is blank.
System Location	Text used to identify the location of the switch. The factory default is blank.
System Contact	Text used to identify a contact person for this switch. The factory default is blank.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours, and minutes since the last switch reboot.
Current SNTP Synchronized Time	The most recent time that the switch was synchronized with an SNTP server.
Checksum	The firmware and boot code MD5 checksum values.
Languages Supported	A list of the languages supported for displaying the web-based management interface. This also identifies the default (built-in) language.
MIBs Supported	A list of MIBs supported by this agent.

Related Commands

Command	Description
set hostname	Configures a name for the switch.
set contact	Configures a contact name for the switch.
set location	Configures a description of the switch location.
show clock	Shows clock configuration details.
show language pack detail	Shows details on the available and active language packs on the switch.

Syslog

The switch generates messages in response to events, faults, or errors occurring on the platform and to changes in configuration or other occurrences. These messages are stored both locally in system memory and can be forwarded to one or more centralized points of collection (i.e., a syslog server) for monitoring purposes or long-term archiving. This section describes the commands you can use to configure and view the system logs.

clear logging buffered

Use this command to clear messages from the in-memory logging buffer.

```
clear logging buffered
```

Command Modes

Global Config

Related Commands

Command	Description
logging buffered	Limits log messages displayed from an in-memory buffer based on severity.

Command	Description
show logging buffered	Use this command to display buffered in-memory logging information, and log entries.

clear logging persistent

Use this command to clear messages from the persistent log memory and the other versions.

```
clear logging persistent
```

Command Modes

Global Config

Related Commands

Command	Description
logging persistent	Configures persistent logging for the switch.
show logging persistent	Displays persistent logging information and log entries.

copy

Use this command to upload event logs from the switch using TFTP or Xmodem.

```
copy source destination
```

Syntax Descriptions

Parameter	Description
source	*source* can be: ▪ **nvram:startup-log version** *x*—This is the startup persistent log. ▪ **nvram:operational-log version** *x*—This is the operational persistent log. Where *x* is the version of the startup or operational log, and can be 1, 2 or 3. If version is not specified, then version current version (version 1) is used.
destination	*destination* can be: {**xmodem** | **tftp**}**://**{*ip-address* | *hostname*}*/filepath/ filename*}**.** For TFTP, the {*ip-address* | *hostname*} parameter is the IP address or hostname of the server, *filepath* is the path to the file, and *filename* is the name of the file you want to give to the file when it is saved.

Command Modes

Privileged EXEC

Examples

The following example saves the startup log in flash to a TFTP server location and names the file.

```
(switch) #copy nvram:startup-log version 1 tftp://10.12.17.182/logs/
startuplog06-24-10.txt

Mode........................................... TFTP
Set Server IP.................................. 10.12.17.182
Path........................................... logs/
Filename....................................... startuplog06-24-10.txt
Data Type...................................... Startup Log

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n)y
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging aggregation enable

Use this command to enable the switch to consolidate consecutive log messages of the same type into a single log message. Use the `no` form of the command to disable this feature.

logging aggregation enable

no logging aggregation enable

Default

Logging aggregation is disabled.

Command Modes

Global Config

Related Commands

Command	Description
logging aggregation maxtime	Sets the logging aggregation time period.
show logging	Displays logging configuration information.

logging aggregation maxtime

Use this command to set the logging aggregation time period. Use the `no` form to reset the time period to the default value (15 sec). If two or more of the same log message are generated consecutively within the configured time interval, and no event occurs in between, then the messages are aggregated into a single log message. The range is 15 seconds to 120 seconds.

logging aggregation maxtime *15-120*

no logging aggregation enable

Default

maxtime—15 sec.

Command Modes

Global Config

Related Commands

Command	Description
logging aggregation enable	Enables logging aggregation.
show logging	Displays logging configuration information.

logging buffered enable

Use this command to enable buffered logging (in-memory). To stop buffered logging, use the `no` form of this command.

```
logging buffered enable

no logging buffered enable
```

Default

Buffered logging is enabled.

Command Modes

Global Config

Related Commands

Command	Description
clear logging buffered	Clears the buffered log.
logging buffered severity	Limits buffered message logging to a specified severity level.

Command	Description
show logging buffered	Displays buffered in-memory logging information and log entries.

logging buffered severity

Use this command to limit buffered message logging to a specified severity level. Use the `no` form of the command to set the severity level to the default value (2).

logging buffered severity *severitylevel*

no logging buffered severity

Syntax Descriptions

Parameter	Description
severitylevel	The level of the traps to be logged. Traps of this level and lower (numerically) are logged. You can specify an integer from 0 to 7 or one of the following keywords: ▪ emergency (0) ▪ alert (1) ▪ critical (2) ▪ error (3) ▪ warning (4) ▪ notice (5) ▪ info (6) ▪ debug (7)

Default

severitylevel—critical (2)

Command Modes

Global Config

Related Commands

Command	Description
clear logging buffered	Clears the buffered log.
logging buffered enable	Enables buffered logging.
show logging buffered	Displays buffered in-memory logging information and log entries.

logging console enable

Use this command to enable logging to a terminal connected to the console port. To stop console logging, use the `no` form of this command.

logging console enable

no logging console enable

Default

Console logging is disabled.

Command Modes

Global Config

Related Commands

Command	Description
logging console severity	Limits buffered message logging to a specified severity level.

logging console severity

Use this command to limit console message logging to a specified severity level. Use the `no` form of the command to set the severity level to the default value (2).

logging console severity *serveritylevel*

no logging console severity

Syntax Descriptions

Parameter	Description
severitylevel	The severity level of the traps to be logged. You can specify an integer from 0 to 7 or one of the following keywords: ▪ emergency (0) ▪ alert (1) ▪ critical (2) ▪ error (3) ▪ warning (4) ▪ notice (5) ▪ info (6) ▪ debug (7)

Default

severitylevel—critical (2).

Command Modes

Global Config

Related Commands

Command	Description
logging console enable	Enables logging to a terminal connected to the console port.

logging host

Use this command to enable logging to a host (syslog server). You can configure up to eight logging hosts.

logging host *addresstype* {*ipaddr* | *hostname*} [*port*] [*severitylevel*]

Syntax Descriptions

Parameter	Description
addresstype	The type of address being passed. Options are **ip** or **dns**.
ipaddr	The IP address of the logging host, if the *addresstype* is specified as **ip**.
hostname	The hostname of the logging host, if the addresstype is specified as **dns.**
port	The port number of the syslog server. The range is 1025–65535.
severitylevel	The severity level of the traps to be logged. You can specify an integer from 0 to 7 or one of the following keywords: - Emergency (0) - Alert (1) - Critical (2) - Error (3) - Warning (4) - Notice (5) - Info (6) - Debug (7)

Defaults

- *port*—514.
- *severitylevel*—Critical (2).

Command Modes

Global Config

Related Commands

Command	Description
logging host remove	Removes a syslog server.
logging console level	Enables logging to the console.
show logging hosts	Displays the configured Syslog servers.

logging host remove

Use this command to remove a syslog server. Use the command **show logging hosts** for a list of host indexes.

```
logging host remove hostindex
```

Syntax Descriptions

Parameter	Description
hostindex	The numeric ID for the host.

Command Modes

Global Config

Related Commands

Command	Description
logging host	Enables logging to the console.
show logging hosts	Displays the configured Syslog servers.

logging persistent enable

Use this command to enable persistent logging to Flash memory. To stop persistent logging, use the `no` form of this command.

logging persistent enable

no logging persistent enable

Default

Persistent logging is disabled.

Command Modes

Global Config

Related Commands

Command	Description
logging persistent severity	Limits buffered message logging to a specified severity level.
logging persistent size	Sets the log size for persistent logging.
show logging persistent	Displays persistent memory logging information and log entries.

logging persistent severity

Use this command to limit persistent logging (to Flash memory) to a specified severity level. Use the `no` form of the command to set the severity level to the default value (2).

logging persistent severity *severity-level*

no logging persistent severity

Syntax Descriptions

Parameter	Description
severity-level	The severity level of the traps to be logged. You can specify an integer from 0 to 7 or one of the following keywords: ▪ emergency—0 ▪ alert—1 ▪ critical—2 ▪ error—3 ▪ warning—4 ▪ notice—5 ▪ info—6 ▪ debug—7

Default

severitylevel—critical (2).

Command Modes

Global Config

Related Commands

Command	Description
logging persistent size	Sets the log size for persistent logging.
show logging persistent	Displays persistent logging information and log entries.

logging persistent size

Use this command to set logging size for persistent logging. Use the `no` form of the command to reset the size to the default. This is relevant to operational logs.

logging persistent size *50-200*

no logging persistent size

Syntax Descriptions

Parameter	Description
50–200	The number of entries to store in the persistent log.

Default

size—200 entries

Command Modes

Global Config

Related Commands

Command	Description
logging persistent	Configures persistent logging on the switch.
show logging persistent	Displays persistent logging information and log entries.
show logging	Displays logging configuration information.

logging syslog enable

Use this command to enable the syslog client on the switch. To disable the syslog client, use the `no` form of this command.

logging syslog enable

no logging syslog enable

Default

The syslog client is disabled.

Command Modes

Global Config

Related Commands

Command	Description
logging syslog facility	Sets the facility for logging messages.
logging syslog port	Specifies the logical port number for the syslog client on the switch.
show logging	Displays logging configuration information.

logging syslog facility

Use this command to set the facility for logging messages. The meaning of the facility value is determined by the system administrator. To reset to the default value, use the `no` form of the command.

logging syslog facility *facility*

no logging syslog facility *facility*

Syntax Descriptions

Parameter	Description
facility	A can take one of the follow values: local0, local1, local2, local3, local4, local5, local 6, local7.

Default

facility—local7

Command Modes

Global Config

Related Commands

Command	Description
logging syslog enable	Enables the syslog client on the switch.
logging syslog port	Specifies the logical port number for the syslog client on the switch.
show logging	Displays logging configuration information.

logging syslog port

Use this command to specify the logical port number for the syslog client on the switch. Use the `no` form of the command to reset the syslog client port number to the default.

logging syslog port *portid*

no logging syslog port *portid*

Syntax Descriptions

Parameter	Description
portid	The port number of the syslog client on the switch, which is an integer in the range 1025–65535.

Default

portid—514.

Command Modes

Global Config

Related Commands

Command	Description
logging syslog enable	Sets the facility for logging messages.

Command	Description
logging syslog facility	Sets the facility for logging messages.
show logging	Displays logging configuration information.

show logging

Use this command to display logging configuration information.

show logging

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show logging

Console Logging                      : disabled
Console Logging Severity Filter      : critical
Buffered Logging                     : enabled
Buffered Logging Severity Filter     : critical
Persistent Logging                   : disabled
Persistent Logging Severity Filter   : critical

Syslog Logging                       : disabled
Logging Client Local Port            : 514
Syslog Logging Facility              : local7

Log Aggregation                      : disabled

Log Messages Received                : 181
Log Messages Dropped                 : 0
Log Messages Relayed                 : 0
```

Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.

Buffered Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity to log to the persistent log. Messages with an equal or lower numerical severity are logged.
Syslog Logging	Shows whether syslog logging is enabled.
Logging Client Local Port	The logical port number for syslog communication with the local syslog client.
Syslog Logging Facility	The syslog facility identification assigned to this system (*local1* through *local7*). The meaning of facility values defined by the system administrator.
Log Messages Received	Then number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	The number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	The number of messages sent to the collector/relay.

Related Commands

Command	Description
logging buffered enable	Enables logging to the in-memory buffer.
logging console enable	Enables logging to a terminal connected to the console port.
logging syslog enable	Enables syslog logging.
logging persistent enable	Enables persistent logging to Flash memory.

show logging buffered

Use this command to display buffered in-memory logging information and log entries.

show logging buffered

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show logging buffered

Buffered (In-Memory) Logging          : enabled
Buffered Logging Wrapping Behavior    : On
Buffered Log Count                    : 112

1995-11-
26 19:29:10 CRIT LOG[LOG]: log_server.c(1827)  2 %% Log service started

Buffered messages filtered       : 111
```

Related Commands

Command	Description
logging buffered enable	Configures buffered logging on the switch.
logging buffered severity	Configures the minimum severity level that log messages must have to be sent to the buffered log.
clear logging buffered	Clear messages from the in-memory logging buffer.

show logging hosts

Use this command to display the configured syslog servers.

show logging hosts

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show logging hosts

Index  IP Address/Hostname       Severity   Port   Status
----- ------------------------  ----------  ------ -------------
1      yahoo.com                 critical    514   Active
```

Index	An ID that is used for deleting hosts.
IP Address / Hostname	IP address or hostname of the logging host.
Severity	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Status	The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

Related Commands

Command	Description
logging host	Enables logging to a host (syslog server).
logging host remove	Removes a syslog server.

show logging persistent

Use this command to display persistent logging information and log entries.

show logging persistent [startup | operational] [{**0** | **1** | **2**}]

Syntax Descriptions

Parameter	Description
startup	Shows the startup log.
operational	Shows the operational log.
0 | 1 | 2	Specifies the version of the log to display: ▪ **0**—Shows the current log. ▪ **1**—Shows the log of the most recent reboot. ▪ **2**—Shows the log of the reboot prior to the most recent.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command when the log type is unspecified.

```
(switch) #show logging persistent

Persistent Logging                    : enabled
Persistent Log Size                   : 200
Persistent Log Count                  : 1
1995-11-26 19:29:10 CRIT LOG[LOG]: log_server.c(1827)  2 %% Log service
started
```

Related Commands

Command	Description
logging persistent enable	Configures persistent logging on the switch.
logging persistent severity	Configures the minimum severity level that log messages must have to be sent to the persistent log.
logging persistent size	Sets the log size for persistent logging.

Command	Description
clear logging persistent	Clears messages from the persistent log memory and the other versions.

show logging traplogs

Use this command to display the SNMP trap events and statistics. The Trap Log capacity is 64 entries.

show logging traplogs

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show logging traplogs

Number of Traps Since Last Reset............... 11
Trap Log Capacity.............................. 64
Number of Traps Since Log Last Viewed.......... 11

Log System Up Time            Trap
--- ------------------------ -----------------------------------------------
  0 0 days 04:15:24           Failed User Login: Unit: 1 User ID: cisco
  1 0 days 04:00:23           Failed User Login: Unit: 1 User ID: cisco
  2 0 days 03:48:10           Failed User Login: Unit: 1 User ID: cisco
  3 0 days 03:47:54           Failed User Login: Unit: 1 User ID: cisco
  4 0 days 02:36:43           Failed User Login: Unit: 1 User ID: cisco
  5 0 days 02:27:40           Failed User Login: Unit: 1 User ID: cisco
  6 0 days 02:27:28           Failed User Login: Unit: 1 User ID: cisco
  7 0 days 00:01:19           Cold Start: Unit: 0
  8 0 days 00:00:42           Link Up: e1
  9 0 days 00:00:23           Temperature change alarm: Sensor ID: 1 Event: 1
 10 0 days 00:00:23           Temperature change alarm: Sensor ID: 0 Event: 1
```

Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.

Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System UP Time	System up time.
Trap	The text of the trap message.

Related Commands

Command	Description
show logging	Displays logging configuration information.

RMON

Smart switch supports Remote Monitoring (RMON) for collecting data about network traffic. A device that supports gathering and reporting the RMON data is referred to as an RMON probe or RMON Agent. An RMON probe provides RMON data to an RMON Manager for analysis and presentation to the User. This section describes the RMON commands.

rmon alarm

Use this command to configure alarm conditions. Use the `no` form of the command to remove an alarm.

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

no rmon alarm *index*

Syntax Descriptions

Parameter	Description
index	The alarm index. The range is 1–300.

Parameter	Description
variable	A fully qualified SNMP object identifier that resolves to a particular instance of an MIB object.
interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1–4294967295.
rthreshold	The rising threshold. The range is 0–4294967295.
fthreshold	The falling threshold. The range is 0–4294967295.
revent	The index of the event that is used when a rising threshold is crossed. The range is 1–65535.
fevent	The event index used when a falling threshold is crossed. The range is 1–300.
type	The method for sampling the variable and for calculating the value to be compared against the thresholds. 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 at the last sample is subtracted from the current value, and the difference compared with the thresholds.
direction	The alarm that might be sent when this entry is first set to valid. If the first sample (after this entry becomes valid) is greater than or equal to the rising threshold, and direction is equal to rising or rising-falling, then a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to the falling threshold, and direction is equal to falling or rising-falling, then a single falling alarm is generated.
name	Enter a name that identifies who configured this alarm. If unspecified, the name is an empty string.

Defaults

- *type*—If unspecified, the type is absolute.
- *direction*—If unspecified, the startup direction is rising-falling.

Command Modes

Global Config

Examples

The following example configures the following alarm conditions:

- Alarm index—1
- Variable identifier—1.3.6.1.2.1.2.2.1.10.5
- Sample interval—10 seconds
- Rising threshold—500000
- Falling threshold—10
- Rising threshold event index—1
- Falling threshold event index—1

```
switch(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.1.10.5 10 50000 10 1 1
```

Related Commands

Command	Description
show rmon alarm	Displays alarm configuration.
show rmon alarm-table	Displays the alarms summary table.

rmon collection history

Use this command in Interface Config mode to enable a Remote Monitoring (RMON) MIB history statistics group on an interface. Use the `no` form of this command to remove a specified RMON history statistics group.

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

Syntax Descriptions

Parameter	Description
index	The requested statistics index group. The range is 1–300.
ownername	Records the RMON statistics group owner name. If unspecified, the name is an empty string.
bucket-number	A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. The range is 1–65535.
seconds	The number of seconds in each polling cycle. If unspecified, it defaults to 1800. The range is 1–3600.

Defaults

- *bucket-number*—50
- *interval seconds*—1800

Command Modes

Interface Config

Examples

The following example enables a Remote Monitoring (RMON) MIB history statistics group on port 1/g8 with the index number 1 and a polling interval period of 2400 seconds.

```
switch(config)#interface e1
switch(config-if-e1)#rmon collection history 1 interval 2400
```

Related Commands

Command	Description
show rmon collection history	Displays the requested group of statistics.

rmon event

Use this command in Global Config mode to configure an event. To remove an event, use the `no` form of this command.

rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]

no rmon event *index*

Syntax Descriptions

Parameter	Description
index	The event index. The range is 1–300.
type	The type of notification that the device generates about this event. The index type can be one of 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 text	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string. The range is 0–127 characters.
description text	A comment describing this event. The range is 0–127 characters.
owner name	Enter a name that specifies who configured this event. If unspecified, the name is an empty string.

Command Modes

Global Config

Examples

The following example configures an event with the trap index of 10.

```
switch(config)#rmon event 10 log
```

Related Commands

Command	Description
show rmon events	Displays the RMON event table.

show environment

Use this command to display functioning of the switch; i.e., the fan status, the temperature, and the power supply status.

show environment

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show environment

Temperature Sensors:

Temperature (Celsius)    Status
---------------------    ------
 67                      OK

Fans:

Description    Status
-----------    ------

Power Supplies:

Description    Status         Source
-----------    -----------    ------
Main           OK             AC
```

Related Commands

Command	Description
show process cpu	Shows the percentage utilization of the CPU by different tasks.

show process cpu

Use this command to see the percentage utilization of the CPU by different tasks.

show process cpu

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show process cpu

Memory Utilization Report
status      bytes
------ ----------
  free 1283317760
 alloc 1819578368
CPU Utilization:
 PID     Name                     5 Sec    1 Min    5 Min
---------------------------------------------------------
15790    cpuUtilMonitorTask       0.00%    0.02%    0.00%
15799    DHCP Client Task         0.19%    0.02%    0.00%
15810    emWeb                    0.00%    0.00%    0.05%
---------------------------------------------------------
 Total CPU Utilization            0.19%    0.04%    0.05%
```

Related Commands

Command	Description
show environment	Displays functioning of the switch; i.e., fans, temperature, and power supply status.

show rmon alarm

Use this command in Privileged EXEC mode to display alarm configuration.

```
show rmon alarm number
```

Syntax Descriptions

Parameter	Description
number	The alarm number.

Command Modes

Privileged Exec

Examples

The following fields display for the specified alarm.

Alarm	The alarm index.
OID	Monitored variable object ID.
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 might be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.
Owner	The entity that configured this entry.

Related Commands

Command	Description
rmon alarm	Configures alarm conditions.

show rmon alarm-table

Use this command in Privileged EXEC mode to display the alarms summary table.

```
show rmon alarm-table
```

Command Modes

Privileged Exec

Examples

The following fields display.

Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

Related Commands

Command	Description
rmon alarm	Configures alarm conditions.

show rmon collection history

Use this command in Privileged EXEC mode to display the requested group of statistics.

show rmon collection history {**ethernet** *interface* | **port-channel** *port-channel-number*}

Syntax Descriptions

Parameter	Description
interface	The port number.
port-channel-number	A LAG ID.

Command Modes

Privileged Exec

Examples

The following fields display:

Index	An index that uniquely identifies the entry.

Interface	The sampled Ethernet interface.
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

Related Commands

Command	Description
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.

show rmon events

Use this command in Privileged EXEC mode to display the RMON event table.

show rmon events

Command Modes

Privileged Exec

Examples

Index	An index that uniquely identifies the entry.
Description	A comment describing this event.

Type	The type of notification that the device generates about this event. It can have the following values: - **none** - **log** - **trap** - **log-trap** In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

Related Commands

Command	Description
rmon event	Configures an RMON event.

show rmon history

Use this command in Privileged EXEC mode to display RMON Ethernet Statistics history.

show rmon history *index* {**throughput** | **errors** | **other**} [**period** *seconds*]

Syntax Descriptions

Parameter	Description
index	The requested set of samples. The range is 1–300.
throughput	Displays throughput counters.
errors	Displays error counters.

Parameter	Description
other	Displays drop and collision counters.
seconds	Specifies the requested period time to display. The range is 0–2147483647.

Command Modes

Privileged Exec

Examples

The following fields might display, depending on the keyword specified.

Time	The date and time the entry was 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.
%	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 fewer than 64 octets (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 fewer than 64 octets (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 number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped. It is just the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

Related Commands

Command	Description
show rmon events	Displays the RMON event table.
show rmon collection history	Displays the requested group of statistics.

Command	Description
show rmon log	Displays the RMON logging table.

show rmon log

Use this command in Privileged EXEC mode to display the RMON logging table.

show rmon log [*event*]

Syntax Descriptions

Parameter	Description
event	The event index. The range is 1–300.

Command Modes

Privileged Exec

Examples

The following fields display.

Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry was created.

Related Commands

Command	Description
show rmon history	Displays RMON Ethernet Statistics history.
show rmon events	Displays the RMON event table.

show rmon statistics

Use this command in Privileged EXEC mode to display RMON Ethernet Statistics.

show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}

Syntax Descriptions

Parameter	Description
interface	Valid Ethernet unit/port.
port-channel-number	Valid port-channel trunk index.

Command Modes

Privileged Exec

Examples

The following fields display.

Dropped	An index that uniquely identifies the event.
Octets	A comment describing this event.
Packets	The time this entry was created.
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).

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).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
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).

Related Commands

Command	Description
show rmon history	Displays RMON Ethernet statistics history.

3

Port Management

This chapter describes commands you use to configure switch ports and link aggregation groups (LAGs). It contains the following sections:

- **Switch Ports**
- **Green Ethernet**
- **Flow Control and Storm Control**
- **Link Aggregation**

Switch Ports

You can use the commands described in this section to configure and view information on switch port capabilities.

auto-negotiate

Use this command to enable auto-negotiation on a port. Use the `no` form of the command to disable the auto-negotiation and put the port to fixed speed of 100 MB full-duplex.

auto-negotiate [*capability1*][*capability2…capability5*]

no auto-negotiate

Syntax Descriptions

Parameter	Description
capability	The capabilities to advertise. Possible values: `10h`, `10f`, `100h`, `100f`, and `1000f`. If capabilities are unspecified, the default to list of all capabilities of the port.

Default

All capabilities are advertised.

Command Modes

Interface Config

Examples

The following example enables auto negotiation on Ethernet port 5.

```
(Switch) (config)#interface e5
(Switch) (Interface e5)#auto-negotiate
```

Related Commands

Command	Description
auto-negotiate all	Enables auto-negotiation on all ports.
show interface advertise	Displays information about auto-negotiation advertisement.

Usage Guidelines

Entering the command with no parameters enables all capabilities. If you had previously entered negotiation with capabilities, this action overwrites the previous configuration so that all capabilities are enabled.

auto-negotiate all

Use this command to set auto-negotiation on all ports. Use the **no** form of the command to disable it on all ports.

auto-negotiate all [*capability1*][*capability2*…*capability5*]

no auto-negotiate all

Syntax Descriptions

Parameter	Description
capability	The capabilities to advertise. Possible values: **10h**, **10f**, **100h**, **100f**, and **1000f**. If capabilities are unspecified, the default to list of all capabilities of the port.

Default

Auto-negotiation is enabled.

Command Modes

Global Config

Examples

The following command enables `10h` and `100h` autonegotiation on all ports:

```
(Switch) (config)#auto-negotiate all 100h
```

Related Commands

Command	Description
auto-negotiate	Enables auto-negotiation on a port.
show port	Displays information about auto-negotiation advertisement.

mtu

Use this command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. Use the `no` form of the command to reset it to the default value (1518). You can use the **mtu** command to configure jumbo frame support for physical and Link Aggregation Group (LAG) interfaces.

mtu ***1518-2048***

no mtu

Syntax Descriptions

Parameter	Description
1518–2048	The MTU size in bytes.

Default

mtu—1518 bytes (untagged)

Command Modes

Interface Config

Related Commands

Command	Description
show port	Displays port information.

shutdown

Use this command to disable a port. Use the `no` form of this command to enable the port.

shutdown

no shutdown

Default

Ports are enabled.

Command Modes

Interface Config

Related Commands

Command	Description
shutdown all	Disables all the ports.

shutdown all

Use this command to disable all the ports. Use the `no` form of this command to enable all ports.

shutdown all

no shutdown all

Default

Ports are enabled.

Command Modes

Global Config

Related Commands

Command	Description
shutdown	Disables a port.

speed

Use this command to configure the speed of an Ethernet interface when auto-negotiation is not enabled.

speed {**100** | **10**} {**half-duplex** | **full-duplex**}

Syntax Descriptions

Parameter	Description
100 | 10	Configures 100 Mbps or 10 Mbps operation.
half-duplex | full duplex	Configures half-duplex or full-duplex port operation.

Command Modes

Interface Config

Usage Guidelines

The **`no auto-negotiate`** command automatically puts the port into 100 Mbps full-duplex mode, so this command does not have a **`no`** form.

Examples

The following command configures port e5 to be in 100 Mbps, half-duplex operation when auto-configuration is disabled.

```
(Switch) (config)#interface e5
(Switch) (Interface e5)#speed 100 half-duplex
```

Related Commands

Command	Description
speed all	Configures the speed of an Ethernet interface when not using auto-negotiation.
show port	Displays port information.

speed all

Use this command to configure the speed of all Ethernet interfaces when not using auto-negotiation.

speed all {**100** | **10**} {**half-duplex** | **full-duplex**}

Syntax Descriptions

Parameter	Description
100 | 10	Configures 100 Mbps or 10 Mbps operation.
half-duplex | full duplex	Configures half-duplex or full-duplex port operation.

Command Modes

Global Config

Examples

The following command sets all ports to 100 Mbps full-duplex operation when Auto Configuration is disabled.

```
(Switch) (config)#speed all 100 full-duplex
```

Related Commands

Command	Description
speed	Configures the speed of an Ethernet interface when not using auto-negotiation.

Command	Description
show port	Displays port information.

show interface advertise

Use this command to display the port autonegotiation status and the advertised speeds for an individual port or all ports.

show interface advertise [**ethernet** *interface*]

Syntax Descriptions

Parameter	Description
Ethernet	Displays information for a specified port. If this parameter is not specified, the command displays information for all ports.

Command Modes

Privileged Exec

Examples

The following command shows command output for all interfaces.

```
(switch) #show interface advertise

Port     Type       Neg       Operational Link Advertisement
-------- ---------- --------- ------------------------------
e1                  Enable    1000f, 100f, 100h, 10f, 10h
e2                  Enable    1000f, 100f, 100h, 10f, 10h
e3                  Enable    1000f, 100f, 100h, 10f, 10h
e4                  Enable    1000f, 100f, 100h, 10f, 10h
e5       PC Mbr     Enable    1000f, 100f, 100h, 10f, 10h
e6       PC Mbr     Enable    1000f, 100f, 100h, 10f, 10h
e7       Mirror     Disable
e8       Probe      Enable    1000f, 100f, 100h, 10f, 10h
e9                  Enable    1000f, 100f, 100h, 10f, 10h
e10                 Enable    1000f, 100f, 100h, 10f, 10h
e11                 Enable    1000f, 100f, 100h, 10f, 10h
e12                 Enable    1000f, 100f, 100h, 10f, 10h
e13                 Enable    1000f, 100f, 100h, 10f, 10h
e14                 Enable    1000f, 100f, 100h, 10f, 10h
e15                 Enable    1000f, 100f, 100h, 10f, 10h
e16      Mirror     Enable    1000f, 100f, 100h, 10f, 10h
```

```
e17                 Enable    1000f, 100f, 100h, 10f, 10h
e18                 Enable    1000f, 100f, 100h, 10f, 10h
```

The following example shows command output for a specific interface.

```
(switch) #show interface advertise ethernet e1
Port:e1
Type  :
Link Status:Down
Auto Neg:Enable
                               1000f 100f 100h 10f 10h
                               ----- ---- ---- ---- ----
Admin Local link Advertisement Y     Y    Y    Y    Y
```

Related Commands

Command	Description
show port	Displays port information.
auto-negotiate	Enables auto-negotiation on a port.

show interface ethernet

Use this command to display detailed statistics for a specific interface or for the entire switch.

show interface ethernet {*interface* | **switchport**}

Syntax Descriptions

Parameter	Description
interface	The port or LAG name.
switchport	Displays information for all ports on the switch.

Command Modes

Privileged Exec

Examples

The following command shows statistics for port e1.

```
(switch) #show interface ethernet e1

Total Packets Received (Octets)................ 0
Packets Received 64 Octets..................... 0
Packets Received 65-127 Octets................. 0
Packets Received 128-255 Octets................ 0
Packets Received 256-511 Octets................ 0
Packets Received 512-1023 Octets............... 0
Packets Received 1024-1518 Octets.............. 0
Packets Received > 1518 Octets................. 0
Packets RX and TX 64 Octets.................... 0
Packets RX and TX 65-127 Octets................ 0
Packets RX and TX 128-255 Octets............... 0
Packets RX and TX 256-511 Octets............... 0
Packets RX and TX 512-1023 Octets.............. 0
Packets RX and TX 1024-1518 Octets............. 0
Packets RX and TX 1519-1522 Octets............. 0
Packets RX and TX 1519-2047 Octets............. 0
Packets RX and TX 2048-4095 Octets............. 0
Packets RX and TX 4096-9216 Octets............. 0

Total Packets Received Without Errors.......... 0
Unicast Packets Received....................... 0
Multicast Packets Received..................... 0
Broadcast Packets Received..................... 0

Total Packets Received with MAC Errors......... 0
Jabbers Received............................... 0
Fragments Received............................. 0
Undersize Received............................. 0
Alignment Errors............................... 0
FCS Errors..................................... 0
Overruns....................................... 0

Total Received Packets Not Forwarded........... 0
Local Traffic Frames........................... 0
802.3x Pause Frames Received................... 0
Unacceptable Frame Type........................ 0
Multicast Tree Viable Discards................. 0
Reserved Address Discards...................... 0
CFI Discards................................... 0
Upstream Threshold............................. 0

Total Packets Transmitted (Octets)............. 0
Packets Transmitted 64 Octets.................. 0
Packets Transmitted 65-127 Octets.............. 0
Packets Transmitted 128-255 Octets............. 0
Packets Transmitted 256-511 Octets............. 0
Packets Transmitted 512-1023 Octets............ 0
Packets Transmitted 1024-1518 Octets........... 0
Max Frame Size................................. 1518
```

```
Total Packets Transmitted Successfully......... 0
Unicast Packets Transmitted.................... 0
Multicast Packets Transmitted.................. 0
Broadcast Packets Transmitted.................. 0

Total Transmit Errors.......................... 0
FCS Errors..................................... 0
Packets Transmitted > 1518 Octets.............. 0
Underrun Errors................................ 0

Total Transmit Packets Discarded............... 0
Single Collision Frames........................ 0
Multiple Collision Frames...................... 0
Excessive Collision Frames..................... 0
Port Membership Discards....................... 0

802.3x Pause Frames Transmitted................ 0
STP BPDUs Transmitted.......................... 0
STP BPDUs Received............................. 0
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 0
MSTP BPDUs Received............................ 0

EAPOL Frames Transmitted....................... 0
EAPOL Start Frames Received.................... 0

Time Since Counters Last Cleared............... 11 day 8 hr 2 min 4 sec
```

The following command shows statistics when the **switchport** parameter is used.

```
(switch010000) #show interface Ethernet switchport
Total Packets Received (Octets)................ 494480
Packets Received Without Error................. 3151
Unicast Packets Received....................... 2357
Multicast Packets Received..................... 196
Broadcast Packets Received..................... 598
Receive Packets Discarded...................... 0

Octets Transmitted............................. 1146731
Packets Transmitted Without Errors............. 3141
Unicast Packets Transmitted.................... 1713
Multicast Packets Transmitted.................. 1412
Broadcast Packets Transmitted.................. 16
Transmit Packets Discarded..................... 0

Most Address Entries Ever Used................. 35
Address Entries Currently in Use............... 30

Maximum VLAN Entries........................... 256
Most VLAN Entries Ever Used.................... 1
Static VLAN Entries............................ 1
```

```
Dynamic VLAN Entries........................... 0
VLAN Deletes................................... 0
Time Since Counters Last Cleared............... 0 day 0 hr 44 min 53 sec
```

Related Commands

Command	Description
show port	Displays port information.

show port

Use this command to display information about auto-negotiation advertisement.

show port {**all** | *interface*}

Syntax Descriptions

Parameter	Description
all	Shows information for all interfaces.
interface	Shows information for the specified interface.

Command Modes

Privileged Exec

Examples

The following example shows command output.

```
(switch) #show port all

               Admin   Physical   Physical   Link   Link    LACP    Flow
 Intf   Type    Mode    Mode       Status    Status Trap    Mode    Mode
------ ------ --------- ---------- ---------- ------ ------- ------ -------
e1            Enable    Auto       10 Half    Up     Enable  Enable Disable
e2            Enable    Auto                  Down   Enable  Enable Disable
e3            Enable    Auto                  Down   Enable  Enable Disable
e4            Enable    Auto                  Down   Enable  Enable Disable
e5            Enable    Auto                  Down   Enable  Enable Disable
e6            Enable    Auto                  Down   Enable  Enable Disable
e7            Enable    Auto                  Down   Enable  Enable Disable
e8            Enable    Auto                  Down   Enable  Enable Disable
e9            Enable    Auto                  Down   Enable  Enable Disable
e10           Enable    Auto                  Down   Enable  Enable Disable
```

```
e11           Enable    Auto                  Down   Enable  Enable Disable
e12           Enable    Auto                  Down   Enable  Enable Disable
e13           Enable    Auto                  Down   Enable  Enable Disable
e14           Enable    Auto                  Down   Enable  Enable Disable
e15           Enable    Auto                  Down   Enable  Enable Disable
e16           Enable    Auto                  Down   Enable  Enable Disable
e17           Enable    Auto                  Down   Enable  Enable Disable
e18           Enable    Auto                  Down   Enable  Enable Disable
e19           Enable    Auto                  Down   Enable  Enable Disable
e20           Enable    Auto                  Down   Enable  Enable Disable
e21           Enable    Auto                  Down   Enable  Enable Disable
e22           Enable    Auto                  Down   Enable  Enable Disable
e23           Enable    Auto                  Down   Enable  Enable Disable
e24           Enable    Auto                  Down   Enable  Enable Disable
g1            Enable    Auto                  Down   Enable  Enable Disable
g2            Enable    Auto                  Down   Enable  Enable Disable
ch1           Enable                          Down   Disable N/A    Disable
ch2           Enable                          Down   Disable N/A    Disable
ch3           Enable                          Down   Disable N/A    Disable
ch4           Enable                          Down   Disable N/A    Disable
```

Interface	The port number.
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: - Mirror—Monitored port. - PC Mbr—Member of a LAG. - Probe—Probe port.
Admin Mode	The port control administration state. The port must be enabled for it to be allowed into the network. The default is enabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, the duplex mode and speed is set from the auto-negotiation process. (The maximum capability of the port is advertised during auto negotiate process.) Otherwise, this setting determines the port duplex mode and transmission rate. The default is **`Auto`**, representing Auto-Negotiate.
Physical Status	The actual port speed and duplex mode.
Link Status	Indicates whether the Link is up or down.
Link Trap	Indicates whether or not a trap is sent when link status changes. The default is enabled.

LACP Mode	Indicates whether Link Aggregation Control Protocol (LACP) is enabled or disabled on this port.
Flow Mode	Indicates whether flow control is enabled or disabled.

Related Commands

Command	Description
show interface ethernet	Displays detailed statistics for an interface or for the entire switch.
speed	Configures the speed of an Ethernet interface when not using auto-negotiation.
auto-negotiate	Enables auto-negotiation on a port.

Green Ethernet

This section describes the commands that enable Green Ethernet power saving features. Green Ethernet features are available on gigabit Ethernet ports operating in copper mode (not fiber mode) and include the following capabilities:

- Energy Detect Mode—Reduces chip power by forcing a port PHY into a low-power mode when the signal from a copper link partner is not present.
- Short Reach Mode—Tests the cable length at startup or when activated by an administrator. If a short cable is detected, the port is put into low-power mode. When the link goes down, low-power mode is disabled.

The Green Ethernet Mode properties are configurable per-port.

green-mode energy-detect

Use this command to enable Energy Detect mode on a gigabit Ethernet interface (in Interface Config mode) or on all gigabit Ethernet interfaces (in Global Config mode). Use the `no` form of the command to disable Energy Detect mode on the interface(s).

green-mode energy-detect [*interface*]

no green-mode energy-detect [*interface*]

Syntax Descriptions

Parameter	Description
interface	The port number.

Default

Energy Detect mode is enabled on all interfaces.

Command Modes

Global Config

Interface Config

Usage Guidelines

When the Energy Detect is enabled, the switch automatically enters the low-power mode when energy on the line is lost, and it resumes normal operation when energy is detected. When the port PHY is in low-power mode, the PHY wakes up after a certain period of time and sends link pulses to monitor for energy from the link partner. If energy is detected while the port is in wake-up mode, the switch returns the port to normal operation. When the wake-up period expires, the port returns to low-power mode.

Related Commands

Command	Description
show green-mode	Displays green-mode configuration and operational status for the switch.

show green-mode

Use this command to show the green mode configuration for a gigabit Ethernet interface or all gigabit Ethernet interfaces.

show green-mode [*interface*]

Syntax Descriptions

Parameter	Description
interface	The port number (**g1** or **g2**).

Command Modes

Privileged Exec

Examples

The following shows sample output for the command when no interface is specified.

```
(switch142E4E) #show green-mode

Interface   Opr Energy-Detect
---------   -----------------
g1          Active
g2          Active
```

The following shows sample output for the command when an interface is specified.

```
(switch1) #show green-mode g1

Energy Detect Admin Mode....................... Enabled
    Operational Status......................... Active
    Reason..................................... No Energy Detected
```

Interface	The gigabit Ethernet interface.
Opr Energy Detect	Indicates whether the feature is active on the interface.
Energy Detect Admin Mode	Indicates whether the feature is administratively enabled

Reason	Indicates the reason why the Energy Detect operational status is Active or Inactive: **No Energy Detected** might display when the Energy Detect operational status is Active and no energy is detected on the link. The following reasons might display when the Energy Detect operational status is Inactive. ▪ Port in Fiber mode—The administrative status might be active but the port is functioning in fiber mode. (Green Ethernet functionality applies only to copper ports.) ▪ Link is up—There is activity on the link. ▪ Admin Mode Disabled—Energy detect mode is administratively disabled.

Related Commands

Command	Description
green-mode energy-detect	Enables Energy Detect mode on a gigabit Ethernet interface or on all gigabit Ethernet interfaces.

Flow Control and Storm Control

This section describes the commands you use to enable flow control and storm control features.

storm-control broadcast

This command enables or disables broadcast storm recovery for a specific interface or for all interfaces. If the rate of Layer 2 broadcast traffic ingressing on an interface exceeds the configured threshold, traffic is dropped. Use the **no** form of the command to disable it.

storm-control broadcast

no storm-control broadcast

Default

Broadcast storm control is disabled.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
storm-control broadcast level	Configures the broadcast storm recovery threshold for an interface or all interfaces.
storm-control broadcast rate	Configures the broadcast storm recovery threshold for an interface or all interfaces.
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control broadcast level

This command enables and configures the broadcast storm recovery threshold for an interface or on all interfaces as percent of port speed. If broadcast storm recovery is active and the rate of Layer 2 broadcast traffic ingressing on an interface exceeds the configured threshold, the traffic is dropped, limiting the rate of broadcast traffic. In Global Config mode, the same percentage is set on all ports.

Use the `no` form of command to reset it to the default value.

```
storm-control broadcast level 0-100
no storm-control broadcast level
```

Syntax Descriptions

Parameter	Description
0–100	The percentage of port speed, above which traffic is dropped.

Default

broadcast level—10%.

Command Modes

Interface Config

Global Config

Related Commands

Command	Description
storm-control broadcast	Enables or disables broadcast storm recovery mode for an interface or all interfaces.
storm-control broadcast rate	Configures the broadcast storm recovery threshold for an interface or all interfaces.
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control broadcast rate

This command enables and configures the broadcast storm recovery threshold for an interface or all interfaces as packets per second. If broadcast storm recovery is active and the rate of Layer 2 broadcast traffic ingressing on an interface exceeds the configured threshold, the traffic is dropped. In Global Config mode the same rate is set on all ports.

Use the `no` form of command to delete the threshold.

storm-control broadcast rate ***0-14880000***

no storm-control broadcast rate

Syntax Descriptions

Parameter	Description
0–14880000	The broadcast traffic rate, in number of packets per second, above which traffic is dropped.

Default

No threshold is configured.

Command Modes

Interface Config

Global Config

Related Commands

Command	Description
storm-control broadcast	Enables broadcast storm recovery mode for an interface or all interfaces.
storm-control broadcast level	Configures the broadcast storm recovery threshold for an interface or all interfaces.
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control flowcontrol

Use this command to enable 802.3x flow control on all ports on the switch or on an individual port.

For half-duplex ports, backpressure is also enabled. If a traffic jam occurs, the switch sends collision frames on the port; transmitting stations are signaled to resend the packets. Flow control is not applicable in this case.

Use the `no` form of command to disable storm-control flow control globally on the switch or on a specific port.

```
storm-control flowcontrol

no storm-control flowcontrol
```

Default

Flow control is disabled on all port.

Command Modes

Global Config

Interface Config

Usage Guidelines

802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can cause high-priority and/or network control traffic loss.

Related Commands

Command	Description
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control multicast

This command enables multicast storm recovery mode for an interface or for all interfaces. If the multicast storm recovery is active and the rate of Layer 2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped.

Use the `no` form of the command to disable it. In Global Config mode, the same percentage is set on all ports.

```
storm-control multicast

no storm-control multicast
```

Default

Multicast storm recovery mode is disabled on all interfaces.

Command Modes

Interface Config

Global Config

Related Commands

Command	Description
storm-control multicast rate	Configures the multicast storm recovery threshold for an interface or all interfaces.

Command	Description
storm-control multicast level	Configures the multicast storm recovery threshold for an interface or all interfaces.
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control multicast rate

This command enables and configures the multicast storm recovery threshold for an interface or all interfaces as packets per second. If multicast storm recovery is active, and if the rate of Layer 2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped.

Use the `no` form of command to remove the rate threshold. In Global Config mode the same rate is set on all ports.

storm-control multicast rate ***0-14880000***

no storm-control multicast rate

Syntax Descriptions

Parameter	Description
0–14880000	The multicast traffic rate, in number of packets per second, above which traffic will be dropped.

Default

No rate is configured.

Command Modes

Interface Config

Global Config

Related Commands

Command	Description
storm-control multicast	Enables multicast storm recovery mode for an interface or all interfaces.
storm-control multicast level	Configures the multicast storm recovery threshold for an interface or all interfaces.
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control multicast level

This command configures the multicast storm recovery threshold for an interface or all interfaces as percent of port speed, and also enables broadcast storm recovery on that interface. If multicast storm recovery is active and the rate of Layer 2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. In Global Config mode the same level is set on all ports.

Use the `no` form of command to reset it to the default value.

```
storm-control multicast level 0-100
no storm-control multicast level
```

Syntax Descriptions

Parameter	Description
0–100	The multicast traffic threshold, as a percentage of port speed, above which traffic will be dropped.

Default

threshold—10% of port speed

Command Modes

Interface Config

Global Config

Related Commands

Command	Description
storm-control multicast	Enables multicast storm recovery mode for an interface or all interfaces.
storm-control multicast rate	Configures the multicast storm recovery threshold for an interface or all interfaces.
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control unicast

This command enables unicast storm recovery mode for an interface. If the unicast storm recovery is active and the rate of destination lookup failure packets ingressing on an interface exceeds the configured threshold, the traffic is dropped.

Use the `no` form of the command to disable this feature.

storm-control unicast

no storm-control unicast

Default

Unicast storm recovery mode is disabled.

Command Modes

Interface Config

Global Config

Related Commands

Command	Description
storm-control unicast level	Configures the unicast storm recovery threshold for an interface or all interfaces.
storm-control unicast rate	Configures the unicast storm recovery threshold for an interface or all interfaces.

Command	Description
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control unicast level

This command enables and configures the unicast storm recovery threshold for an interface or all interfaces as percent of port speed. If unicast storm recovery is active, and if the rate of destination lookup failure packets ingressing on an interface exceeds the configured threshold, the traffic is dropped. In Global Config mode the same level is set on all ports.

Use the `no` form of command to reset it to the default value (5).

storm-control unicast level ***0-100***

no storm-control unicast level ***0-100***

Syntax Descriptions

Parameter	Description
0–100	The unicast traffic threshold, as a percentage of port speed, above which traffic is dropped.

Default

threshold—10% of port speed

Command Modes

Interface Config

Global Config

Related Commands

Command	Description
storm-control unicast	Enables unicast storm recovery mode for an interface or all interfaces.

Command	Description
storm-control unicast rate	Configures the unicast storm recovery threshold for an interface or all interfaces.
show storm-control	Shows storm control configuration on a port or on all ports.

storm-control unicast rate

This command enables and configures the unicast storm recovery rate for an interface as packets per second. If unicast storm recovery is active and the rate of destination lookup failure packets ingressing on an interface exceeds the configured threshold, the traffic is dropped. In Global Config mode the same rate is set on all ports. Use the `no` form of command to remove the rate threshold.

storm-control unicast rate ***0-14880000***

no storm-control unicast rate

Syntax Descriptions

Parameter	Description
0–14880000	The unicast traffic rate, in number of packets per second, above which traffic is dropped.

Default

No unicast storm recovery rate is configured.

Command Modes

Interface Config

Global Config

Related Commands

Command	Description
storm-control unicast	Enables unicast storm recovery mode for an interface.

Command	Description
storm-control unicast level	Configures the unicast storm recovery threshold for an interface.
show storm-control	Shows storm control configuration on a port or on all ports.

show storm-control

This command shows storm control configuration on a port or on all ports.

show storm-control [**all** | *interface*]

no storm-control [**all** | *interface*]

Syntax Descriptions

Parameter	Description
all	Shows storm control information for all ports.
interface	Shows storm control information for the specified port only.

Command Modes

Privileged Exec

Examples

The following shows sample output from the command.

```
(Switch) #show storm-control

Broadcast Storm Control Mode................... Disable
Broadcast Storm Control Level.................. 5 percent
Multicast Storm Control Mode................... Disable
Multicast Storm Control Level.................. 5 percent
Unicast Storm Control Mode..................... Disable
Unicast Storm Control Level.................... 5 percent
802.3x Flow Control Mode....................... Disable
(Switch) #show storm-control all

        Bcast   Bcast    Mcast   Mcast    Ucast   Ucast
 Intf   Mode    Level    Mode    Level    Mode    Level
------ ------- -------- ------- -------- ------- --------
e1     Disable       5% Disable       5% Disable       5%
e2     Disable       5% Disable       5% Disable       5%
```

```
e3      Enable        5% Disable        5% Disable        5%
e4      Disable       5% Disable        5% Disable        5%
e5      Disable       5% Disable        5% Disable        5%
e6      Disable       5% Disable        5% Disable        5%
e7      Disable       5% Disable        5% Disable        5%
e8      Disable       5% Disable        5% Disable        5%
.
.
.
e24     Disable       5% Disable        5% Disable        5%
```

Related Commands

Command	Description
storm-control unicast	Enables unicast storm recovery mode for an interface or all interfaces.
storm-control multicast	Enables multicast storm recovery mode for an interface or all interfaces.
storm-control broadcast	This command enables broadcast storm recovery mode for an interface or all interfaces.

Link Aggregation

Link Aggregation allows one or more full-duplex Ethernet links to be aggregated together to form a Link Aggregation Group (LAG). This allows the switch to treat the LAG as if it is a single physical port, with improved fault tolerance and load-sharing capability.

A LAG interface can be either static or dynamic.

- Static LAG—Ports are assigned to a LAG by the administrator. The ports remain dedicated LAG members until configured otherwise.
- Dynamic LAG—Ports are designated as candidates for joining a LAG, and form it automatically by exchanging special frames called Link Aggregation Protocol Data Units (LACPDUs). When formed, the LAG might include only a subset of the eligible ports, depending on the port number limitations for LAGs and other factors. When not included as a member of a LAG, a port functions as standalone port.

All members of a LAG must be of the same type (static or dynamic).

This section describes the commands you use to configure link aggregation.

addport

This command adds a port to a LAG.

addport *logical interface*

Syntax Descriptions

Parameter	Description
logical interface	The LAG number that the port will be added to.

Command Modes

Interface Config

Examples

The following command adds interface e5 to LAG ch1:

```
(Switch) (config)#interface e5
(Switch) (Interface e5)#addport ch1
```

Related Commands

Command	Description
deleteport (Interface Config)	Deletes a port from a LAG.
deleteport (Global Config)	Deletes all configured member ports from a LAG.
show port-channel brief	Displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.

deleteport (Interface Config)

This command deletes the port from the LAG. The interface is the logical interface number of a configured LAG.

deleteport *logical interface*

Syntax Descriptions

Parameter	Description
logical interface	The LAG number that the port will be deleted from.

Command Modes

Interface Config

Examples

The following command deletes interface e5 from LAG ch1.

```
(Switch)  (config)#interface e5
(Switch)  (Interface e5)#deleteport ch1
```

Related Commands

Command	Description
addport	Adds a port to a LAG.
deleteport (Global Config)	Deletes all configured member ports from a LAG.
show port-channel brief	Displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.

deleteport (Global Config)

This command deletes all configured member ports from the LAG. The **all** parameter is only for completeness and pertains only to the members of the specified LAG interface.

deleteport {*logical interface*} **all**

Syntax Descriptions

Parameter	Description
logical interface	The LAG number that the port will be deleted from.
all	Specifies that all ports will be deleted from the LAG.

Command Modes

Global Config

Related Commands

Command	Description
addport	Adds a port to a LAG.
deleteport (Interface Config)	Deletes a port from a LAG.
show port-channel brief	Displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.

port lacpmode

This command enables the Link Aggregation Control Protocol (LACP) on a port. Use the `no` form of command to disable LACP on a port.

port lacpmode

no port lacpmode

Default

LACP mode operation is enabled on all ports.

Command Modes

Interface Config

Related Commands

Command	Description
port lacpmode all	Enables LACP on all physical ports.
port lacptimeout (Interface Config)	Sets the timeout on a physical interface of a particular device type.
port lacptimeout (Global Config)	Sets the timeout for all interfaces of a particular device type.

Command	Description
port-channel adminmode	Enables a LAG.

NOTE LACP mode is for the physical interface, when this port is configured as a member of static LAG then this configurable does not apply and this port can become an active member of the LAG. The LACP mode must be enabled for this port to participate in a dynamic LAG. If this mode is off and this port belongs to a dynamic LAG this port will fail to become an active member.

port lacpmode all

This command enables Link Aggregation Control Protocol (LACP) on all physical ports. Use the `no` form of command to disable LACP on all ports.

port lacpmode all

no port lacpmode all

Command Modes

Global Config

Related Commands

Command	Description
port lacpmode	Enables LACP on a port.
port lacptimeout (Interface Config)	Sets the timeout on a physical interface of a particular device type.
port lacptimeout (Global Config)	Sets the timeout for all interfaces of a particular device type.
port-channel adminmode	Enables a LAG.

port lacptimeout (Interface Config)

This command sets the timeout on a physical interface of a particular device type (actor or partner) to either long or short timeout. Use the `no` form of command to set the timeout to its default value on a physical interface of a specific device type (actor or partner).

```
port lacptimeout {actor | partner} {long | short}
```

```
no port lacptimeout {actor | partner}
```

Syntax Descriptions

Parameter	Description
actor	Configures the port timeout when the port LACP role is actor (actively sends LACPDUs on the network).
partner	Configures the port timeout when the port LACP role is partner (does not actively send LACPDUs, but responds to LACPDUs from actors).
long	Sets a long timeout period.
short	Sets a short timeout period.

Default

All actors and partners have a long timeout period.

Command Modes

Interface Config

Related Commands

Command	Description
port lacpmode	Enables LACP on a port.
port lacptimeout (Global Config)	Sets the timeout for all interfaces of a particular device type.

port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout. Use the `no` form of command to set the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

```
port lacptimeout {actor | partner} {long | short}
```

```
no port lacptimeout {actor | partner}
```

Syntax Descriptions

Parameter	Description
actor	Configures the port timeout when the port LACP role is actor (actively sends LACPDUs on the network).
partner	Configures the port timeout when the port's LACP role is partner (does not actively send LACPDUs, but responds to LACPDUs from actors).
long	Sets a long timeout period.
short	Sets a short timeout period.

Default

All actors and partners have a long timeout period.

Command Modes

Global Config

Related Commands

Command	Description
port lacpmode	Enables LACP on a port.
port lacptimeout (Interface Config)	Sets the timeout on a physical interface of a particular device type.

port-channel adminmode

This command enables a LAG. Use the `no` form of command to disable a LAG.

port-channel adminmode [**all**]

no port-channel adminmode

Syntax Descriptions

Parameter	Description
all	Configures all LAGs with the same administrative mode setting.

Default

By default all LAGs are administratively enabled.

Command Modes

Global Config

Related Commands

Command	Description
show port-channel brief	Displays the static capability of all LAG interfaces on the device as well as a summary of individual LAG interfaces.
show port channel	Displays an overview of all port-channels (LAGs) on the switch.

port-channel load-balance

This command selects the load-balancing option used on a LAG. Traffic is balanced on a LAG by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet and associating that pattern with a particular link. Use the `no` form of the command to reset it to the default value.

port-channel load-balance {**1** | **2**} {*interface* | **all**}

no port-channel load-balance {*interface* | **all**}

Syntax Descriptions

Parameter	Description
1	Load balances based on the source/destination MAC, VLAN, EtherType, and incoming port associated with all packets.
2	Load balances based on the source/destination IP and source/destination TCP/UDP Port fields of IP packets, and falls back to Source/Destination MAC for non IP packets.
interface	LAG identifier.
all	In Global Config Mode, this option applies the command to all currently configured LAGs.

Default

The default load-balance is method **2**.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
show port-channel brief	Displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.
show port channel	Displays an overview of all LAGs on the switch.

port-channel static

This command enables static mode on a LAG interface. By default the static mode for a new LAG is disabled; the LAG is dynamic. However, if the maximum number of allowable dynamic LAGs are already present in the system, static mode for a new LAG is enabled. You can only use this command on LAG interfaces. Use the `no` form of command to set the static mode on a particular LAG interface to the default value.

port-channel static

no port-channel static

Default

Ports are not configured as members of any static LAGs.

Command Modes

Interface Config

Related Commands

Command	Description
port-channel adminmode	Enables a LAG.
show port-channel brief	Displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.

show lacp actor

Use this command to display attributes for ports that are serving as a LAG actor; that is, they actively send LACPDUs to other potential LAG members to dynamically form a LAG.

show lacp actor {*interface* | **all**}

Syntax Descriptions

Parameter	Description
interface	Shows LACP actor attributes for the specified interface.

Parameter	Description
all	Shows LACP actor attributes for all interfaces.

Command Modes

Privileged EXEC

Examples

The following command shows LACP actor attributes for all interfaces.

```
(Switch) #show lacp actor all

         Sys    Admin   Port      Admin
 Intf  Priority  Key  Priority    State
------ -------- ----- -------- -----------
e1     32768    53    128      ACT|AGG|LTO
e2     32768    418   128      ACT|AGG|LTO
e3     32768    418   128      ACT|AGG|LTO
e4     32768    419   128      ACT|AGG|LTO
e5     32768    57    128      ACT|AGG|LTO
```

Intf	The port name.
Sys Priority	A nonconfigurable system priority assigned to the switch.
Admin Key	A number that determines the dynamic LAG(s) that the interface can join. All interfaces in a dynamic LAG must share the same administration key.
Port Priority	A nonconfigurable priority assigned to the port.

Admin State	Indicates the following values, separated by a vertical bar: ACT or PSU—The port LACP mode: ▪ ACT (Active mode)—The port sends LACPDUs on the switch at a configurable interval. ▪ PSU (Partner mode)—The port only responds to LACPDUs sent from active ports. AGG or IND—The port mode with respect to link aggregation: ▪ AGG (Aggregate mode)—The port is participating a link aggregation. ▪ IND (Individual mode)—The port is not participating in link aggregation and is functioning as an individual port. LTO or STO—The time after which an LACPDU is no longer valid: ▪ LTO (Long Timeout)—The LAG member receives less frequent LACP transmissions and retains the information longer. ▪ STO (Short Timeout)—The LAG member receives more frequent periodic LACP transmissions and more aggressively times-out the information it receives.

Related Commands

Command	Description
show lacp partner	Displays LACP partner attributes.
show port-channel brief	Displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.
show port channel	Displays an overview of all LAGs on the switch.

show lacp partner

Use this command to display attributes for interfaces that a serving as partners in a LAG (that is, they receive and respond to LACP requests from LAG actors).

show lacp actor {*interface* | **all**}

Syntax Descriptions

Parameter	Description
interface	Shows LACP partner attributes for the specified interface.
all	Shows LACP partner attributes for all interfaces.

Command Modes

Privileged EXEC

Examples

The following command shows LACP partner attributes for all interfaces.

```
(Switch) #show lacp partner all

       Sys      System       Admin Prt Prt     Admin
 Intf  Pri      ID            Key   Pri Id      State
------ --- ----------------- ----- --- ----- -----------
e1     0   00:00:00:00:00:00 0     0   0     ACT|AGG|LTO
e2     0   00:00:00:00:00:00 0     0   0     ACT|AGG|LTO
e3     0   00:00:00:00:00:00 0     0   0     ACT|AGG|LTO
e4     0   00:00:00:00:00:00 0     0   0     ACT|AGG|LTO
e5     0   00:00:00:00:00:00 0     0   0     ACT|AGG|LTO
```

Intf	The port name.
Sys Pri	The nonconfigurable system priority assigned to the switch in partner mode.
System ID	The MAC address of the LAG that the switch is a partner member of.
Admin Key	A number that determines the dynamic LAG(s) that the interface can join. All interfaces in a dynamic LAG must share the same administration key.

Port Priority	The port priority of the interface when serving as a LAG partner. The default priority is for a partner is 128. If the port is not serving as a LAG partner, the priority is 0.
Port ID	The port number assigned to the port as a LAG partner member.
Admin State	Indicates the following values, separated by a vertical bar: ACT or PAS—The port LACP mode: ▪ ACT (Actor mode)—The port sends LACPDUs on the switch at a configurable interval. ▪ PRT (Partner mode)—The port only responds to LACPDUs sent from active ports. AGG or IND—The port mode with respect to link aggregation: ▪ AGG (Aggregate mode)—The port can participate in link aggregation. ▪ IND (Individual mode)—The port cannot participate in link aggregation. LTO or LTS—The time after which an LACPDU is no longer valid: ▪ LTO (Long Timeout)—The LAG member is configured to receive less frequent LACP transmissions and retains the information longer. ▪ STO (Short Timeout)—The LAG member is configured to receive more frequent periodic LACP transmissions and more aggressively times-out information it receives.

Related Commands

Command	Description
show port-channel brief	Displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.

Command	Description
show port channel	Displays an overview of all LAGs on the switch.

show port-channel

This command displays an overview of all LAGs on the switch.

show port-channel {*logical interface* | **all**}

Syntax Descriptions

Parameter	Description
logical interface	The LAG ID.
all	Displays information on all LAGs.

Command Modes

Privileged EXEC

Examples

The following example shows output for all configured LAGs.

```
(Switch) #show port-channel all

Log.       Channel              Adm.      Mbr    Device/        Port      Port
Intf        Name          Link  Mode Type Ports  Timeout        Speed     Active
------ --------------- ------ ---- ---- ------ ------------- --------- -------
ch1    lag1            Down   En.  Dyn. e2     actor/long     Auto      False
                                               partner/long
                                          e3   actor/long     Auto      False
                                               partner/long
ch2    lag2            Down   En.  Stat e4     actor/long     Auto      False
                                               partner/long
```

Logical Intf	The port name.
Channel Name	The LAG name.
Link	Indicates whether the LAG is up or down.

Admin Mode	Indicates whether the LAG is administratively enabled or disabled.
Type	Indicates whether the LAG is a dynamic or static LAG.
Mbr Ports	The ports that are current members of the LAG.
Device/Timeout	Indicates the time after which an LACPDU is no longer valid when the port is in the active and partner roles: ▪ Long—The LAG member is configured to receive less frequent LACP transmissions and retain the information longer. ▪ Short—The LAG member is configured to receive more frequent periodic LACP transmissions and more aggressively time-out the information it receives.
Port Speed	Indicates whether the LAG is configured to autonegotiate the port speed (Auto) for all its member ports, or indicates the configured value (10/100/1000 Mbps) for all member ports.
Port Active	Indicates whether the port is currently active as a LAG member.

Related Commands

Command	Description
show port-channel brief	Displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.

show port-channel brief

This command displays the static capability of all LAG interfaces on the device and a summary of individual LAG interfaces.

```
show port-channel brief
```

Command Modes

Privileged EXEC

Examples

The following command shows information for all LAGs.

```
(Switch) #show port-channel brief

Logical   Port-Channel Name Link State  Trap     Type    Mbr Ports ActivePorts
Interface                               Flag
--------- ----------------- ---------- -------- ------- --------- ------------
ch1       lag1              Down       Enabled  Dynamic e2 , e3
ch2       lag2              Down       Enabled  Static  e4
```

Logical Intf	The port name.
Port-Channel Name	The LAG name.
Link State	Indicates whether the LAG is up or down.
Trap Flag	Indicates whether a trap is generated when the Link State changes.
Type	Indicates whether the LAG is a dynamic or static LAG.
Mbr Ports	The ports that are members of the LAG, whether or not they are currently active in the LAG.
Active Ports	The ports that are active ports on the LAG.

Related Commands

Command	Description
show port channel	Displays an overview of all port-channels (LAGs) on the switch.

show port-channel system priority

Use this command to display the LAG system priority.

show port-channel system priority

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
(Switch) #show port-channel system priority

System Priority................................ 32768
```

Related Commands

Command	Description
show port-channel brief	Displays the static capability of all LAG interfaces on the device as well as a summary of individual LAG interfaces.
show port channel	Displays an overview of all LAGs on the switch.

4

VLAN Management

This chapter describes how to configure virtual LANs (VLANs), voice-over-IP functionality, the link-layer discover protocol (LLDP), and media VLAN capabilities.

It contains the following topics:

- **VLAN**
- **LLDP-MED**
- **Auto-VoIP**
- **Media VLAN**

VLAN

This section describes the commands you use to create VLANs and configure port VLAN memberships.

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number. Use the **no** form of the command to delete the specified VLAN.

vlan *2-4094*

no vlan *2-4094*

Syntax Descriptions

Parameter	Description
2–4094	The VLAN ID.

Command Modes

VLAN Config

Related Commands

Command	Description
vlan default	Configures the default VLAN on the switch.

vlan database

Use the command in Global Config mode to enter the VLAN Config mode.

```
vlan database
```

Command Modes

Privileged Exec

Related Commands

Command	Description
vlan	Creates a new VLAN.

vlan default

Use this command to configure the default VLAN on the switch. To reset the default VLAN to VLAN 1, use the `no` form of this command. This command does not create a VLAN; the VLAN that you are going to configure as the default VLAN must be created prior identifying it as the default VLAN by using this command.

```
vlan default vlan-id

no vlan default
```

Syntax Descriptions

Parameter	Description
2–4094	The VLAN ID.

Default

The default VLAN is VLAN 1.

Command Modes

VLAN Config

Related Commands

Command	Description
vlan	Creates a VLAN and assigns it an ID.

vlan priority

Use this command to configure the default IEEE 802.1p port priority assigned for untagged packets for a specific interface.

vlan priority *priority*

Syntax Descriptions

Parameter	Description
priority	The 802.1p priority value. The range is 0–7.

Default

priority—0

Command Modes

Interface Config

Related Commands

Command	Description
vlan	Creates a VLAN and assigns it an ID.

switchport access vlan

Use this command to configure the VLAN ID when the interface is in access mode. (In Access mode, the port belongs to one or more VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).) To reset the parameter to the default value, use the `no` form of this command.

switchport access vlan *vlan-id*

no switchport access vlan

Syntax Descriptions

Parameter	Description
vlan-id	The VLAN ID.

Default

The VLAN ID of the default VLAN.

Command Modes

Interface Config

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.

switchport general acceptable-frame-type tagged-only

Use this command to configure the Acceptable Frame Type Admit Only VLAN Tagged for a General port. To enable untagged frames at ingress, use the `no` form of this command.

switchport general acceptable-frame-type tagged-only

no switchport general acceptable-frame-type tagged-only

Default

Both tagged and untagged frames are accepted.

Command Modes

Interface Config

Related Commands

Command	Description
switchport general allowed vlan	Adds VLANs to or removes VLANs from a general port.
switchport general pvid	Configures the Port VLAN ID (PVID) when the interface is in general mode.

switchport general allowed vlan

Use this command to add VLANs to or remove VLANs from a general port.

switchport general allowed vlan {add *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}

Syntax Descriptions

Parameter	Description
vlan-list	Specify the VLAN ID of each VLAN, separated by a space.
tagged	Configures the port to admit frames tagged with this VLAN ID and forward them with the VLAN tag. Ports are often configured as tagged when they connect to other switches or routers that handle VLAN-tagged traffic.
untagged	Configures the port to admit frames from this VLAN and forward them without a VLAN tag. Ports are often configured as untagged when they connect to hosts or peripherals that might not manage VLAN-tagged traffic.

Default

VLANs are added as untagged VLANs.

Command Modes

Interface Config

Related Commands

Command	Description
switchport general acceptable-frame-type tagged-only	Configures the Acceptable Frame Type to Admit Only VLAN Tagged for a General Port.
switchport general pvid	Configures the Port VLAN ID (PVID) when the interface is in general mode.

switchport general pvid

Use this command to configure the Port VLAN ID (PVID) when the interface is in general mode. (Use the `switchport mode general` command to set the VLAN membership mode of a port to `general`.) To configure the default value, use the `no` form of this command. The VLAN ID might belong to a non-existent VLAN.

switchport general pvid *vlan-id*

no switchport general pvid *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The VLAN ID to be used as the PVID.

Default

The default PVID is 1. If the VLAN ID is non-existent, then VLAN ID is set to the reserved VLAN, 4094.

Command Modes

Interface Config

Related Commands

Command	Description
switchport general allowed vlan	Adds VLANs to or remove VLANs from a general port.

switchport general ingress-filtering disable

Use this command to disable port ingress filtering. To enable ingress filtering on a port, use the **no** form of this command.

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Default

Ingress filtering is enabled.

Command Mode

Interface Config

switchport trunk allowed vlan

Use this command to add or remove a trunk port as a tagged member of one or more VLANs.

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

Syntax Descriptions

Parameter	Description
vlan-list	The VLAN IDs to be added to or removed from the port VLAN memberships, separated by a space.

Command Mode

Interface Config

Related Commands

Command	Description
switchport trunk native-vlan	Configures the VLAN ID of the native VLAN for the port.
show interfaces switchport	Displays the switchport configuration.

switchport mode

Use this command to configure the VLAN membership mode of a port. To reset the mode to the appropriate default for the switch, use the `no` form of this command.

switchport mode {**access** | **trunk** | **general**}

no switchport mode

Syntax Descriptions

Parameter	Description
access	An access port is a member of only one VLAN and its PVID is set to that VLAN ID. The port Accept Frame Type is set to Accept Only Untagged and Priority Tagged frames. An access port only egresses untagged packets.

Parameter	Description
trunk	A trunk port might belong to multiple VLANs, but can be untagged only in one VLAN and might be tagged on 0 or more VLANs. A trunk port's Accept Frame Type is: ▪ Admit All Frame if it is a member of both untagged and tagged VLANs ▪ Admit Only Untagged/Priority Frame if it is a member of one untagged VLAN and not a member of any other VLANs. ▪ Admit Only VLAN-Tagged Frame if it is a member of only tagged VLAN(s) and not a member of an untagged VLAN. A trunk only egresses tagged packets.
general	The port is a full-support 802.1q VLAN interface. All VLAN features can be configured on a port in general mode.

Default

All ports are Trunk ports.

Command Modes

Interface Config

Related Commands

Command	Description
switchport access vlan	Configures the VLAN ID when the interface is in access mode.
switchport general allowed vlan	Adds VLANs to or remove VLANs from a general port.
switchport trunk allowed vlan	Add and remove a trunk port as tagged member of one or more VLANs.
switchport trunk native-vlan	Sets the native VLAN for an interface in trunk mode.

switchport trunk native-vlan

Use this command to set the native VLAN for an interface in trunk mode. The native VLAN identifies the single untagged VLAN membership for a trunk port.

switchport trunk native-vlan *1-4094*

Syntax Descriptions

Parameter	Description
1–4094	The VLAN ID of the native VLAN.

Command Modes

Interface Config

Related Commands

Command	Description
switchport trunk allowed-vlan	Adds and removes a trunk port as tagged member of one or more VLANs.
show interfaces switchport	Displays switchport configuration.

show interfaces switchport

Use this command to display VLAN membership and related configuration parameters for the port.

show interfaces switchport *interface*

Syntax Descriptions

Parameter	Description
interface	The interface ID.

Command Modes

Privileged Exec

Examples

The following example shows switchport configuration for an interface.

```
(switch) #show interfaces switchport e1

Port: e1
VLAN Membership mode:Trunk Mode

Operating parameters:
PVID: 1
Ingress Filtering: Enabled
Acceptable Frame Type: Admit All
Default Priority: 0

Port e1 is member in:

VLAN    Name                              Egress rule    Type
----    --------------------------------- -----------    --------
1       Default                           Untagged       Default

Static configuration:
PVID: 1
Ingress Filtering: Enabled
Acceptable Frame Type: Admit All

Port e1 is statically configured to:

VLAN    Name                              Egress rule
----    --------------------------------- -----------
1       Default                           Untagged
```

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.

LLDP-MED

This section describes the commands used to configure and display information on the Link-Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED).

lldp med

Use this command to enable LLDP-MED on an interface. Use the **no** form of the command to disable LLDP-MED.

```
lldp med

no lldp med
```

Default

LLDP-MED is disabled on all interfaces.

Command Modes

Interface Config

Related Commands

Command	Description
lldp med all	Enables LLDP-MED on all ports.
show lldp med	Displays a summary of the current LLDP-MED configuration.

lldp med all

Use this command to enable LLDP-MED on all the ports. Use the **no** form of the command to disable LLDP-MED.

```
lldp med

no lldp med
```

Default

LLDP-MED is globally disabled.

Command Modes

Global Config

Related Commands

Command	Description
lldp med	Enables LLDP-MED on an interface.
show lldp med	Displays a summary of the current LLDP-MED configuration.

lldp med confignotification

Use this command to configure a port to send the topology change notifications. Use the `no` form of the command to disable notifications.

lldp med confignotification

no lldp med confignotification

Default

The sending of topology change notifications is disabled on all interfaces.

Command Modes

Interface Config

Related Commands

Command	Description
lldp med confignotification all	Configures all ports to send the topology change notification.
show lldp med	Displays a summary of the current LLDP-MED configuration.

lldp med confignotification all

Use this command to configure all ports to send topology change notifications. Use the `no` form of the command to disable notifications.

lldp med confignotification

no lldp med confignotification

Default

The sending of topology change notifications is globally disabled.

Command Modes

Global Config

Related Commands

Command	Description
lldp med confignotification	Configures an individual port to send topology change notifications.
show lldp med	Displays a summary of the current LLDP-MED configuration.

lldp med inventory-tlv asset-id

Use this command to set the asset ID of the platform.

lldp med inventory-tlv asset-id *asset-id-string*

Syntax Descriptions

Parameter	Description
asset-id-string	The asset-id text.

Default

No asset-id string is configured.

Command Modes

Global Config

Related Commands

Command	Description
show lldp med	Displays a summary of the current LLDP-MED configuration.

lldp med location-tlv co-ordinate

Use this command to set coordinate-based Location Type Length Values (TLVs), as defined by RFC3825. Use the `no` form of the command to clear the location details.

lldp med location-tlv co-ordinate *value*

no lldp med location-tlv co-ordinate

Syntax Descriptions

Parameter	Description
value	The location coordinates expressed as 16 octets in hexadecimal, as follows: xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx Refer to RFC 3825 for details.

Command Modes

Global Config

Related Commands

Command	Description
lldp med location-tlv civic-addr	Sets the civic address-based Location TLV to specify the location of the switch.
lldp med location-tlv elin-addr	Sets the ELIN address-based Location TLV to specify an emergency number.
show lldp med location-tlv	Shows the details of the Location TLVs configured.

lldp med location-tlv civic-addr

Use this command to set the civic address-based Location TLV . Use the `no` form of the command to clear the location details.

lldp med location-tlv civic-addr country *country-code CA-type CA-value* [*CA-type CA-value*]

lldp med location-tlv civic-addr

Syntax Descriptions

Parameter	Description
country-code	A two-character code, as defined by ISO 3166. For example, FR (France), DE (Germany), or IN (India).
CA-type	The civic address type. CA-type values can be as follows: ▪ 3 = city. ▪ 6 = street (name). ▪ 25 = building name. Multiple CA-type and value pairs can be entered in a single command.
CA-value	The civic address value associated with the specified CA type. Each value can be 0–250 characters.

Command Modes

Global Config

Examples

The following example configures the country, city, street name, and building name.

```
(switch) (Config)#lldp med location-tlv civic-addr country us 3 Baltimore 6
Charles 25 LincolnTowers
```

Usage Guidelines

Every time this command is executed, the city, street, and building parameters are updated. If any one of these parameters are left out of the command when it is executed, that parameter will be empty when it is stored in the configuration.

Related Commands

Command	Description
lldp med location-tlv co-ordinate	Sets the coordinate-based Location TLV, as defined by RFC3825.
lldp med location-tlv elin-addr	Sets the ELIN-address-based Location TLV to specify the emergency number.
show lldp med location-tlv	Shows the details of the Location TLVs configured.

lldp med location-tlv elin-addr

Use this command to set the Emergency Location Identification Number (ELIN) to be advertised in Location TLVs. Use the **no** form of the command to reset the ELIN to NULL.

lldp med location-tlv elin-addr *emergency-number*

no lldp med location-tlv elin-addr

Syntax Descriptions

Parameter	Description
emergency-number	The ELIN number. The range is 10–25 numeric characters.

Default

No emergency number is configured.

Command Modes

Global Config

Examples

The following example configures and ELIN address.

```
(switch) (Config)#lldp med location-tlv elin-addr 5622086169
```

Related Commands

Command	Description
lldp med location-tlv co-ordinate	Sets the coordinate-based Location TLV, as defined by RFC3825.
lldp med location-tlv civic-addr	Sets the civic address-based Location TLV to specify the location of the switch.
show lldp med location-tlv	Shows the details of the Location TLVs configured.

lldp med location-tlv type

Use this command to set the location TLV type to use in the LLDP-MED Location TLV advertisement.

```
lldp med location-tlv type {ELIN | civic | coordinate}
```

Syntax Descriptions

Parameter	Description
ELIN	Emergency Location Identification Number of the switch.
civic	Geographic description of the location, such as city, street name, and building name.
coordinate	GPS coordinates in hexadecimal format.

Default

The default location TLV type is Civic.

Command Modes

Global Config

Related Commands

Command	Description
lldp med location-tlv co-ordinate	Sets the coordinate-based Location TLV, as defined by RFC3825.
lldp med location-tlv civic-addr	Sets the civic address-based Location TLV to specify the location of the switch.
lldp med location-tlv elin-addr	Sets the ELIN address-based Location TLV to specify the emergency number.
show lldp med location-tlv	Shows the details of the Location TLVs configured.

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP-MED set are transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs). You can enter the command with no optional key words to include all TLV types.

Use the `no` form of the command to remove the TLV. You can enter the command without any key words to remove all TLV types.

lldp med transmit-tlv [**capabilities**][**inventory**][**location**][**network-policy**]

no lldp med transmit-tlv[**capabilities**][**inventory**][**location**][**network-policy**]

Syntax Descriptions

Parameter	Description
Capabilities	Transmit the LLDP-MED capabilities TLV.
Inventory	Transmit the LLDP-MED inventory TLV.
Location	Transmit the LLDP-MED location TLV.
network-policy	Transmit the LLDP-MED network policy TLV.

Default

The capabilities and network policy TLVs.

Command Modes

Interface Config

Related Commands

Command	Description
lldp med transmit-tlv all	Specifies which optional TLVs in the LLDP-MED set are transmitted in the LLDPDUs for all the ports.
show lldp med	Displays a summary of the current LLDP-MED configuration.

lldp med transmit-tlv all

Use this command to specify which optional TLV) in the LLDP-MED set are transmitted in the LLDPDUs for all the ports. You can enter the command with no optional key words to include all TLV types.

Use the `no` form of the command to remove the configured TLV. You can enter the command with no optional key words to remove all TLV types from all ports.

lldp med transmit-tlv all [**capabilities**][**inventory**][**location**][**network-policy**]

no lldp med transmit-tlv all [**capabilities**][**inventory**][**location**][**network-policy**]

Syntax Descriptions

Parameter	Description
Capabilities	Transmit the LLDP-MED capabilities TLV.
Inventory	Transmit the LLDP-MED inventory TLV.
Location	Transmit the LLDP-MED location TLV.
network-policy	Transmit the LLDP-MED network policy TLV.

Default

The capabilities and network policy TLVs are transmitted.

Command Modes

Global Config

Related Commands

Command	Description
lldp med transmit-tlv	Specifies which optional TLVs in the LLDP-MED set are transmitted in the LLDPDUs for specific ports.
show lldp med	Displays a summary of the LLDP-MED configuration.

show lldp med

Use this command to display a summary of the current LLDP-MED configuration.

show lldp med

Command Modes

Privileged Exec

Examples

The following example shows command output.

```
(switch) #show lldp med

LLDP MED Global Configuration

Fast Start Repeat Count:  3
Device Class:  Network Connectivity
```

Related Commands

Command	Description
show lldp med local-device detail	Displays detailed information about the LLDP-MED data that a specific interface transmits.

show lldp med location-tlv

Use this command to show the details of the Location TLVs.

show lldp med location-tlv

Command Modes

Privileged Exec

Examples

The following example shows command output.

```
(switch) #show lldp med location-tlv

LLDP MED Location Configuration


Location Sub Type.............................. civic
Emergency Number(ELIN)......................... 5622086169
Civic Address Information

country........................................ us
 CA-TYPE    CA-VALUE
 -------    --------------------
 3          Baltimore
 6          Charles
 25         LincolnTowers
Coordinates....................................
23:51:13:09:01:23:12:00:23:51:13
:09:01:23:12:00
```

Related Commands

Command	Description
lldp med location-tlv co-ordinate	Sets the coordinate-based Location TLV, as defined by RFC3825.
lldp med location-tlv civic-addr	Sets the civic address-based Location TLV to specify the location of the switch.
lldp med location-tlv elin-addr	Sets the ELIN address-based Location TLV to specify the emergency number.

show lldp med local-device detail

Use this command to display detailed information about the LLDP-MED data that a specific interface transmits.

show lldp med local-device detail *interface*

Syntax Descriptions

Parameter	Description
interface	The port number.

Command Modes

Privileged Exec

Examples

The following command shows LLDP-MED details for port e1:

```
(Switch) #show lldp local-device detail e1

LLDP Local Device Detail

Interface: e1

Chassis ID Subtype: MAC Address
Chassis ID: 00:02:BC:02:02:02
Port ID Subtype: MAC Address
Port ID: 01:02:03:04:05:06
System Name:
System Description: Emulation, 0.0.0.0,
 Linux 2.6.20-16-server
Port Description:
System Capabilities Supported: bridge
System Capabilities Enabled: bridge
Management Address:
    Type: 802
    Address: 00:02:BC:02:02:02
```

Related Commands

Command	Description
show lldp med	Displays a summary of the current LLDP-MED configuration.

show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP-MED data to the system. You can show information about LLDP-MED remote data received on all valid LLDP interfaces or on a specific physical interface.

show lldp med remote-device {*interface* | **all**}

Syntax Descriptions

Parameter	Description
interface	The interface ID.
all	Shows data received on all LLDP interfaces.

Command Modes

Privileged Exec

Examples

The following command shows LLDP remote data received on all interfaces.

```
(Switch) #show lldp remote-device all
LLDP Remote Device Summary

Local
Interface  RemID   Chassis ID         Port ID             System Name
-------    ------- -----------------  ------------------   -----------------
-
e1
e2
e3
e4
e5
e6
e7         2      00:FC:E3:90:01:0F  00:FC:E3:90:01:11
e7         3      00:FC:E3:90:01:0F  00:FC:E3:90:01:12
e7         4      00:FC:E3:90:01:0F  00:FC:E3:90:01:13
e7         5      00:FC:E3:90:01:0F 00:FC:E3:90:01:14
e8
.
.
.
e24
```

Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

Related Commands

Command	Description
show lldp med remote-device detail	Displays detailed information about remote devices that transmit current LLDP-MED data to an interface on the system.

show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP-MED data to an interface on the system.

show lldp med remote-device detail {*interface* | **all**}

Syntax Descriptions

Parameter	Description
interface	The interface ID.
all	Shows data for all remote LLDP devices.

Command Modes

Privileged Exec

Examples

The following command shows LLDP remote device information received on port e7.

```
(Switch) #show lldp remote-device detail e7
LLDP Remote Device Detail Local Interface: e7
Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled: Time to Live: 24 seconds
```

Related Commands

Command	Description
show lldp med remote-device	Displays the summary information about remote devices that transmit current LLDP-MED data to the system.

Auto-VoIP

The Auto-VoIP feature identifies voice-over-Internet Protocol streams in Ethernet switches and provides them with a better class-of-service (CoS) than ordinary traffic. The switch supports two types of Auto-VoIP:

- Protocol-based—Identifies a VoIP session using the Session Initiation Protocol (SIP) and H.323 control traffic, and assigns these packets the highest priority on the voice VLAN.
- OUI-based—Defines an Organizationally Unique Identifier (OUI, the first three bytes of the MAC address) to be detected in client packets and assigns the configured priority value.

This section describes how to configure Auto-VoIP.

auto-voip oui

Use this command to configure a new Organizationally Unique Identifier (OUI). Use the `no` form of the command to delete the configured OUI.

auto-voip oui *hh:hh:hh* **oui-desc** *description*

no auto-voip oui *oui*

Syntax Descriptions

Parameter	Description
oui	The identifier, specified as three hexadecimal pairs separated by a colon.
oui-desc	A text string that identifies the OUI.

Command Modes

Global Config

Example

```
(switch) (Config)#auto-voip oui aa:bb:cc oui-desc signalTel
```

Related Commands

Command	Description
show auto-voip oui-table	Shows all configured OUIs.

auto-voip oui-based

Use this command to enable the OUI-based VoIP Profile on an interface. Use the `no` form of the command to disable the profile.

auto-voip oui-based

no auto-voip oui-based

Default

OUI-based VoIP is disabled on all interfaces.

Command Modes

Interface Config

Related Commands

Command	Description
auto-voip oui-based all	Enables the VoIP Profile on all the interfaces of the switch.
auto-voip oui-prioirity	Configure the class-of-service priority assigned to OUI-based VoIP traffic.
auto-voip oui-vlan	Configures the VLAN to be assigned to OUI-based VoIP traffic.
show auto-voip oui-based	Displays the VoIP Profile settings on an interface or interfaces.

auto-voip oui-based all

Use this command to enable the OUI VoIP profile on all switch interfaces. Use the `no` form of the command to disable the profile.

auto-voip oui-based all

no auto-voip oui-based all

Default

The OUI-based VoIP profile is globally disabled.

Command Modes

Global Config

Related Commands

Command	Description
auto-voip oui-based	Enables the VoIP Profile on an interface.
auto-voip oui-prioirity	Configure the class-of-service priority assigned to OUI-based VoIP traffic.

Command	Description
auto-voip oui-vlan	Configures the VLAN to be assigned to OUI-based VoIP traffic.
show auto-voip oui-based	Displays the VoIP Profile settings on the interface or interfaces.

auto-voip oui-priority

Use this command to configure the class-of-service priority assigned to OUI-based VoIP traffic. Use the `no` form of the command to reset the priority to the default, the highest priority queue available on the system.

auto-voip oui-priority *priority*

no auto-voip oui-priority

Syntax Descriptions

Parameter	Description
priority	A class of service priority level to assign to OUI-based VoIP packets. The range is 0-7, with 0 being the highest priority.

Default

The highest priority queue available in the system.

Command Modes

Global Config

Related Commands

Command	Description
auto-voip oui-based	Enables the VoIP Profile on an interface.
auto-voip oui-based all	Enables the VoIP Profile on all the interfaces of the switch.

Command	Description
auto-voip oui-vlan	Configures the VLAN to be assigned to OUI-based VoIP traffic.
show auto-voip oui-based	Displays the VoIP Profile settings on the interface or interfaces.

auto-voip oui-vlan

Use this command to configure the VLAN to be assigned to OUI-based VoIP traffic. Use the `no` form of the command to reset the VLAN to the default (no VLAN).

```
auto-voip oui-priority priority

no auto-voip oui-priority
```

Syntax Descriptions

Parameter	Description
priority	A class of service priority level to assign to OUI-based VoIP packets. The range is 0-7, with 0 being the highest prioirity.

Default

The highest priority queue available in the system.

Command Modes

Global Config

Related Commands

Command	Description
auto-voip oui-based	Enables the VoIP Profile on an interface.
auto-voip oui-based all	Enables the VoIP Profile on all the interfaces of the switch.

Command	Description
auto-voip oui-prioirity	Configure the class-of-service priority assigned to OUI-based VoIP traffic.
show auto-voip oui-based	Displays the VoIP Profile settings on the interface or interfaces.

auto-voip protocol-based

Use this command to enable the protocol-based VoIP Profile on an interface. Use the `no` form of the command to disable the profile.

auto-voip protocol-based

no auto-voip protocol-based

Default

The protocol-based VoIP profile is disabled on all interfaces.

Command Modes

Interface Config

Related Commands

Command	Description
auto-voip protocol-based all	Enables the VoIP Profile on all the interfaces of the switch.
show auto-voip protocol-based	Displays the VoIP Profile settings on the interface or interfaces of the switch.
show auto-voip sessions	Displays the currently running Auto-VoIP sessions on an interface or interfaces.

auto-voip protocol-based all

Use this command to enable the protocol-based VoIP profile on all switch interfaces. Use the `no` form of the command to disable the profile.

auto-voip protocol-based all

no auto-voip protocol-based all

Default

The protocol-based VoIP profile is globally disabled.

Command Modes

Global Config

Related Commands

Command	Description
auto-voip protocol-based	Enables VoIP Profile on an interface.
show auto-voip protocol-based	Displays the VoIP Profile settings on the interface or interfaces of the switch.
show auto-voip sessions	Displays the currently running Auto-VoIP sessions on an interface or interfaces.

show auto-voip oui-based interface

Use this command to display the VoIP profile settings for the specified VoIP type on an interface or on all switch interfaces.

```
show auto-voip oui-based interface {interface | all}
```

Syntax Descriptions

Parameter	Description
interface	Shows Auto VoIP information for the specified port.
all	Shows Auto VoIP information for all ports.

Command Modes

Privileged Exec

Examples

The following example shows command output.

```
(switch) #show auto-voip oui-based interface e1

Interface  Auto VoIP Mode Port Status
---------  -------------- -----------
e1         Enabled        Down
```

AutoVoIP Mode	The Auto VoIP mode on the interface.
Port Status	The operational status of the port.

Related Commands

Command	Description
auto-voip oui-based	Enables the VoIP Profile on an interface.
auto-voip oui-based all	Enables the VoIP Profile on all the interfaces of the switch.
show auto-voip sessions	Displays the currently running protocol-based Auto VoIP sessions on an interface or interfaces.

show auto-voip oui-table

Use this command to show all configured Organizationally Unique Identifiers (OUIs) on the switch.

show auto-voip oui-table

Command Modes

Privileged Exec

Examples

The following example shows command output.

```
(switch) #show auto-voip oui-table

OUI           Status         Description
---------     ----------     ---------

00:01:E3      Default        SIEMENS
00:03:6B      Default        CISCO1
00:12:43      Default        CISCO2
00:0F:E2      Default        H3C
00:60:B9      Default        NITSUKO
00:D0:1E      Default        PINTEL
00:E0:75      Default        VERILINK
00:E0:BB      Default        3COM
00:04:0D      Default        AVAYA1
00:1B:4F      Default        AVAYA2
AA:BB:CC      Configured     signalTel
```

Related Commands

Command	Description
auto-voip oui	Configures a new OUI.
show auto-voip oui-based interface	Displays the VoIP profile settings for the specified VoIP type on an interface or on all switch interfaces.
show auto-voip oui-based interface	Displays the Auto VoIP configuration of an interface or all interfaces.

show auto-voip protocol-based interface

Use this command to display the profile-based VoIP settings for an interface or for all switch interfaces.

show auto-voip protocol-based interface {*interface* | **all**}

Syntax Descriptions

Parameter	Description
interface	Shows Auto VoIP information for the specified port.

Parameter	Description
all	Shows Auto VoIP information for all ports.

Command Modes

Privileged Exec

Examples

The following example shows command output.

```
(switch) #show auto-voip protocol-based interface e1

Interface  Auto VoIP Mode Traffic Class Port Status
---------  -------------- ------------- -----------
e1         Enabled        7             Up
```

AutoVoIP Mode	The Auto VoIP mode on the interface.
Traffic Class	The CoS Queue or Traffic Class to which all VoIP traffic is mapped. This is not configurable and defaults to the highest CoS queue available in the system for data traffic.
Port Status	The operational status of the port.

Related Commands

Command	Description
auto-voip protocol-based	Enables the VoIP Profile on an interface.
auto-voip protocol-based all	Enables the VoIP Profile on all the interfaces of the switch.
show auto-voip sessions	Displays the currently running Auto-VoIP sessions on an interface or interfaces.

show auto-voip sessions

Use this command to display the currently running protocol based Auto-VoIP sessions on all switch interfaces.

show auto-voip sessions

Command Modes

Privileged Exec

Examples

The following example shows command output.

```
(switch) (Config)#exit
(switch) #show auto-voip sessions

Source IP       Destination IP  Source Port Destination Port Protocol
--------------- --------------- ----------- ---------------- --------
```

Related Commands

Command	Description
auto-voip protocol-based	Enables the protocol-based VoIP Profile on an interface.
show auto-voip protocol-based	Displays the VoIP Profile settings on the interface or interfaces.

Media VLAN

This section describes the commands that configure the Media VLAN feature that enables switch ports to carry voice, video, and signaling traffic with an assigned priority value. Assigning different priorities to traffic enables separation of media and data traffic coming into a port.

The switch uses the IP-DSCP or 802.1p value in packets from media devices to assign this traffic to high priority queues.

media-vlan (Global Config)

Use this command to enable the Media-VLAN capability on the switch. Use the **no** form of command to disable the Media-VLAN capability on the switch.

media-vlan

no media-vlan

Default

The Media-VLAN capability is disabled.

Command Modes

Global Config

Related Commands

Command	Description
show media-vlan	Shows global Media VLAN status and configuration details on an interface.

media-vlan (Interface Config)

Use this command to enable the Media-VLAN capability on the interface. Use the `no` form of the command to disable the Media-VLAN capability on the interface. The details configured through this command becomes the Network Policy for LLDP-MED.

media-vlan {**voice** | **voice-signaling** | **video-signaling** | **video-conferencing** | **streaming-video** | **soft-phone** | **guest-voice-signaling** | **guest-voice**}**[vlan** *vlan-id*][**dot1p** *priority*] |**[dscp** *dscp*][**untagged**] **no media-vlan** {**voice** | **voice-signaling** | **video-signaling** | **video-conferencing** | **streaming-video** | **soft-phone** | **guest-voice-signaling** | **guest-voice**}

Syntax Descriptions

Parameter	Description
voice **voice-signalling** **video-signaling** **video-conferencing** **streaming-video** **soft-phone** **guest-voice-signaling** **guest-voice**	The type of media VLAN to define on the interface. These are defined in the LLDP-MED IEEE 802.1AB (LLDP) specification. (See also http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html)
vlan-id	The voice VLAN ID.
priority	The 802.1p priority for the Media-VLAN on the port. The range is 0–7.
dscp	The DSCP value. The range is 0–64.
untagged	Configure the voice/video device to send untagged voice traffic.

Defaults

- Media VLAN is disabled.
- The default DSCP value is 46.

Command Modes

Interface Config

Related Commands

Command	Description
media-vlan	Enables the Media-VLAN capability on the switch.

show media-vlan

Use this command to show global Media VLAN status and configuration details on an interface.

show media-vlan [**interface** {*interface* | **all**}]

Syntax Descriptions

Parameter	Description
interface	The interface ID. When the **interface** keyword is not specified, the command displays the global Media VLAN mode.
all	Displays Media VLAN information for all interfaces.

Command Modes

Privileged Exec

Examples

When the **interface** parameter is not specified, only the global mode of the Voice VLAN is displayed:

```
(switch) #show media-vlan

Administrative Mode............... Disable
```

When the **interface** parameter is specified, additional information displays:

```
(switch) #show media-vlan interface e1

Media VLAN Operational Status..... Down
CoS Override Mode................. trust

Application             Status  Untagged  VLAN Id  Priority  DSCP
-----------             ------  --------  -------  --------  ----
voice                   Disable
voice-signaling         Disable
```

```
guest-voice              Disable
guest-voice-signaling    Disable
soft-phone               Disable
video-conferencing       Disable
streaming-video          Disable
video-signaling          Disable
```

Related Commands

Command	Description
media-vlan	Enables the Media-VLAN capability on the switch.

Spanning Tree Protocol

This chapter describes how to configure the spanning tree, rapid spanning tree, and multiple spanning tree protocols.

spanning-tree

Use this command to enable the operation mode of spanning tree. To disable it, use the `no` form of this command.

spanning tree

no spanning tree

Default

Spanning tree is globally enabled.

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree port mode all	Enables the spanning tree administrative mode for all ports.
spanning-tree port mode	Enables the spanning tree administrative mode on a specific port.

spanning tree auto edge

Use this command to specify that the port is an Auto Edge Port. This allows this port to transition to the Forwarding State after the expiration of 3 times the Hold Time in all instances. This is also known as the fast convergence of leave nodes of spanning tree.

Use the `no` form of the command to remove the Auto Edge configuration from the port.

spanning-tree auto-edge

no spanning-tree auto-edge

Default

Auto Edge is enabled on all ports.

Command Modes

Interface Config

Related Commands

Command	Description
spanning-tree edgeport	Specifies that the port is an Edge Port.
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.

spanning-tree bpdufilter

Use this command to discard BPDUs received on the specified interface. Use the `no` form of the command to disable discarding BPDUs on the interface.

spanning-tree bpdufilter

no spanning-tree bpdufilter

Default

BPDU discarding is disabled.

Command Modes

Interface Config

Related Commands

Command	Description
spanning-tree bpdu flood	Allows flooding of BPDUs received on non-spanning tree ports to all other non-spanning-tree ports on an interface.
spanning-tree bpdu flooding	Allows the flooding of BPDUs received on non-spanning-tree ports to all other non-spanning-tree ports.
spanning-tree bpdufilter default	Discards BPDUs received on all the ports.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.

spanning-tree bpdufilter default

Use this command to discard BPDUs received on all ports. Use the `no` form of the command to disable discarding BPDUs on all ports.

```
spanning-tree bpdufilter default

no spanning-tree bpdufilter default
```

Default

BPDU discarding is disabled.

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree bpdufilter	Discards BPDUs received on the specified interface.

spanning-tree bpdumigrationcheck

Use this command to force the specified port or all ports to transmit RST or MST BPDUs. This can be used to test whether all legacy bridges on the LAN have been removed.

spanning-tree bpdumigrationcheck [**all** | *interface*]

Command Modes

Global Config

Related Commands

Command	Description
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.

spanning-tree bpdu flood

Use this command to allow flooding of BPDUs received on non-spanning tree ports to all other non-spanning-tree ports on the interface. Use the `no` form of the command to disable flooding.

spanning-tree bpdu flood

no spanning-tree bpdu flood

Default

BPDU flooding is enabled by default on all interfaces.

Command Modes

Interface Config

Related Commands

Command	Description
spanning-tree bpdufilter	Discards BPDUs received on the specified interface.

Command	Description
spanning-tree bpdufilter default	Discards BPDUs received on the interface.
spanning-tree bpdu flooding	Allows the flooding of BPDUs received on non-spanning-tree ports to all other non-spanning-tree ports on the interface.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.

spanning-tree bpdu flooding

Use this command to allow flooding of BPDUs received on non-spanning tree ports to all other non-spanning-tree ports. Use the `no` form of the command to disable flooding.

spanning-tree bpdu flooding

no spanning-tree bpdu flooding

Default

BPDU flooding is enabled.

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree bpdufilter	Discards BPDUs received on the specified interface.
spanning-tree bpdu flood	Allows flooding of BPDUs received on non-spanning tree ports to all other non-spanning-tree ports on an interface.
spanning-tree bpdufilter default	Discards BPDUs received on all the ports.

Command	Description
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.

spanning-tree configuration name

Use this command to set the Multiple Spanning Tree (MST) Configuration Identifier Name that identifies the configuration that the switch is currently using. Use the **no** form of the command to reset it to the default value.

spanning-tree configuration name *name*

no spanning-tree configuration name

Syntax Descriptions

Parameter	Description
name	A string of up to 32 characters.

Default

The default MST configuration name is the base MAC address for the switch.

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree configuration revision	Sets the MST Configuration Identifier Revision Level, which identifies the configuration that the switch is currently using.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.

Command	Description
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.

spanning-tree configuration revision

Use this command to set the MST Configuration Identifier Revision Level, which identifies the configuration that the switch is currently using. Use the **no** form of the command to reset it to the default value.

NOTE This configuration is applicable only when spanning tree mode is MSTP.

spanning-tree configuration revision *0-65535*

no spanning-tree configuration revision

Syntax Descriptions

Parameter	Description
0–65535	A number in the range of 0 to 65535.

Default

revision—0

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree	Enables the operation mode of spanning tree.
spanning-tree configuration name	Sets the MST Configuration Identifier Name, which identifies the configuration that the switch is currently using.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.

Command	Description
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.

spanning-tree edgeport

Use this command to specify that this port is an edge port. This allows this port to transition to the Forwarding State without delay in all instances. This is also known as fast convergence of leave nodes of spanning tree.

Use the `no` form of the command to remove the edge port configuration.

```
spanning-tree edgeport

no spanning-tree edgeport
```

Default

Edge port configuration is disabled on all ports.

Command Modes

Interface Config

Related Commands

Command	Description
Spanning Tree Auto Edge	Specifies that the port is an Auto Edge Port.
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.

spanning-tree forward-time

Use this command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port enters forwarding mode. Use the no form of this command to return to the default value.

Use the `no` form of the command to return to the default interval.

spanning-tree forward-time {*seconds*}

no spanning-tree forward-time

Syntax Descriptions

Parameter	Description
4–30	The seconds parameter in the range of 4 to 30 seconds.

Default

The forward-time is 15 seconds.

Command Modes

Interface Config

Usage Guidelines

Configure forwarding time with a value less than or equal to (spanning-tree max-age/2)+1.

Related Commands

Command	Description
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.
spanning-tree max-age	Changes the interval between messages the spanning tree receives from the root switch.
spanning-tree port mode	Enables the spanning tree administrative mode on a specific port.

spanning-tree max-age

Use this command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a Bridge Protocol Data Unit (BPDU) message from the root switch within this interval, it recomputes the Spanning Tree Protocol (STP) topology.

The max-age setting must be greater than the hello-time setting.

Use the `no` form of the command to return to the default interval.

spanning-tree max-age {*seconds*}

no spanning-tree max-age

Syntax Descriptions

Parameter	Description
4–30	The seconds parameter in the range of 6 to 40 seconds.

Default

The max-age is 20 seconds.

Command Modes

Interface Config

Related Commands

Command	Description
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.
spanning-tree forward-time	Determines how long each of the listening and learning states last before the port enters forwarding mode.
spanning-tree port mode	Enables the spanning tree administrative mode on a specific port.

spanning-tree mode

Use this command to configure the spanning tree protocol. To return to the default configuration, use the no form of this command.

spanning tree mode {**stp** | **rstp** | **mstp**}

no spanning tree mode

Syntax Descriptions

Parameter	Description
stp	Configures common Spanning Tree mode.
rstp	Configures Rapid Spanning Tree mode.
mstp	Configures Multiple Spanning Tree mode.

Default

Rapid Spanning Tree Protocol (RSTP) is enabled.

Command Modes

Global Config

Related Commands

Command	Description
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.
show spanning-tree brief	Displays spanning tree settings for the bridge.

spanning-tree mst

Use this command to set the Path Cost or Port Priority for the specified port within the multiple spanning tree instances or in the common and internal spanning tree. Use the no form of this command to reset these values to their defaults.

spanning-tree mst *mstid* {{**cost** *1-200000000* | **auto**} | {**external-cost** *1- 200000000* | **auto**} | **port-priority** *0-240*}

no spanning-tree mst *mstid*

Syntax Descriptions

Parameter	Description
mstid	A parameter that corresponds to an existing multiple spanning tree instance. The configurations are applied to that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *mstid*, the configurations are applied to the single spanning tree of STP and RSTP, or the CIST of MSTP depending on the configured spanning tree mode. If the spanning tree mode is STP or RSTP, *mstid* must be 0.
cost | auto	Sets the Port Path Cost of this port for the spanning tree or spanning tree instance depending on the spanning tree mode and *mstid* parameter. You can set the path cost as a number in the range of 1 to 200000000 or auto. If you select auto, the path cost value is set based on Link Speed.
external-cost | auto	Sets the External Port Path Cost for MST instance 0; i.e., CIST instance. You can set the external cost as a number in the range of 1 to 200000000 or auto. If you specify auto, the external path cost value is set based on Link Speed. The External Port Path Cost is applicable only when the panning tree mode is mstp.
port-priority	Sets the priority of the port for the spanning tree or spanning tree instance depending on the spanning tree mode and the *mstid* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default

- **cost**—auto
- **external-cost**—auto
- **port-priority**—28

Command Modes

Interface Config

Examples

The following command sets the path cost for mst 1.

```
(switch) (Interface e1)#spanning-tree mst 1 cost 1000
```

The following command sets the port priority for mst 1

```
(switch) (Interface e1)#spanning-tree mst 1 port-priority 240
```

The following command sets the external path cost for the common and internal spanning tree (mst instance 0).

```
(switch) (Interface e1)#spanning-tree mst 0 external-cost 1000
```

Related Commands

Command	Description
spanning-tree port mode all	Enables the spanning tree administrative mode for all the ports.
spanning-tree port mode	Enables the spanning tree administrative mode on a specific port.
spanning-tree configuration name	Sets the MST Configuration Identifier Name, which identifies the configuration that the switch is currently using.
spanning-tree mst instance	Adds a multiple spanning tree instance to the switch.
spanning-tree mst vlan	Adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree.
spanning-tree priority	Configures the spanning tree bridge priority.
spanning-tree mst	Sets the Path Cost or Port Priority for the specified port within the multiple spanning tree instances or in the common and internal spanning tree.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.

Command	Description
show spanning-tree mst port summary	Displays the settings of one or all ports within the specified multiple spanning tree instance.
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.

spanning-tree mst instance

Use this command to add a multiple spanning tree instance to the switch. Use the `no` form of this command to remove a multiple spanning tree instance from the switch and reallocate all VLANs allocated to the deleted instance to the common and internal spanning tree.

spanning-tree mst instance *mstid*

no spanning-tree mst instance

Syntax Descriptions

Parameter	Description
mstid	A number within a range of 1 to 4094, that identifies the new instance ID to be added/removed.

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree configuration name	Sets the MST Configuration Identifier Name, which identifies the configuration that the switch is currently using.
spanning-tree configuration revision	Sets the MST Configuration Identifier Revision Level, which identifies the configuration that the switch is currently using.

Command	Description
spanning-tree mode	Configures the spanning-tree protocol.
spanning-tree mst vlan	Adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree.
spanning-tree mst	Sets the Path Cost or Port Priority for the specified port within the multiple spanning tree instances or in the common and internal spanning tree.
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.

spanning-tree mst priority

Use this command to set the priority for a particular spanning tree instance. Use the `no` form of the command to remove the association. Use the `no` form of the command to reset the priority of the specified instance to the default value (32768.).

spanning-tree mst priority *mstid mstpriority*

no spanning-tree mst vlan *mstid*

Syntax Descriptions

Parameter	Description
mstid	A number that identifies an MST instance.
mstpriority	The MST priority value in the range 0–61440. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge for the MST instance.

Default

mstpriority—32768

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree priority	Configures the spanning tree bridge priority for the common and internal (CST) spanning tree instance (instance 0).
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.

spanning-tree mst vlan

Use this command to add an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. Use the `no` form of the command to remove the association.

spanning-tree mst vlan *mstid vlan-id*

no spanning-tree mst vlan *mstid vlan-id*

Syntax Descriptions

Parameter	Description
mstid	A number that corresponds to the desired existing multiple spanning tree instance.
vlan-id	The VLAN range can be specified as a list or as a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-).

Command Modes

Global Config

Usage Guidelines

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

NOTE This configuration is applicable only when spanning tree mode is MSTP.

Related Commands

Command	Description
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.

spanning-tree port mode

Use this command to enable the spanning tree administrative mode on a specific port. To disable it, use the `no` form of this command.

```
spanning tree port mode
no spanning tree port mode
```

Default

Spanning tree is enabled on all ports.

Command Modes

Interface Config

Related Commands

Command	Description
spanning-tree	Enables the operation mode of spanning tree.
spanning-tree port mode all	Enables the spanning tree administrative mode for all the ports.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.

spanning-tree port mode all

Use this command to enable the spanning tree administrative mode for all ports. To disable it, use the `no` form of this command.

spanning tree port mode all

no spanning tree port mode all

Default

Spanning tree is enabled on all ports.

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree	Enables the operation mode of spanning tree.
spanning-tree port mode	Enables the spanning tree administrative mode on a specific port.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.
show spanning-tree brief	Displays spanning tree settings for the bridge.
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.

spanning-tree priority

Use this command to configure the spanning tree bridge priority for the common and internal (CST) spanning tree instance (instance 0). The priority value determines which bridge is elected as the root bridge. To reset the priority to the default value, use the `no` form of this command.

spanning tree priority *mstid 0-61440*

no spanning tree priority

Syntax Descriptions

Parameter	Description
mstid	The ID of the multiple spanning tree instance to configure.
0–61440	The priority value to assign to the MST instance.

Default

priority—32768.

Command Modes

Global Config

Related Commands

Command	Description
spanning-tree priority	Configures the spanning tree bridge priority.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.

show spanning-tree

Use this command to display spanning tree settings for the common and internal spanning tree.

show spanning-tree

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command:

```
(Switch) #show spanning-tree

Bridge Priority................................ 32768
Bridge Identifier.............................. 80:00:00:11:88:2A:35:41
Time Since Topology Change..................... 0 day 1 hr 10 min 31 sec
Topology Change Count.......................... 0
Topology Change in progress.................... FALSE
Designated Root................................ 80:00:00:11:88:2A:35:41
Root Path Cost................................. 0
Root Port Identifier........................... 00:00
Bridge Max Age................................. 20
Bridge Max Hops................................ 20
Bridge Tx Hold Count........................... 6
Bridge Forwarding Delay........................ 15
Hello Time..................................... 2
Bridge Hold Time............................... 6
CST Regional Root.............................. 80:00:00:11:88:2A:35:41
Regional Root Path Cost........................ 0
     Associated FIDs           Associated VLANs
     ---------------           ----------------
     1                         1
     16                        16
     17                        17
     18                        18
     19                        19
     20                        20
```

Related Commands

Command	Description
spanning-tree mode	Configures the spanning tree protocol.
spanning-tree priority	Configures the spanning tree bridge priority.
show spanning-tree brief	Displays spanning tree settings for the bridge.
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.

show spanning-tree brief

Use this command to display spanning tree settings for the bridge.

show spanning-tree brief

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command:

```
(Switch) #show spanning-tree brief
Bridge Priority................................ 32768
Bridge Identifier.............................. 80:00:00:11:88:2A:35:41
Bridge Max Age................................. 20
Bridge Max Hops................................ 20
Bridge Hello Time.............................. 2
Bridge Forward Delay........................... 15
Bridge Hold Time............................... 6
```

Related Commands

Command	Description
spanning-tree priority	Configures the spanning-tree bridge priority.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.
show spanning-tree interface	Displays spanning tree settings and parameters for an interface.

show spanning-tree interface

Use this command to display the settings and parameters for a specific switch port within the common and internal spanning tree. The status of ports is per-instance; therefore status is displayed via the **show spanning-tree mst port detailed** command.

show spanning-tree interface *interface*

Syntax Descriptions

Parameter	Description
interface	The interface ID.

Command Modes

Privileged EXEC

Examples

The following shows sample output for a specific interface:

```
(switch) #show spanning-tree interface e1
```

```
Hello Time.................................... Not Configured
Port Mode..................................... Enabled
BPDU Filter Mode.............................. Disabled
BPDU Flood Mode............................... Enabled
Auto Edge..................................... TRUE
Port Up Time Since Counters Last Cleared....... 0 day 0 hr 5 min 24 sec
STP BPDUs Transmitted......................... 0
STP BPDUs Received............................ 0
RSTP BPDUs Transmitted........................ 0
RSTP BPDUs Received........................... 0
MSTP BPDUs Transmitted........................ 0
MSTP BPDUs Received........................... 0
```

Related Commands

Command	Description
spanning-tree port mode	Enables the spanning tree administrative mode on a port.
spanning-tree bpdufilter	Discards BPDUs received on the specified interface.
spanning-tree bpdufilter default	Discards BPDUs received on all ports.
spanning-tree edgeport	Specifies that the port is an Edge Port.
show spanning-tree	Displays spanning tree settings for the common and internal spanning tree.
show spanning-tree brief	Displays spanning tree settings for the bridge.

show spanning-tree mst port detailed

Use this command to display the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance.

show spanning-tree mst port detailed *mstid interface*

Syntax Descriptions

Parameter	Description
mstid	The multiple spanning tree instance ID.
interface	The interface ID.

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command:

```
(Switch) #show spanning-tree mst port detailed 10 e12

MST Instance ID................................ 10
Port Identifier................................ 80:56
Port Priority.................................. 128
Port Forwarding State.......................... Disabled
Port Role...................................... Disabled
Auto-calculate Port Path Cost.................. Enabled
Port Path Cost................................. 0
Designated Root................................ 80:0A:00:11:88:2A:35:41
Root Path Cost................................. 0
Designated Bridge.............................. 80:0A:00:11:88:2A:35:41
Designated Port Identifier..................... 00:00
Loop Inconsistent State........................ FALSE
Transitions Into Loop Inconsistent State....... 0
Transitions Out Of Loop Inconsistent State..... 0
```

Related Commands

Command	Description
spanning-tree configuration name	Sets the MST Configuration Identifier Name, which identifies the configuration that the switch is currently using.
spanning-tree mst instance	Adds an MST instance to the switch.
spanning-tree priority	Configures the spanning tree bridge priority.

Command	Description
spanning-tree mst	Sets the Path Cost or Port Priority for the specified port within the MST instances or for the common and internal spanning tree.
show spanning-tree mst port summary	Displays the settings for one or all ports within the specified MST instance.
show spanning-tree mst summary	Displays summary information about all MST instances in the switch.

show spanning-tree mst port summary

Use this command to display the settings of one or all ports within the specified MST instance.

show spanning-tree mst port summary *mstid* {*interface* | **all**}

Syntax Descriptions

Parameter	Description
mstid	The multiple spanning tree instance ID. If you specify 0 (defined as the default CIST ID), the status summary displays for one or all ports within the common and internal spanning tree.
interface	The interface ID.
all	Shows summary information for all ports.

Command Modes

Privileged EXEC

Examples

The following is example output when the **all** keyword is used.

```
(switch) #show spanning-tree mst port summary 10 all

            STP                  STP            Port
Interface   Mode   Type         State           Role       Desc
--------- -------- ------- ----------------- ---------- ----------
e1        Enabled          Disabled          Disabled
e2        Enabled          Disabled          Disabled
e3        Enabled          Disabled          Disabled
e4        Enabled          Disabled          Disabled
e5        Enabled  PC Mbr  Disabled          Disabled
e6        Enabled  PC Mbr  Disabled          Disabled
e7        Enabled  Mirror  Disabled          Disabled
e8        Enabled  Probe   Disabled          Disabled
e9        Enabled          Disabled          Disabled
e10       Enabled          Disabled          Disabled
e11       Enabled          Disabled          Disabled
e12       Enabled          Forwarding        Master
e13       Enabled          Disabled          Disabled
e14       Enabled          Disabled          Disabled
e15       Enabled          Disabled          Disabled
e16       Enabled  Mirror  Disabled          Disabled
e17       Enabled          Disabled          Disabled
e18       Enabled          Disabled          Disabled
e19       Enabled          Disabled          Disabled
e20       Enabled          Disabled          Disabled
e21       Enabled          Disabled          Disabled
e22       Enabled          Disabled          Disabled
e23       Enabled          Disabled          Disabled
e24       Enabled          Disabled          Disabled
g1        Enabled          Disabled          Disabled
g2        Enabled          Disabled          Disabled
ch1       Enabled          Disabled          Disabled
ch2       Enabled          Disabled          Disabled
ch3       Enabled          Disabled          Disabled
ch4       Enabled          Disabled          Disabled
```

Related Commands

Command	Description
spanning-tree configuration name	Sets the MST Configuration Identifier Name, which identifies the configuration that the switch is currently using.
spanning-tree mst instance	Adds a multiple spanning tree instance to the switch.

Command	Description
spanning-tree priority	Configures the spanning tree bridge priority.
spanning-tree mst	Sets the Path Cost or Port Priority for the specified port within the multiple spanning tree instances or in the common and internal spanning tree.
show spanning-tree mst port summary	Displays the settings of one or all ports within the specified multiple spanning tree instance.
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.

show spanning-tree mst summary

Use this command to display summary information for all multiple spanning tree instances in the switch.

show spanning-tree mst summary

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
(Switch) #show spanning-tree mst summary
MST Instance ID................................ 10

     Associated FIDs           Associated VLANs
     ---------------           ----------------
     10                        10
     11                        11
     12                        12
     13                        13
     14                        14
     15                        15

MST Instance ID................................ 40

     Associated FIDs           Associated VLANs
     ---------------           ----------------
     16                        16
     17                        17
     18                        18
```

```
    19                         19
    20                         20
```

Related Commands

Command	Description
spanning-tree mst	Sets the Path Cost or Port Priority for the specified port within the multiple spanning tree instances or in the common and internal spanning tree.
show spanning-tree mst port summary	Displays the settings of one or all ports within the specified multiple spanning tree instance.
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.
show spanning-tree vlan	Displays the association between a VLAN and a multiple spanning tree instance.

show spanning-tree vlan

Use this command to display the association between a VLAN and a multiple spanning tree instance.

show spanning-tree vlan *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The VLAN ID.

Command Modes

Privileged EXEC

Examples

The following example shows spanning tree information for a VLAN.

```
(Switch) #show spanning-tree vlan 20

VLAN Identifier............................... 20
Associated MST Instance....................... 40
```

Related Commands

Command	Description
show spanning-tree mst port detailed	Displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance.
show spanning-tree mst port summary	Displays the settings of one or all ports within the specified multiple spanning tree instance.
show spanning-tree mst summary	Displays summary information about all multiple spanning tree instances in the switch.

MAC Address Tables

This chapter describes the commands you use to configure static MAC addresses and view the MAC address forwarding database.

bridge address

Use this command to add a static MAC station address to the bridge table. To delete the MAC address, use the `no` form of this command. Using the no form of the command without specifying a MAC address to delete all static MAC addresses belonging to this VLAN. This MAC address is not learned on any other port and packets are not discarded.

bridge address *vlan-id mac-address*[**permanent**][**delete-on-timeout**][**secure**]

no bridge address [*mac-address*] *vlan-id*

Syntax Descriptions

Parameter	Description
mac-address	The MAC address for this entry.
vlan-id	The VLAN ID to associate with the MAC address.
permanent	The bridge table entry will not be deleted due to timing out.
delete-on-timeout	The bridge table entry will be deleted when it times out.
secure	Secure MAC addresses are used with the Port Security feature. If the associated port is locked, only packets with specified source MAC addresses are forwarded on the port.

Default

Bridge table entries are permanent.

Command Modes

Interface Config

Related Commands

Command	Description
show mac-addr-table static	Displays static entries in the bridge-forwarding database.

bridge aging-time

Use this command to configure the forwarding database address aging timeout in seconds. Use the `no` form of the command to reset it to the default value.

bridge aging-time ***10-1000000***

no bridge aging-time

Syntax Descriptions

Parameter	Description
10–100000	The seconds parameter in the range of 10 to 1,000,000 seconds.

Default

300 seconds

Command Modes

Global Config

Related Commands

Command	Description
show mac-addr-table	Displays the forwarding database entries.

clear mac-addr-table

Use this command to remove any learned entries from the forwarding database.

clear mac-addr-table

Command Modes

Privileged Exec

Related Commands

Command	Description
show mac-addr-table	Displays the forwarding database entries.

show mac-addr-table

Use this command to display the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a frame. Enter **all** or no parameters to display the entire table.

show mac-addr-table [{*mac-address vlan-id* | **all** | **count** | **interface** *interface* | **vlan** *vlan-id*}]

Syntax Descriptions

Parameter	Description
mac-address	Shows forwarding database entries for the specified MAC address.
vlan-id	Shows forwarding database entries in the specified VLAN.
all	Shows all forwarding database entries.
count	Displays summary information about the forwarding database table.
interface	Displays MAC addresses on a specific interface.

Command Modes

Privileged Exec

Examples

The following information is displayed if optional parameters are *all* or *mac-address* and *vlan-id* are specified. Only the Mac Address, Interface, and Status fields appear if a *vlan-id* is specified in the command.

Version 1.0.1.nn

```
(switch) #show mac-addr-table all

      MAC Address        Interface  IfIndex     Status
-----------------------  ---------  -------  ------------
00:01:00:00:00:01:00:00   e1        1        Learned
00:01:00:01:01:02:02:04   e1        1        Learned
00:01:00:08:A1:7E:58:A4   e1        1        Learned
00:01:00:0F:FE:03:8D:30   e1        1        Learned
00:01:00:0F:FE:03:8D:9A   e1        1        Learned
00:01:00:10:18:53:03:B5   e1        1        Learned
00:01:00:10:18:82:1A:59   e1        1        Learned
00:01:00:12:32:00:43:23   e1        1        Learned
00:01:00:12:32:00:43:25   e1        1        Learned
00:01:00:13:46:64:49:8D   e1        1        Learned
00:01:00:13:46:8D:2D:3A   e1        1        Learned
00:01:00:14:2A:2C:41:B6   e1        1        Learned
00:01:00:14:2A:2C:44:55   e1        1        Learned
00:01:00:14:2A:2C:5E:14   e1        1        Learned
00:01:00:17:9A:02:01:00   e1        1        Learned
00:01:00:1B:90:F9:6C:00   e1        1        Learned
00:01:00:1B:D5:EE:32:83   e1        1        Learned
00:01:00:1F:3A:4C:1A:87   e1        1        Learned
00:01:00:66:55:44:33:22   e1        51       Management
```

Version 1.0.2.nn

```
(switch) #show mac-addr-table all

VLAN    MAC Address      Interface  IfIndex     Status
----  -----------------  ---------  -------  -------------
1     00:11:B2:12:2D:4E      Mgmt      51       Management
1     00:1E:C9:AA:AA:E4      e16       16       Learned
```

VLAN	The VLAN where the MAC address was learned.
Mac Address	A unicast MAC address that the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example **`00:01:00:1F:3A:4C:1A:87`**. In an IVL system the MAC address is displayed as 8 bytes. The first two bytes indicate the VLAN ID in hexadecimal format. For example, **`00:01`** indicates VLAN ID 1.

Interface	The port where this address was learned.
Interface Index	The interface index of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: ▪ Static—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. ▪ Learned—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. ▪ Management—System MAC address.

If you enter the interface *interface* parameter, in addition to the MAC Address and Status fields, the following fields display:

VLAN ID	The VLAN where the MAC address was learned.
Dynamic Address Count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address	Number of MAC addresses in the forwarding database that were manually entered.
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can accommodate.

Related Commands

Command	Description
bridge address	Adds a static MAC-layer station address to the bridge table.

Command	Description
clear mac-addr-table	Removes any learned entries from the forwarding database.
show mac-addr-table static	Displays static entries in the bridge-forwarding database.
show mac-addr-table dynamic	Displays dynamic entries in the bridge-forwarding database.

show mac-addr-table dynamic

Use this command to display dynamic entries in the bridge-forwarding database.

show mac-addr-table dynamic [*vlan-id*]]*interface*]

Syntax Descriptions

Parameter	Description
vlan-id	Shows dynamic forwarding database entries in the specified VLAN. The range is 1–4094.
interface	Displays dynamic MAC addresses on a specific interface.

Command Modes

Privileged Exec

Examples

In this example, all static entries in the bridge-forwarding database are displayed.

```
(switch) #show mac-addr-table dynamic

VLAN    MAC Address      Interface     Status
---- ----------------- ---------  ------------
1    00:00:10:60:43:A2   e1          Learned
1    00:02:BC:00:00:77   e1          Learned
1    00:02:BC:11:01:79   e1          Learned
1    00:0F:FE:03:8D:57   e1          Learned
1    00:0F:FE:03:9B:F1   e1          Learned
1    00:0F:FE:08:8D:CD   e1          Learned
1    00:10:18:53:03:F4   e1          Learned
1    00:10:18:58:36:01   e1          Learned
1    00:10:18:80:04:5B   e1          Learned
1    00:10:18:80:04:5D   e1          Learned
1    00:11:88:58:60:32   e1          Learned
```

```
1     00:13:C3:49:2A:84    e1         Learned
1     00:14:2A:26:47:F8    e1         Learned
1     00:14:6C:EA:68:09    e1         Learned
1     00:19:30:36:79:2C    e1         Learned
1     00:1B:90:F9:6C:00    e1         Learned
1     00:21:9B:C6:51:B3    e1         Learned
```

Related Commands

Command	Description
show mac-addr-table	Displays entries in the MAC address table.
show mac-addr-table static	Displays static entries in the MAC address table.
bridge address	Adds a static MAC-layer station address to the bridge table.

show mac-addr-table static

Use this command to display the static entries in the bridge-forwarding database.

show mac-addr-table static [*vlan-id*] [*interface*]

Syntax Descriptions

Parameter	Description
vlan-id	Shows static forwarding database entries in the specified VLAN. The range is 1–4094.
interface	Displays static MAC addresses on a specific interface.

Command Modes

Privileged Exec

Examples

In this example, all static entries in the bridge-forwarding database are displayed.

```
switch#show bridge address-table static
Vlan    Mac Address       Port    Type
----    --------------    ----    -----
1       0001.0001.0001    e1      Static
```

Related Commands

Command	Description
show mac-addr-table	Displays entries in the MAC address table.
show mac-addr-table dynamic	Displays dynamic entries in the MAC address table.
bridge address	Adds a static MAC-layer station address to the bridge table.

7

Multicast

This chapter describes how to use the CLI to configure multicast packet handling and the IGMP and MLD snooping capabilities.

It contains the following sections:

Multicast Forwarding and MAC Filtering

Use the following commands to configure set multicast forwarding properties and configure static multicast MAC address filters.

macfilter

Use this command to add a static filter entry with MAC-layer station source address or IP group address. To delete the MAC address or IP address, use the `no` form of this command.

macfilter {*mac-address* | *ip-address*} *vlan-id*

no macfilter {*mac-address* | *ip-address*} *vlan-id*

Syntax Descriptions

Parameter	Description
mac-address	The multicast MAC address is a 6-byte hexadecimal number in b1:b2:b3:b4:b5:b6 format. MAC addresses restricted from the command are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF.

Parameter	Description
ip-address	An IPv4 address.
vlan-id	A valid VLAN.

Command Modes

Global Config

Examples

The following command creates a filter for a MAC address on VLAN 10.

```
(Switch) #macfilter 225.1.2.3 10
```

Related Commands

Command	Description
macfilter adddest all	Adds all the ports to the destination filter set for the MAC filter with the given MAC address or IP address, and VLAN ID.
macfilter adddest	Adds the port to the destination filter set for the MAC filter with the given MAC address or IP address and VLAN ID.
show mac-address-table staticfiltering	Displays the Static Multicast Filtering entries in the Multicast Forwarding Database (MFDB) table.

macfilter adddest

Use this command to add the port to the destination filter set for the MAC filter with the given MAC address or IP address and VLAN ID. Use the `no` form of the command to remove all ports from the destination filter set.

macfilter adddest {*mac-address* | *ip-address*} *vlan-id*

no macfilter adddest {*mac-address* | *ip-address*} *vlan-id*

Syntax Descriptions

Parameter	Description
mac-address	The multicast MAC address, specified as a 6-byte hexadecimal number in b1:b2:b3:b4:b5:b6 format.
ip-address	An IPv4 address.
vlan-id	A valid VLAN.

Command Modes

Interface Config

Related Commands

Command	Description
macfilter adddest all	Adds all the ports to the destination filter set for the MAC filter with the given MAC address or IP address, and VLANID.
macfilter	Adds a static filter entry with MAC-layer station source address or IP Group Address.
show mac-address-table staticfiltering	Displays the Static Multicast Filtering entries in the Multicast Forwarding Database (MFDB) table.

macfilter adddest all

Use this command to add all the ports to the destination filter set for the MAC filter with the given MAC address or IP address, and VLAN ID. Use the `no` form of the command to remove all ports from the destination filter set.

macfilter adddest all {*mac-address* | *ip-address*} *vlan-id*

no macfilter adddest all {*mac-address* | *ip-address*} *vlan-id*

Syntax Descriptions

Parameter	Description
mac-address	The multicast MAC address, specified as a 6-byte hexadecimal number in b1:b2:b3:b4:b5:b6 format.
ip-address	An IPv4 address.
vlan-id	A valid VLAN.

Command Modes

Global Config

Related Commands

Command	Description
macfilter adddest	Adds the port to the destination filter set for the MAC filter with the given MAC address or IP address and VLAN ID.
macfilter	Adds a static filter entry with MAC-layer station source address or IP Group Address.
show mac-address-table staticfiltering	Displays the Static Multicast Filtering entries in the Multicast Forwarding Database (MFDB) table.

set multicast filter-unregistered

Use this command to drop unregistered-multicast-addresses on a port in a VLAN. Use the `no` form of this command to return to the default.

set multicast filter-unregistered {[**vlan** *vlan-id*] | **all**}

no set multicast filter-unregistered {[**vlan** *vlan-id*]| **all**}

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.

Parameter	Description
all	Enables filtering unregistered multicast packets on all VLANs on the interface.

Command Modes

Global Config

Related Commands

Command	Description
set multicast forward-unregistered	Enables forwarding to unregistered multicast addresses.
set multicast forward-all	Enables forwarding of all multicast packets on a port in a VLAN.
show multicast filtering	Displays the multicast filtering mode configuration on the switch.

set multicast forward-all

Use this command to enable forwarding of all multicast packets on all ports in a VLAN, or on all ports in all VLANs. Use the `no` form of this command to return to defaults.

```
set multicast forward-all {[vlan vlan-id]| all}

no set multicast forward-all {[vlan vlan-id] | all}
```

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.
all	Enables forwarding multicast packets on all VLANs on a port.

Command Modes

Global Config

Related Commands

Command	Description
set multicast forward-unregistered	Enables forwarding to unregistered multicast addresses.
set multicast filter-unregistered	Drops unregistered-multicast-addresses on a port in a VLAN.
show multicast filtering	Displays the multicast filtering mode configuration on the switch.

set multicast forward-unregistered

Use this command to enable forwarding to unregistered multicast addresses.

set multicast forward-unregistered {[**vlan** *vlan-id*]| **all**}

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.
all	Enables forwarding unregistered multicast addresses in all VLANs on the switch.

Command Modes

Global Config

Usage Guidelines

If routers exist on the VLAN, do not change the unregistered multicast addresses state to drop on the routers ports.

Related Commands

Command	Description
set multicast forward-all	Enables forwarding of all multicast packets on a port in a VLAN.
set multicast filter-unregistered	Drops unregistered-multicast-addresses on a port in a VLAN.
show multicast filtering	Displays the multicast filtering mode configuration on the switch.

show mac-address-table multicast

Use this command to display static multicast filtering configuration.

show mac-address-table multicast {*macaddr*}

Command Modes

Privileged Exec

Examples

The following command displays information on all static multicast filters.

```
(Switch) #show mac-address-table multicast

                                                                        Fwd
      MAC Address        Source   Type     Description    Interface  Interfa
ce
-----------------------  ------  -------  --------------  ---------  -------
--
00:01:01:00:5E:01:02:03  IGMP    Dynamic  Network Assist  Fwd:       Fwd:
                                                          e24        e24
00:01:33:33:00:00:00:03  MLD     Dynamic  Network Assist  Fwd:       Fwd:
                                                          e24        e24
```

Related Commands

Command	Description
macfilter	Adds a static filter entry with MAC-layer station source address or IP Group Address.

Command	Description
macfilter adddest all	Adds all the ports to the destination filter set for the MAC filter with the given MAC address or IP address, and VLAN ID.
show mac-address–table static filtering	Displays the Static Multicast Filtering entries in the Multicast Forwarding Database (MFDB) table.

show mac-address-table staticfiltering

Use this command to display the Static Multicast Filtering entries in the Multicast Forwarding Database (MFDB) table.

show mac-address-table staticfiltering

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show mac-address-table staticfiltering

      MAC Address          Type      Description           Interfaces
-----------------------  -------  ----------------  -------------------
00:01:55:33:00:00:00:01  Static   Mgmt Config       Fwd: e2,e4
```

Related Commands

Command	Description
macfilter	Adds a static filter entry with MAC-layer station source address or IP Group Address.
macfilter adddest all	Adds all the ports to the destination filter set for the MAC filter with the given MAC address or IP address, and VLAN ID.

show multicast filtering

This command displays the multicast filtering mode configuration on the switch.

show multicast filtering[*vlan-id*]

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure. If no VLAN is specified, then data displays for all VLANs.

Command Modes

Privileged Exec

Examples

The following shows sample output for all VLANs.

```
(switch) #show multicast filtering

 VLAN ID    Filtering Mode
----------  --------------------
1           Forward-unregistered
2           Forward-unregistered
```

Related Commands

Command	Description
set multicast forward-unregistered	Enables forwarding to unregistered multicast addresses.
set multicast filter-unregistered	Drops unregistered-multicast-addresses on a port in a VLAN.
set multicast forward-all	Enables forwarding of all multicast packets on a port in a VLAN.

IGMP Snooping

Use the following commands to configure the switch to perform snooping on Internet Group Management Protocol messages.

set igmp

Use this command to enable IGMP snooping globally on the switch and on a particular VLAN. To disable it, use the **no** form of this command.

NOTE IGMP snooping must be enabled globally for it to be active on any interfaces on which it is enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

set igmp [*vlan-id*]

no set igmp [*vlan-id*]

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure IGMP snooping on. When no VLAN ID specified, IGMP snooping is enabled globally on the switch.

Default

IGMP snooping is disabled by default on all VLANs.

Command Modes

VLAN Config

Related Commands

Command	Description
show igmpsnooping	Displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

set igmp fast-leave

Use this command to enable or disable IGMP Snooping fast-leave administration mode on a selected VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface. Use the `no` form of command to disable IGMP Snooping fast-leave administration mode on the selected VLAN.

set igmp fast-leave *vlan-id*

no set igmp fast-leave *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure in fast-leave mode.

Default

IGMP fast-leave mode is disabled by default on all VLANs.

Command Modes

VLAN Config

Usage Guidelines

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Fast-leave processing is supported only with IGMP version 2 hosts.

Related Commands

Command	Description
show igmpsnooping	Displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

set igmp groupmembership-interval

Use this command to set the IGMP Group Membership Interval time on a VLAN. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a specific interface before deleting the interface from the entry. Use the `no` form of the command to reset it to the default value.

set igmp groupmembership-interval *vlan-id 2-3600*

no set igmp groupmembership-interval *vlan-id 2-3600*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure in fast-leave mode.
Group Membership Interval	The interval from 2 to 3600 seconds.

Default

group membership interval—260 seconds

Command Modes

VLAN Config

Related Commands

Command	Description
show igmpsnooping	Displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

set igmp maxresponse

Use this command to set the IGMP Maximum Response time on a particular VLAN. The Maximum Response time is the amount of time in seconds that a switch waits after sending a query on an interface before deleting a particular group on that interface. Use the `no` form of the command to reset it to the default value. This configured value used when querier is enabled.

set igmp maxresponse *vlan-id 1-25*

no set igmp maxresponse *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.
1–25	This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default

maximum response time—10 seconds

Command Modes

VLAN Config

Related Commands

Command	Description
show igmpsnooping	Displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

set igmp mcrtrexpiretime

Use this command to set the Multicast Router Present Expiration time. The time is set on a particular VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. Use the `no` form of the command to reset it to the default value. This timer is used only for dynamically identified router attached ports.

set igmp mcrtrexpiretime *vlan-id 0-3600*

no set igmp mcrtrexpiretime *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.
0–3600	The expiration time. The range is 0–3600 seconds. A value of 0 indicates an infinite time-out (no expiration).

Default

expiration time—0 (no expiration)

Command Modes

VLAN Config

Related Commands

Command	Description
show igmpsnooping	Displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

set igmp mrouter

Use this command to configure the VLAN ID (*vlan-id*) that has the multicast router mode enabled. Use the `no` form of the command to disable it.

set igmp mrouter *vlan-id*

no set igmp mrouter *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.

Default

IGMP mrouter is disabled on all VLANs.

Command Modes

Interface Config

Related Commands

Command	Description
show igmpsnooping mrouter vlan	Displays information about static and dynamic multicast router information on the port.
show igmpsnooping mrouter interface	Displays information about statically configured mrouter ports.

set igmp mrouter interface

Use this command to configure the interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs. Use the **no** form of the command to disable it.

set igmp mrouter interface

no set igmp mrouter interface

Default

IGMP mrouter is disabled on all interfaces.

Command Modes

Interface Config

Related Commands

Command	Description
show igmpsnooping mrouter vlan	Displays information about static and dynamic multicast router information on the port.
show igmpsnooping mrouter interface	Displays information about statically configured mrouter ports.
show igmpsnooping	Displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

show igmpsnooping

Use this command to display IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

show igmpsnooping *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.

Command Modes

Privileged Exec

Examples

When the optional argument *vlan-id* is not used, the command displays the following information.

```
(switch) #show igmpsnooping

Admin Mode.................................... Disable
Multicast Control Frame Count................. 0
VLANs enabled for IGMP snooping............... None
```

Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify a value for *vlan-id*, the following information appears.

```
(switch) #show igmpsnooping 2

VLAN ID....................................... 2
IGMP Snooping Admin Mode...................... Disabled
Fast Leave Mode............................... Disabled
Group Membership Interval (secs).............. 260
Max Response Time (secs)...................... 10
Multicast Router Expiry Time (secs)........... 0
```

VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a specific interface, which is participating in the VLAN, before deleting the interface from the entry. This value might be configured.
Maximum Response Time	The amount of time in seconds the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value might be configured.
Multicast Router Expiry Time	The amount of time in seconds to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value might be configured.

Related Commands

Command	Description
set igmp	Enables IGMP snooping on a particular VLAN.
set igmp fast-leave	Enables or disable IGMP Snooping fast-leave admin mode on a selected VLAN.
set igmp groupmembership-interval	Sets the IGMP Group Membership Interval time on a VLAN.
set igmp maxresponse	Sets the IGMP Maximum Response time on a particular VLAN.
set igmp mcrtrexpiretime	Sets the Multicast Router Present Expiration time.

show igmpsnooping mrouter interface

Displays information about statically configured mrouter ports.

show igmpsnooping mrouter interface *interface*

Syntax Descriptions

Parameter	Description
interface	The port on which to display multicast router information.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show igmpsnooping mrouter interface e15

Slot/Port...................................... e15
Multicast Router Attached...................... Disable
```

Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.

Related Commands

Command	Description
set igmp mrouter interface	Configures the interface as a multicast router interface.

show igmpsnooping mrouter vlan

This command displays information about static and dynamic multicast router information on the mrouter port.

show igmpsnooping mrouter vlan *interface*

Syntax Descriptions

Parameter	Description
interface	The port on which to display IGMP snooping multicast router information.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show igmpsnooping mrouter vlan e15

Slot/Port.................................... e15

VLAN ID
2
4
```

Interface	The port on which multicast router information is being displayed.
VLAN ID	list of VLANs that this interface has statically being configured or seen an mrouter.

Related Commands

Command	Description
set igmp mrouter	Configures the VLAN ID (*vlan-id*) that has the multicast router mode enabled.

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

show mac-address-table igmpsnooping

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show mac-address-table igmpsnooping

      MAC Address          Type      Interfaces
-----------------------  -------  --------------
00:01:01:00:5E:01:02:03  Dynamic  Fwd: e24
```

The following fields display for the configured IGMP Snooping table entries:

MAC Address	A multicast MAC address for which the switch has forwarding or Filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 00:01:01:00:5e:01:02:03. In an IVL system the MAC address is displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Related Commands

Command	Description
set igmp	Enables IGMP snooping on a particular VLAN.

MLD Snooping

Use the following commands to configure the switch to perform snooping on Multicast Listener Discovery Protocol messages.

set mld

This command enables MLD Snooping globally on all VLANs or on a particular VLAN. When enabled on a VLAN, MLD Snooping is enabled on all interfaces participating in the VLAN. Use the `no` form of the command to disable it globally or on a particular VLAN.

MLD Snooping supports the following:

- Validation of address version, payload length consistencies and discarding of the frame upon error.
- Maintenance of the forwarding table entries based on the MAC address versus the IPv6 address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

set mld [*vlan-id*]

no set mld [*vlan-id*]

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.

Default

MLD is disabled on all VLANs.

Command Modes

VLAN Config

Related Commands

Command	Description
show mldsnooping	Displays MLD Snooping information.

set mld fast-leave

Use this command to enable MLD Snooping fast-leave administration mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving and MLD done message for that multicast group without first sending out MAC-based general queries to the interface Use the `no` form of command to disable MLD Snooping fast-leave administration mode on the selected VLAN.

set mld fast-leave *vlan-id*

no set mld fast-leave *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.

Default

Fast-leave mode is disabled on all VLANs.

Command Modes

VLAN Config

Related Commands

Command	Description
show mldsnooping	Displays MLD Snooping information.

set mld groupmembership-interval

Use this command to set the MLD Group Membership Interval time on a VLAN. The Group Membership Interval is the amount of time in seconds that a switch waits for a report from a particular group on a specific interface before deleting the interface from the entry. Use the `no` form of the command to reset it to the default value.

set mld groupmembership-interval *vlan-id 2-3600*

no set mld groupmembership-interval *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.
2–3600	The interval. The range is 2–3600 seconds.

Default

group membership interval—260 seconds

Command Modes

VLAN Config

Related Commands

Command	Description
show mldsnooping	Displays MLD Snooping information.

set mld maxresponse

Use this command to set the IGMP Maximum Response time on a particular VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface. Use the `no` form of the command to reset it to the default value.

set mld maxresponse *vlan-id 1-65*

no set mld maxresponse *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.
2–65	The maximum response time. The range is 2–65 seconds. This value must be less than the MLD Query Interval time value.

Default

maximum response time—10 seconds

Command Modes

VLAN Config

Related Commands

Command	Description
show mldsnooping	Displays MLD Snooping information.

set mld mcrtrexpiretime

Use this command to set the Multicast Router Present Expiration time. The time is set on a particular VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. Use the `no` form of the command to reset it to the default value.

set mld mcrtrexpiretime *vlan-id 0-3600*

no set mld mcrtrexpiretime *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.

Parameter	Description
0–3600	The multicast router present expiration time. The range is 0–3600 seconds. A value of 0 indicates an infinite time-out; i.e. no expiration.

Default

expiration time—0 (no time-out)

Command Modes

VLAN Config

Related Commands

Command	Description
show mldsnooping	Displays MLD Snooping information.

set mld mrouter

Use this command to configure the VLAN ID (*vlan-id*) that has the multicast router mode enabled. Use the `no` form of the command to disable it.

set mld mrouter *vlan-id*

no set mld mrouter *vlan-id*

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to configure.

Default

MLD mrouter is disabled by default on all VLANs.

Command Modes

Interface Config

Related Commands

Command	Description
show mldsnooping mrouter interface	Displays information about statically configured mrouter ports.
show mldsnooping mrouter vlan	Displays information about static and dynamic multicast router information on the port.

set mld mrouter interface

Use this command to configure the interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs. Use the `no` form of the command to disable it.

set mld mrouter interface

no set mld mrouter interface

Default

MLD mrouter is disabled on all interfaces.

Command Modes

Interface Config

Related Commands

Command	Description
show mldsnooping mrouter interface	Displays information about statically configured mrouter ports.
show mldsnooping mrouter vlan	Displays information about static and dynamic multicast router information on the port.

show mac-address-table mldsnooping

This command displays the MLD Snooping entries in the MFDB table.

show mac-address-table mldsnooping

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show mac-address-table mldsnooping

      MAC Address          Type      Interfaces
-----------------------  -------  ----------------
00:01:33:33:00:00:00:03  Dynamic    Fwd: e24
```

The following fields display:

MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 00:05:33:33:45:67:89:AB. In an IVL system, the MAC address is displayed as a MAC address and a VLAN ID combination of 8 bytes.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Related Commands

Command	Description
set mld	Enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.

show mldsnooping

Use this command to display MLD Snooping information for all VLANs or for a specified VLAN. Configured information is displayed whether or not MLD Snooping is enabled.

show mldsnooping {*vlan-id*}

Syntax Descriptions

Parameter	Description
vlan-id	The ID of the VLAN to display information on. If no VLAN ID is specified, information for all VLANs displays.

Command Modes

Privileged Exec

Examples

When the optional argument *vlan-id* is not used, the command displays the following information.

```
(switch) #show mldsnooping

Admin Mode..................................... Disable
Multicast Control Frame Count.................. 0
VLANs enabled for MLD snooping................. None
```

Admin Mode	Indicates whether or not MLD Snooping is active on the switch.
MLD Control Frame Count	The number of MLD control frames that are processed by the CPU.
VLANS Enabled for MLD Snooping	The list of VLANS on which MLD Snooping is enabled.

When you specify a value for *vlan-id*, the following information appears.

```
(switch) #show mldsnooping 2

VLAN ID........................................ 2
MLD Snooping Admin Mode........................ Disabled
```

```
Fast Leave Mode.............................. Disabled
Group Membership Interval (secs)............... 260
Max Response Time (secs)....................... 10
Multicast Router Expiry Time (secs)............ 0
```

VLAN ID	The VLAN ID.
MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether MLD Snooping Fast-leave is active on the VLAN.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a specific interface, which is participating in the VLAN, before deleting the interface from the entry. This value might be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value might be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value might be configured.

Related Commands

Command	Description
set mld	Enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.
set mld fast-leave	Enables MLD Snooping fast-leave admin mode on a selected interface or VLAN.
set mld groupmembership-interval	Sets the MLD Group Membership Interval time on a VLAN.
set mld maxresponse	Sets the IGMP Maximum Response time on a particular VLAN.

Command	Description
set mld mcrtrexpiretime	Sets the Multicast Router Present Expiration time.

show mldsnooping mrouter interface

This command displays information about static and dynamic multicast routers on the port.

show mldsnooping mrouter interface *interface*

Syntax Descriptions

Parameter	Description
interface	The port on which to display MLD snooping multicast router information.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show mldsnooping mrouter interface e15

Slot/Port..................................... e15
Multicast Router Attached..................... Enable
```

Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.

Related Commands

Command	Description
set mld mrouter	Configures the VLAN ID (*vlan-id*) that has the multicast router mode enabled.
set mld mrouter interface	Configures the interface as a multicast router interface.

show mldsnooping mrouter vlan

This command displays information about static and dynamic multicast routers on the port.

show mldsnooping mrouter vlan *interface*

Syntax Descriptions

Parameter	Description
interface	The port on which to display MLD snooping multicast router information.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show mldsnooping mrouter vlan e15

Slot/Port..................................... e15

VLAN ID
2                                             Untagged
```

Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

Related Commands

Command	Description
set mld mrouter	Configures the VLAN ID (*vlan-id*) that has the multicast router mode enabled.

8

Security

This chapter describes how to use the CLI to configure security features. It includes the following topics:

- **General**
- **RADIUS**
- **Dot1x**
- **MAC Based Port Security**

General

show net connections

Use this command to display the active and open TCP/UDP services.

show net connections

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show net connections

Protocol type  Port   State      Remote IP address                 Service n
ame
------------- ----- ----------- ---------------------------------- ---------
-
TCP           2222  Listen
UDP           0     Active
UDP           1032  Active
UDP           4567  Active
UDP           1033  Active
UDP           5353  Active
UDP          5353  Active                                         
TCP          80    Listen                                         HTTP
UDP          0     Active                                         
TCP          23    Listen                                         Telnet
TCP          23    Established 10.12.17.82:2692                   Telnet
UDP          546   Active                                         
TCP          0     Disabled                                       SSH
```

RADIUS

This section describes how to configure RADIUS client functionality and RADIUS servers on the switch. RADIUS functionality is primarily used for switch management access authentication and IEEE 802.1X ("dot1X") port access control.

radius server attribute nas-ip-addr

Use this command to configure the RADIUS client to include the NAS-IP Address attribute in the RADIUS requests. If a specific IP address is entered, then the RADIUS client uses that IP address in the NAS-IP-Address attribute in RADIUS communication. If the IP address is not specified, the RADIUS client does not send any value for this attribute.

Use the `no` form of the command to disable this attribute. The no form functions the same whether or not an IP address is specified in the command.

radius server attribute nas-ip-addr[*ip-address*]

no radius server attribute nas-ip-addr[*ip-address*]

Syntax Descriptions

Parameter	Description
ip-address	The IP address to use in the NAS-IP-Address attribute in RADIUS communication. If the command is entered with no specific IP address, the RADIUS client does not send include any value for the NAS-IP-Address attribute.

Command Modes

Global Config

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.
show radius servers	Displays summary data and details on RADIUS servers.

radius server deadtime

Use this command to improve RADIUS response times when servers are unavailable. The switch will continue to send transaction requests to servers for the specified time after they have been found to be unavailable. To set the deadtime to 0, use the `no` form of this command.

radius server deadtime *minutes*

no radius server deadtime

Syntax Descriptions

Parameter	Description
minutes	The time in minutes a RADIUS server will be bypassed after the switch determines it is unavailable. The range is 0–2000 minutes.

Default

minutes—0 minutes

Command Modes

Global Config

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.

Command	Description
show radius servers	Displays summary data and details on RADIUS servers.

radius server host

Use this command to configure the IP address or DNS name of a RADIUS server. You can also configure the logical UDP port number for RADIUS communication with the server.

If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the no form of the command.

Use the `no` form of command to remove the RADIUS server. The *ip-addr|dnsname* parameter must match the IP address or DNS name of the previously configured server.

radius server host {{*ip-address* | *dnsname*} [**port** *1025-65535*]}

no radius server host {*ip-address* | *dnsname*}

Syntax Descriptions

Parameter	Description
ip-address	The IP address of the RADIUS server.
dnsname	The hostname of the RADIUS server. To specify a hostname, ensure that the DNS client capability is configured on the switch.
1025–65535	If you use the optional **port** parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The range is 1025–65535. The default value is 1812.

Command Modes

Global Config

Related Commands

Command	Description
radius server key	Configures the key to be used in RADIUS client communication with the specified server.
radius server priority	Specifies the order in which the servers are to be used.
radius server deadtime	Improve RADIUS response times when servers are unavailable.
radius server attribute nas-ip-addr	Specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests.
radius server msgauth	Enables the Message Authenticator attribute to be used for the specified RADIUS server.
radius server retransmit	Globally configures the number of unsuccessful transmissions of RADIUS messages that the client must make before it attempts to use the fall back server.
radius server timeout	Globally configures the timeout value (in seconds) after which the RADIUS client must retransmit to the RADIUS server if no response is received.
show radius	Displays the configured global parameters of the RADIUS client.
show radius servers	Displays summary data and details on RADIUS servers.
show radius statistics	Displays the summary statistics of configured RADIUS servers.

radius server key

Use this command to configure the key to be used in RADIUS client communication with the specified server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

You can enter the RADIUS password in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. To enter the key in encrypted format, use the **encrypted** keyword.

radius server key {*ip-address* | *dnsname*} [**encrypted** *password*]

Syntax Descriptions

Parameter	Description
ip-address	The IP address of the RADIUS server.
dnsname	The hostname of the RADIUS server. To specify a hostname, ensure that the DNS client capability is configured on the switch.
encrypted	Enables entering an already-encrypted key in hexadecimal format.
password	The key for communicating with this server. In non-encrypted format, the key must be an alphanumeric value not exceeding 16 characters. In ecrypted format, the key must be a 128-character hexadecimal value.

Command Modes

Global Config

Examples

The following example configures a key without encryption.

```
(switch) (Config)#radius server key 10.172.69.32

Enter secret (16 characters max):******

Re-enter secret:******
```

The following example configures a key with encryption.

```
radius server key 10.172.69.32 encrypted
a205e003300ec4710c25f7010baf13cbee97d00c1e8eacebec00d84cca14c4c97671f2539e0f
910647969f3741db47975fb1d9ccca04e73c6f3d7ec65c0d994d
```

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.
show radius servers	Displays summary data and details on RADIUS servers.

radius server msgauth

Use this command to enable the message authenticator attribute to be used for the specified RADIUS server. Use the `no` form of this command to disable the attribute.

radius server msgauth {*ip-address* | *hostname*}

no radius server msgauth {*ip-address* | *hostname*}

Syntax Descriptions

Parameter	Description
ip-address	The IP address of the RADIUS server.
hostname	The hostname of the RADIUS server. To specify a hostname, ensure that the DNS client capability is configured on the switch.

Default

The use of the message authenticator attribute is enabled by default on all RADIUS servers.

Command Modes

Global Config

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.
show radius servers	Displays summary data and details on RADIUS servers.

radius server priority

Use this command to specify the order in which the servers are to be used, with 1 being the highest priority.

radius server priority {*ip-address* | *dnsname*} *priority*

Syntax Descriptions

Parameter	Description
ip-address	The IP address of the RADIUS server.
dnsname	The hostname of the RADIUS server. To specify a hostname, ensure that the DNS client capability is configured on the switch.
priority	The priority of the server. The range is 0 (highest) to 66535 (lowest).

Default

priority—8

Command Modes

Global Config

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.
show radius servers	Displays summary data and details on RADIUS servers.

radius server retransmit

Use this command to globally configure the number of unsuccessful transmissions of RADIUS messages that the client must make before it attempts to use the fall back server.

Use the `no` form of this command to set the value of this global parameter to the default value.

radius server retransmit *retries*

no radius server retransmit

Syntax Descriptions

Parameter	Description
retries	The number of messages transmissions before attempting to use the fall-back server. The range is 1–10.

Default

retries—3

Command Modes

Global Config

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.
show radius servers	Displays summary data and details on RADIUS servers.

radius server timeout

Use this command to globally configure the timeout value (in seconds) after which the RADIUS client must retransmit to the RADIUS server if no response is received. Use the `no` form of the command to reset the timeout to the default.

radius server timeout *seconds*

no radius server timeout

Syntax Descriptions

Parameter	Description
seconds	The timeout value after which a request must be retransmitted to the RADIUS server if no response is received. The range is 1–30 seconds.

Default

seconds—3

Command Modes

Global Config

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.

Command	Description
show radius servers	Displays summary data and details on RADIUS servers.

show radius

Use this command to display the values configured for the global parameters of the RADIUS client.

show radius

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show radius

Number of Configured Authentication Servers.... 1
Number of Retransmits.......................... 3
Timeout Duration............................... 3
Dead Time...................................... 0
RADIUS Attribute 4 Mode........................ Disable
RADIUS Attribute 4 Value....................... 0.0.0.0
```

Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request re-transmissions.
Dead Time	The length of time an unavailable RADIUS server is skipped.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.

RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

Related Commands

Command	Description
radius server deadtime	Improves RADIUS response times when servers are unavailable.
radius server attribute nas-ip-addr	Specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests.
radius server retransmit	Globally configures the number of unsuccessful transmissions of RADIUS messages that the client must make before it attempts to use the fall back server.
radius server timeout	Globally configures the timeout value (in seconds) after which the RADIUS client must retransmit to the RADIUS server if no response is received.
show radius statistics	Displays the summary statistics of configured RADIUS Authenticating servers.

show radius servers

Use this command to display summary data and details on RADIUS servers. Information on all the RADIUS servers is displayed by default.

show radius servers [{*ip-address* | *dnsname*}]

Syntax Descriptions

Parameter	Description
ip-address	The IP address of the RADIUS server.
dnsname	The hostname of the RADIUS server. To specify a hostname, ensure that the DNS client capability is configured on the switch.

Command Modes

Privileged Exec

Examples

The following shows sample output for when no server is specified.

```
(switch) #show RADIUS servers

Cur
rent Host Address                 Port  Priority
---- ------------------------ ----- ---------
  *  10.23.31.1               1812  8
     RADIUS-Server1           1812  8
```

The following shows sample output for the command when a server is specified.

```
(switch) #show radius servers RADIUS-Server1

RADIUS Server DNS Address...................... RADIUS-Server1
RADIUS Server IP Address....................... 10.24.1.2
RADIUS Server Name............................. Default-RADIUS-Server
Host Address................................... 10.131.11.166
Port........................................... 1812
Secret Configured.............................. No
Number of Retransmits.......................... 3
Message Authenticator.......................... Enable
Timeout Duration............................... 3
RADIUS Attribute 4 Mode........................ Disable
RADIUS Attribute 4 Value....................... 0.0.0.0
```

RADIUS Server DNS Address	The DNS name of the authenticating server.
RADIUS Server IP Address	The IP address of the authenticating server.
RADIUS Server Name	Displays the RADIUS server name, or “Default-RADIUS-Server” if no name is provided.
Port	The port used for communication with the authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.

Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.
radius server key	Configures the key to be used in RADIUS client communication with the specified server.
radius server priority	Specifies the order in which the servers are to be used.
radius server attribute nas-ip-addr	Specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests.
radius server msgauth	Enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.
radius server retransmit	Globally configures the number of unsuccessful transmissions of RADIUS messages that the client must make before it attempts to use the fall back server.
radius server timeout	Globally configures the timeout value (in seconds) after which the RADIUS client must retransmit to the RADIUS server if no response is received.

show radius statistics

Use this command to display the summary statistics for configured RADIUS Authenticating servers.

show radius statistics {*ip-address* | *dnsname*}

Syntax Descriptions

Parameter	Description
ip-address	The IP address of the RADIUS server.
dnsname	The hostname of the RADIUS server. To specify a hostname, ensure that the DNS client capability is configured on the switch.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show radius statistics 10.172.69.32

RADIUS Server Name............................ Default-RADIUS-Server
Server Host Address........................... 10.172.69.32
Access Requests............................... 0
Access Retransmissions........................ 0
Access Accepts................................ 0
Access Rejects................................ 0
Access Challenges............................. 0
Malformed Access Responses.................... 0
Bad Authenticators............................ 0
Pending Requests.............................. 0
Timeouts...................................... 0
Unknown Types................................. 0
Packets Dropped............................... 0
```

RADIUS Server Name	The DNS name of the server.
Server Host Address	The IP address of the server.

Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Related Commands

Command	Description
radius server host	Configures the IP address or DNS name of a RADIUS server.
show radius	Displays the values configured for the global parameters of the RADIUS client.
show radius servers	Displays summary data and details on RADIUS servers.

Dot1x

Port-based access control provides a method for networks to control whether hosts can access services provided by a connected port. You can configure the switch to use port-based network access control based on the IEEE 802.1X ("dot1X") protocol.

A port can be configured either as an 802.1X authenticator or a supplicant:

- A supplicant is a port that requests access to the network. The supplicant provides credentials to the network that the another node on the network—the authenticator—uses to request authentication from a server.
- An authenticator is a port that must be authenticated before it permits other nodes on the network to use the services it provides access to. The authenticator relays supplicant requests and credentials to an authentication server, and authorizes or denies access to the supplicant.

In the authentication process, 802.1X supports Extensible Authentication Protocol (EAP) over LANs (EAPOL) message exchanges between supplicants and authenticators.

This section describes the commands you use to configure 802.1X operation on the switch.

authentication dot1x

This command assigns the authentication method to use for 802.1X port security. Use the `no` form of the command to disable 802.1X port security.

authentication dot1x *method1* [*method2*]

no authentication dot1x

Syntax Descriptions

Parameter	Description
method1	The first method to use to authenticate. Possible value are: - radius—Uses the list of all authentication servers for authentication - local—Uses locally configured users as the authentication list. - none—No authentication is used.
method2	The backup method to use if authentication using *method1* fails. The same choices are available for method2 as for method1; however, method 1 cannot be repeated.

Command Modes

Global Config

Usage Guidelines

No authentication is enabled by default.

clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

clear dot1x statistics {*interface* | **all**}

Syntax Descriptions

Parameter	Description
interface	The interface for which to clear statistics.
all	Clears statistics for all interfaces.

Command Modes

Privileged Exec

Related Commands

Command	Description
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port, and the 802.1X statistics for a specified port.

dot1x pae

Use this command to enable the authenticator or supplicant mode on the interface. Use the no form of the command to reset it to the default role (authenticator).

NOTE An interface can be an authenticator or a supplicant, but not both.

dot1x pae {**authenticator** | **supplicant**}

no dot1x pae

Syntax Descriptions

Parameter	Description
authenticator	The port must be authenticated before it permits other nodes on the network to use the services it provides access to. The authenticator relays supplicant requests and credentials to an authentication server, and authorizes or denies access to the supplicant.

Parameter	Description
supplicant	The port is configured to requests access to the network. The supplicant provides credentials to the network that the another node on the network—the authenticator—uses to request authentication from a server.

Default

All interfaces are configured as authenticators.

Command Modes

Interface Config

Related Commands

Command	Description
dot1x supplicant port-control	Configures the authentication mode for supplicant on the interface.
dot1x supplicant user	Configures the supplicant user.

dot1x port-control

Use this command to enable the IEEE 802.1X operation on the port. Use the **no** form of the command to reset it to the default operating mode (auto).

NOTE Dot1x is not applicable to LAG ports.

```
dot1x port-control {force-unauthorized | force-authorized | auto}

no dot1x port-control
```

Syntax Descriptions

Parameter	Description
force-unauthorized	The authenticator PAE unconditionally sets the controlled port to unauthorized.

Parameter	Description
force-authorized	The authenticator PAE unconditionally sets the controlled port to authorized.
auto	The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Default

802.1X Port Control is enabled in **auto** mode.

Command Modes

Interface Config

Related Commands

Command	Description
dot1x port-control	Enables the IEEE 802.1X operation on all the port.
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port, and the 802.1X statistics for a specified port.

dot1x port-control all

Use this command to enable the IEEE 802.1X operation on all the ports. Use the `no` form of the command to reset the mode to the default value (**auto**).

dot1x port-control all {**force-unauthorized** | **force-authorized** | **auto**}

no dot1x port-control all

Syntax Descriptions

Parameter	Description
force-unauthorized	The authenticator PAE unconditionally sets the controlled port to unauthorized.
force-authorized	The authenticator PAE unconditionally sets the controlled port to authorized.
auto	The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and authentication server.

Default

802.1X Port Control is enabled in **auto** mode.

Command Modes

Global Config

Related Commands

Command	Description
dot1x port-control	Enables the IEEE 802.1X operation on the port.
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port, and the 802.1X statistics for a specified port.

dot1x re-authentication

Use this command to enable periodic re-authentication of the client or to force an immediate reauthentication of the client. To return to the default setting, use the `no` form of this command.

dot1x re-authentication [**force**]

no dot1x re-authentication

Syntax Descriptions

Parameter	Description
force	Initiates reauthentication instantly. If this keyword is not specified, then reauthentication occurs when the timeout period expires, as specified by the **dot1x timeout reath-period** command.

Default

Periodic authentication is enabled.

Command Modes

Interface Config

Related Commands

Command	Description
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port, and the 802.1X statistics for a specified port.

dot1x supplicant portcontrol

Use this command to configure the authentication mode for supplicant on the interface. Use the `no` form of the command to reset it to the default mode (auto).

dot1x supplicant portcontrol {**force-unauthorized** | **force-authorized** | **auto**}

no dot1x supplicant portcontrol

Syntax Descriptions

Parameter	Description
force-unauthorized	The authenticator PAE unconditionally sets the controlled port to unauthorized.
force-authorized	The authenticator PAE unconditionally sets the controlled port to authorized.
auto	The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

Default

Supplicants are enabled in **auto** mode.

Command Modes

Interface Config

Related Commands

Command	Description
dot1x supplicant user	Configures the supplicant user.
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port, and the 802.1X statistics for a specified port.

dot1x supplicant user

Use this command to configure an existing user as a supplicant user. Use the `no` form of the command to delete the supplicant user.

dot1x supplicant user *user*

no dot1x supplicant user *user*

Syntax Descriptions

Parameter	Description
user	Assigns a user name to the supplicant.

Command Modes

Interface Config

Related Commands

Command	Description
show dot1x users	Displays 802.1x port security user information for locally configured users.

dot1x system-auth-control

Use this command to enable 802.1X services globally. To disable 802.1X services globally, use the `no` form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Default

802.1X services are globally disabled.

Command Modes

Global Config

Related Commands

Command	Description
dot1x port-control	Enables the IEEE 802.1X operation on the port.

Command	Description
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port, and the 802.1X statistics for a specified port.

dot1x timeout quiet-period

Use this command to set the number of seconds that the switch remains in the quiet state following a failed authentication exchange (when for example, the client provides an invalid password). To return to the default setting, use the `no` form of this command.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Syntax Descriptions

Parameter	Description
seconds	The time that the switch remains in the quiet state following a failed authentication exchange. The range is 0–65535 seconds.

Default

seconds—60

Command Modes

Interface Config

Usage Guidelines

During the quiet period, the switch does not accept or initiate any authentication requests. Change the default value of this command only 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, enter a smaller number than the default.

Related Commands

Command	Description
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port and the 802.1X statistics for a specified port.

dot1x timeout reauth-period

Use this command to set the number of seconds between re-authentication attempts. To return to the default setting, use the `no` form of this command.

dot1x timeout reauth-period *seconds*

no dot1x timeout reauth-period

Syntax Descriptions

Parameter	Description
seconds	The time between re-authentication attempts. The range is 300–65535 seconds.

Default

seconds—3600

Command Modes

Interface Config

Related Commands

Command	Description
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port, and the 802.1X statistics for a specified port.

dot1x timeout server-timeout

Use this command to set the time that the switch waits for a response from the authentication server. To return to the default setting, use the **no** form of this command. The actual timeout is the smaller of this parameter or the product of the RADIUS transmission and the RADIUS timeout.

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Syntax Descriptions

Parameter	Description
seconds	The time that the switch waits for a response from the authentication server. The range is 1–65535 seconds.

Default

seconds—30

Command Modes

Interface Config

Related Commands

Command	Description
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port and the 802.1X statistics for a specified port.

dot1x timeout supp-timeout

Use this command to set the time that the switch waits for a response before retransmitting an Extensible Authentication Protocol (EAP)-request frame to the client. To return to the default setting, use the `no` form of this command.

Change the default value of this command only 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, enter a smaller number than the default.

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Syntax Descriptions

Parameter	Description
seconds	The time that the switch waits for a response before retransmitting an Extensible Authentication Protocol (EAP)-request frame to the client. The range is 1–65535 seconds.

Default

seconds—30

Command Modes

Interface Config

Related Commands

Command	Description
show dot1x users	Displays 802.1x port security user information for locally configured users.

dot1x timeout tx-period

Use this command to set the number of seconds that the switch 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 setting, use the **no** form of this command.

Change the default value of this command only 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, enter a smaller number than the default.

dot1x timeout tx-period ***seconds***

no dot1x timeout tx-period

Syntax Descriptions

Parameter	Description
seconds	The time that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request. The range is 1–65535 seconds.

Default

seconds—30

Command Modes

Interface Config

Related Commands

Command	Description
show dot1x	Shows a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port and the 802.1X statistics for a specified port.

dot1x user

Use this command to add the specified user to the list of users with access to the specified port or all ports. Use the `no` form of the command to remove the user.

dot1x user *user* {*interface* | **all**}

no dot1x user *user* {*interface* | **all**}

Syntax Descriptions

Parameter	Description
user	The user name to configure. This must be a configured user.
interface	The interface to provide the user access to.
all	Adds the user to the access list for all interfaces.

Command Modes

Global Config

Related Commands

Command	Description
show dot1x users	Displays 802.1x port security user information for locally configured users.

show dot1x

Use this command to show a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port, and the 802.1X statistics for a specified port.

show dot1x [{**summary** {*interface* | **all**} | **detail** *interface* | **statistics** *interface*]

Syntax Descriptions

Parameter	Description
summary	Displays 802.1X configuration for the specified port or all ports.
interface	The port number.
all	Displays information on all ports.
detail	Displays detailed 802.1X configuration for the specified port or for all port.
statistics	Displays frame counts and other statistics for the port or for all ports.

Command Modes

Privileged Exec

Examples

If you do not enter any parameters, the global 802.1X status displays.

```
(switch) #show dot1x

Administrative Mode.............. Disabled
```

If you use the optional parameter **summary** *{interface | all}*, the 802.1X configuration for the specified port or all ports are displayed.

```
(switch) #show dot1x summary all

                                 Operating      Reauthentication
Interface    Control Mode       Control Mode       Enabled      Port Statu
s
--------- ------------------ ------------------ ---------------- -----------
--
e1        auto               auto               TRUE             Authorized
```

```
e2        auto               auto               TRUE              Authorized
e3        auto               auto               TRUE              Authorized
e4        auto               auto               TRUE              Authorized
e5        auto               auto               TRUE              Authorized
e6        auto               auto               TRUE              Authorized
e7        auto               auto               TRUE              Authorized
e8        auto               auto               TRUE              Authorized
e9        auto               auto               TRUE              Authorized
e10       auto               auto               TRUE              Authorized
e11       auto               auto               TRUE              Authorized
e12       auto               auto               TRUE              Authorized
e13       auto               auto               TRUE              Authorized
e14       auto               auto               TRUE              Authorized
e15       auto               auto               TRUE              Authorized
e16       auto               auto               TRUE              Authorized
e17       auto               auto               TRUE              Authorized
e18       auto               auto               TRUE              Authorized
e19       auto               auto               TRUE              Authorized
e20       auto               auto               TRUE              Authorized
e21       auto               auto               TRUE              Authorized
e22       auto               auto               TRUE              Authorized
e23       auto               auto               TRUE              Authorized
e24       auto               auto               TRUE              Authorized
g1        auto               auto               TRUE              Authorized
g2        auto               auto               TRUE              Authorized
```

Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are auto, force authorized, and force unauthorized.
Reauthenticatio n Enabled	Indicates whether re-authentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

If you use the optional parameter **detail** *interface*, the detailed 802.1X configuration for the specified port is displayed.

```
(switch) #show dot1x detail e15

Port........................................... e15
Protocol Version............................... 1
PAE Capabilities............................... Authenticator
Control Mode................................... auto
```

```
Authenticator PAE State........................ Initialize
Port Status.................................... Authorized
Backend Authentication State................... Initialize
Quiet Period (secs)............................ 60
Transmit Period (secs)......................... 30
Supplicant Timeout (secs)...................... 30
Server Timeout (secs).......................... 30
Maximum Requests............................... 2
Reauthentication Period (secs)................. 3600
Reauthentication Enabled....................... TRUE
Key Transmission Enabled....................... FALSE
Session Timeout................................ 0
Session Termination Action..................... Default
```

Port	The interface whose configuration is displayed.
Protocol Version	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | authorized | unauthorized.
PAE Capabilities	Indicates whether the port can act as an Authenticator or Supplicant.
Control Mode	The control mode under which this port is operating. Possible values are auto, force authorized, and force unauthorized.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0–65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1–65535.

Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1–65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/ Identity before timing out the supplicant. The value will be in the range of 1–10.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1–65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are 'True" or "False".
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Session Timeout	The time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port.
Session Termination Action	The action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed.

If you use the optional parameter **statistics** *interface*, the following 802.1X statistics for the specified port display.

```
(switch) #show dot1x statistics e15

Port........................................... e15
EAPOL Frames Received.......................... 0
EAPOL Frames Transmitted....................... 0
EAPOL Start Frames Received.................... 0
EAPOL Logoff Frames Received................... 0
Invalid EAPOL Frames Received.................. 0
EAPOL Length Error Frames Received............. 0
```

Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

Related Commands

Command	Description
dot1x port-control	Enables the IEEE 802.1X operation on the port.
dot1x pae	Enables the authenticator or supplicant mode on the interface.
dot1x supplicant port-control	Configures the authentication mode for supplicant on the interface.
dot1x supplicant user	Configures the supplicant user.
dot1x re-authentication	Enables periodic re-authentication of the client.

dot1x system-auth-control	Enables 802.1X globally.
dot1x timeout reauth-period	Sets the number of seconds between re-authentication attempts.
dot1x timeout server-timeout	Sets the time that the switch waits for a response from the authentication server.
dot1x timeout quiet-period	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange.
dot1x timeout supp-timeout	Sets the time that the switch waits for a response before retransmitting an Extensible Authentication Protocol (EAP)-request frame to the client.
dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.
clear dot1x statistics	Resets the 802.1x statistics for the specified port or for all ports.
authentication dot1x	Assigns the authentication list to use for 802.1x port security.

show dot1x clients

Use this command to display detailed information about the users who have successfully authenticated on the system or on a specified port.

show dot1x clients {*interface* | **all**}

Syntax Descriptions

Parameter	Description
interface	The port number.
all	Displays information on all ports.

Command Modes

Privileged Exec

Examples

The following shows sample output for all interfaces.

```
(switch) #show dot1x clients e6

Interface.................................... e6
User Name.................................... cisco
Supp MAC Address............................. 00:14:2A:14:CF:52
Session Time................................. 98
Session Timeout.............................. 2
```

Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port.

Related Command

Command	Description
show dot1x users	Displays 802.1x port security user information for locally configured users.

show dot1x users

Use this command to display 802.1x port security user information for locally configured users.

show dot1x users *interface*

Syntax Descriptions

Parameter	Description
interface	The port number.

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show dot1x users e15

Users
-----------------
cisco
```

Related Commands

Command	Description
dot1x supplicant user	Configures the supplicant user.

MAC Based Port Security

You can use the commands described in this section to enable port security on a per-port basis. When a port is secured (locked), only packets with allowable source MAC addresses can be forwarded. All other packets are discarded.

port-security

Use this command to enable port security. Use the `no` form of the command to disable port security.

port-security

no port-security

Default

Port security is disabled globally.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
show port-security	Displays the port-security settings.

port-security mac-address move

Use this command to convert dynamically locked MAC addresses to statically locked addresses on an interface.

port-security mac-address move

Command Modes

Interface Config

Related Commands

Command	Description
show port-security	Displays the port-security settings.

port-security max-dynamic

Use this command to set the maximum number of dynamically locked MAC addresses allowed on a specific port. Use the `no` form of the command to reset it to the default value.

port-security max-dynamic *maxvalue*

no port-security max-dynamic

Syntax Descriptions

Parameter	Description
maxvalue	The maximum number of dynamically locked MAC addresses allowed on the port. The total number of static and dynamic addresses cannot exceed 256.

Default

maxvalue—0

Command Modes

Interface Config

Related Commands

Command	Description
show port-security	Displays the port-security settings.

port-security max-static

Use this command to set the maximum number of statically locked MAC addresses allowed on a specific port. Use the **no** form of the command to reset it to the default value.

port-security max-static *maxvalue*

no port-security max-static

Syntax Descriptions

Parameter	Description
maxvalue	The maximum number of statically locked MAC addresses allowed on a specific port. The total number of static and dynamic addresses cannot exceed 256.

Default

maxvalue—256

Command Modes

Interface Config

Related Commands

Command	Description
show port-security	Displays the port-security settings.

port-security reset port

Use this command to reset the port shutdown by Port Security. If port is not shut down by port-security, then no action is taken.

```
port-security reset port
```

Command Modes

Interface Config

Related Commands

Command	Description
show port-security	Displays the port-security settings.

port-security violation action

Use this command to configure the port behavior for MAC addresses violating the MAC based Port Security. Use the **no** form of the command to reset it to the default values.

```
port-security violation action {discard | {discard-with-trap [rap seconds] |
    {discard-with-shutdown}} {forward-no-learn}}
```

```
no port-security violation action
```

Syntax Descriptions

Parameter	Description
discard	Packets that violate the port-security configuration are discarded, with no further action.
discard-with-trap	Packets that violate the port-security configuration are discarded and a trap will be sent to the trap log.
seconds	The minimum number of seconds between two consecutive traps. The range is 1–1000000.
discard-with-shutdown	Packets that violate the port-security configuration are discarded and the port is shutdown.
forward-no-learn	Packets that violate the port-security configuration are forwarded, but not added to the forwarding database.

Defaults

- Packets that violate the port-security configuration are discarded, with no further action.
- *seconds*—1

Command Modes

Interface Config

Related Commands

Command	Description
show port-security	Displays the port-security settings.

show port-security

Use this command to display the port-security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces. It also shows whether the port is shut down by the port-security feature.

show port-security [{*interface* | **all**}]

Syntax Descriptions

Parameter	Description
interface	The port number.
all	Displays port security configuration for all ports.

Command Modes

Privileged Exec

Examples

This field displays if you do not supply any parameters

```
(switch) #show port-security

Port Security Administration Mode: Enabled
```

If you specify an interface, the following fields display:

```
(switch142E4E) #show port-security e1

        Admin    Dynamic    Static    Violation            Trap      Port
Intf    Mode     Limit      Limit     Action       Trap    Frequency Status
------  -------  ---------  --------  ------------ -------- -------- ------
-
e1      Disabled 0          256       discard      Disabled N/A       Active
```

If you specify the **all** parameter, the same files display for all interfaces.

Intf	The port name.
Admin Mode	Port Locking mode for the interface.

Dynamic Limit	The maximum number of dynamically allocated MAC Addresses.
Static Limit	The maximum number of statically allocated MAC Addresses.
Violation Action	The action to be taken upon a violation.
Trap	Indicates whether traps are enabled or disabled.
Trap Frequency	The trap frequency in seconds.
Port Status	Possible values are Shutdown and Active.

Related Commands

Command	Description
show port-security	Displays the port security administrative mode.

9

Quality of Service

This chapter describes how to use the CLI to configure rate limits for the interfaces and class-of-service processing for switch traffic. It includes the following sections:

- **Rate Limit Profile Commands**
- **Class of Service Commands**

Rate Limit Profile Commands

The rate-limiting feature enables you to set a maximum incoming traffic rate for a port. When the data rate exceeds configured rate, the switch drops all further traffic from the port. Rate limits are applied per port and per VLAN.

To apply rate limits, you first use this page to create one or more rate limit profiles. Profiles specify the criteria that determines when the rate limit is exceeded and, optionally, identify the VLAN that it applies to. Then, you assign rate limit profiles to interfaces.

This section describes the commands you use to create rate limit profiles and assign them to interfaces.

rate-limit profile (Global)

Use this command to create rate limit profile. If a VLAN ID is specified, then the rate limit is for that VLAN only. The profile created with this command can be applied to any interface separately at interface level.

rate-limit profile ***profile-id*** **cir** ***cir-value*** **cbs** ***burst-size*** [**vlan** ***vlan-id***]

Syntax Descriptions

Parameter	Description
profile-id	An ID number you assign to the profile. The range is 1–64.
cir	The committed information rate, which is the rate at which data is transmitted. The rate is averaged over a minimum time increment.
cir-value	The committed information rate value in Kbps. The range is 64 Kbps to the port max speed.
cbs	The committed burst size in KB, which guarantees amount of bandwidth for “bursty” traffic on the port. The range is 4–16384KB KB.
burst-size	The committed burst size value in Kbps. The range is 4–16384 Kbps.
vlan-id	The VLAN ID this profile applies to.

Command Modes

Global Config

Examples

The following command creates a rate limit for VLAN 2 traffic.

```
(switch) (Config)#rate-limit profile 1 cir 64 cbs 64 vlan 2
```

Related Commands

Command	Description
rate-limit profile (Interface)	Applies a profile on a port.
show rate-limit profile	Displays parameters configured in a profile.

rate-limit profile (Interface)

Use this command to apply the profile on a port.

rate-limit profile *profile-id*

Syntax Descriptions

Parameter	Description
profile-id	The rate profile ID number.

Command Modes

Interface Config

Examples

The following command applies rate limit profile 1 to port e15:

```
(switch) (Interface e15)#rate-limit profile 1
```

Related Commands

Command	Description
rate-limit profile (Global)	Creates rate limit profile.
show rate-limit profile	Displays parameters configured in a profile.
show rate-limit interface	Displays the rate limiting profiles on the port.

show rate-limit

Use this command to display the rate limiting profiles on a port.

show rate-limit Interface {*interface*}

Syntax Descriptions

Parameter	Description
interface	The port number.

Command Modes

Privileged EXEC

Examples

The following command shows the rate limit profile applied to interface e15:

```
(switch) #show rate-limit interface e15

Profile ID................................... 1
Cir.......................................... 64 Kbps
Cbs.......................................... 64 KB
VLAN id...................................... 2
```

Related Commands

Command	Description
rate-limit profile (Global)	Creates rate limit profile.
rate-limit profile (Interface)	Applies a profile on a port.
show rate-limit profile	Displays parameters configured in a profile.

show rate-limit profile

Use this command to display parameters configured in a profile.

show rate-limit profile {*profile-id* | **all**}

Syntax Descriptions

Parameter	Description
profile-id	The rate profile ID number.
all	Shows all configured rate limit profiles.

Command Modes

Privileged EXEC

Examples

The following command shows all configured rate limit profiles.

```
(switch) #show rate-limit profile all

Profile ID.................................. 1
Cir......................................... 64 Kbps
Cbs......................................... 64 KB
VLAN id..................................... 2

Profile ID.................................. 2
Cir......................................... 128 Kbps
Cbs......................................... 256 KB
VLAN id..................................... 1
```

Related Commands

Command	Description
rate-limit profile (Global)	Creates rate limit profile.
rate-limit profile (Interface)	Applies the profile on a port.
show rate-limit	Displays the rate limiting profiles on the port.

Class of Service Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class for an interface (in Interface Config mode) or for all interfaces (in Global Config Mode). Use the **no** form of this command to reset an 802.1p priority to its default internal traffic class value for an interface or all interfaces.

classofservice dot1p-mapping ***dot1ppriority trafficclass***

no classofservice dot1p-mapping

Syntax Descriptions

Parameter	Description
dot1ppriority	The 802.1p priority value. The range is 0–7.
trafficclass	The *trafficclass* value. The range is 1–8.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
show classofservice dot1p-mapping	Displays the global Dot1p (IEEE 802.1p) priority mapping to internal traffic classes or the mappings for a specific interface.

classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. Use the `no` form of this command to map each IP DSCP value to its default internal traffic class value.

classofservice ip-dscp-mapping *ipdscp trafficclass*

no classofservice ip-dscp-mapping

Syntax Descriptions

Parameter	Description
ipdscp	The DSCP value, which can be specified as an integer from 0 to 63, or symbolically through one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **ef**.
trafficclass	The *trafficclass* value. The range is 1–8.

Command Modes

Global Config

Related Commands

Command	Description
show classofservice ip-dscp mapping	Displays the global IP DSCP mapping to internal traffic classes.

classofservice ip-precedence-mapping

This command maps an IP-precedence value to an internal traffic class for an interface (in Interface Config mode) or for all interfaces (in Global Config Mode). Use the `no` form of this command to reset an IP precedence value its default internal traffic class value for an interface or all interfaces.

classofservice ip-precedence-mapping *ip-precedence-value trafficclass*

no classofservice ip-precedence-mapping

Syntax Descriptions

Parameter	Description
ip-precedence-value	The IP precedence value. The range is 0–7.
trafficclass	The *trafficclass* value. The range is 1–8.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
show classofservice ip-precedence-mapping	Displays the global IP precedence value mapping to internal traffic classes or the mapping for a specific interface.

classofservice trust

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. Use the **no** form of the command to set the interface mode to the default value (trust dot1p).

NOTE Interface Config mode configuration overrides the Global Config mode configuration for the interface.

classofservice trust {**dot1p** | **ip-dscp** | **ip-precedence** | **untrusted** | **all**}

no classofservice trust

Syntax Descriptions

Parameter	Description
dot1p	Configures the interface to use the 802.1p priority values encoded in incoming packets to assign traffic to queues. The port uses the 802.1p priority value in VLAN-tagged Ethernet frames. For untagged frames, the port default priority is assigned.
ip-dscp	Configures the interface to use the IP DSCP values encoded in incoming packets to assign traffic to queues. The port uses the DSCP marking in the IP packet header for both VLAN tagged and untagged IP packets. Non-IP tagged and untagged frames are assigned the port default priority.
ip-precedence	Configures the interface to use the IP precedence values encoded in incoming packets to assign traffic to queues. If no value is provided, the default priority of the port is assigned. Non-IP frames are assigned the 802.1p priority (VLAN-tagged frames). Untagged non-IP packets share the traffic with Q1 traffic.
untrusted	Configures the interface to ignore the priority values encoded in incoming packets and to use the port’s own priority value instead.
all	Configures the interface to use all encoded priority settings. For IP packets, the port uses the DSCP marking to determine the priority. For non-IP frames, the port uses the 802.1p priority if the frame is VLAN-tagged and the port default priority if the frame is not VLAN tagged.

Default

All ports default to **trust all**.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
show classofservice trust	Displays the current trust mode setting for a specific interface.
show vlan port	Displays the default port priority for a specific interface.
vlan priority	Configure the default port priority for a specific interface.

cos-queue min-bandwidth

Use this command to specify the minimum transmission bandwidth guarantee for each interface queue. The total number of queues supported per interface is platform-specific. Use the `no` form of the command to restore the default for each queue's minimum bandwidth value.

The Interface-Config mode configuration takes precedence over the Global-Config mode configuration.

cos-queue min-bandwidth *bw-1 bw-2 … bw-n*

no cos-queue min-bandwidth

Syntax Descriptions

Parameter	Description
bw-1... bw-n	A percentage of link rate. The range is 0–100 percent. The first value entered corresponds to queue 1, the second to queue 2, and so on. A value of 0 indicates no guaranteed minimum bandwidth for that queue. The sum of all values entered must not exceed 100.

Default

The minimum bandwidth guarantee for each queue is 0% of the link rate.

Command Modes

Global Config

Interface Config

Examples

The following command configures a bandwidth for each of the eight available queues on all interfaces. The total of all bandwidths is 100%.

```
(switch) (Config)#cos-queue min-bandwidth 20 20 20 10 10 10 5 5
```

Related Commands

Command	Description
show interfaces cos-queue	Displays the class-of-service queue configuration for the specified interface.
traffic-shape	Specifies the maximum transmission bandwidth limit on egress for the interface as a whole.

cos-queue wrr

Use this command to activate the weighted scheduler mode for each specified queue. Use the **no** form of the command to restore the default strict scheduler mode for each specified queue.

cos-queue wrr *queue-id-1* [*queue-id-2… queue-id-n*]

no cos-queue wrr *queue-id-1*[*queue-id-2… queue-id-n*]

Syntax Descriptions

Parameter	Description
queue-id-1… queueid-n	The queue IDs on which to use the weighted scheduler mode. Each queue must be separated by a space.

Default

All ports are configured in strict mode.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
show interfaces cos-queue	Displays the class-of-service queue configuration for the specified interface.
traffic-shape	Specifies the maximum transmission bandwidth limit on egress for the interface as a whole.

traffic-shape

Use this command to specify the maximum transmission bandwidth limit on egress for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. Use the `no` form of the command to disable the traffic shaping.

NOTE The Interface Config mode configuration takes precedence over the Global Config mode configuration.

traffic-shape *bw*

no traffic-shape

Syntax Descriptions

Parameter	Description
bw	The maximum bandwidth value. The range is a percentage of the bandwidth (0-100). A value of 0 means traffic-shape is disabled.

Default

Traffic shaping disabled.

Command Modes

Global Config

Interface Config

Related Commands

Command	Description
cos-queue min-bandwidth	Specifies the minimum transmission bandwidth guarantee for each interface queue.
cos-queue wrr	Activates the weighted scheduler mode for each specified queue.
show interfaces cos-queue	Displays the class-of-service queue configuration for the specified interface.

show classofservice dot1p-mapping

Use this command to display the global Dot1p (802.1p) priority mapping to internal traffic classes or the mappings for a specific interface.

show classofservice dot1p-mapping [*interface*]

Syntax Descriptions

Parameter	Description
interface	The port number. If specified, the Dot1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Command Modes

Privileged Exec

Examples

The following command displays the global 802.1p mapping:

```
(switch) #show classofservice dot1p-mapping
 User Priority   Traffic Class
 -------------   -------------
       0               3
       1               1
       2               2
       3               4
       4               5
       5               6
```

```
        6                  7
        7                  8
```

User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

Related Commands

Command	Description
classofservice dot1p-mapping	Maps an 802.1p priority to an internal traffic class.

show classofservice ip-dscp mapping

Use this command to display the global IP DSCP mapping to internal traffic classes.

show classofservice ip-dscp-mapping

Command Modes

Privileged Exec

Examples

The following example shows the first set of DSCP mappings.

```
(switch) #show classofservice ip-dscp-mapping

    IP DSCP        Traffic Class
 -------------     -------------
   0(be/cs0)            1
   1                    1
   2                    1
   3                    1
   4                    1
   5                    1
   6                    1
   7                    1
   8(cs1)               1
   9                    1
   10(af11)             1
   11                   1
   12(af12)             1
   13                   1
   14(af13)            1
   15                  1
   16(cs2)             2
   17                  2
   18(af21)            2
   19                  2
--More-- or (q)uit
```

Related Commands

Command	Description
classofservice ip-dscp-mapping	Maps an IP DSCP value to an internal traffic class.

show classofservice ip-precedence-mapping

Use this command to display the global IP Precedence mapping to internal traffic classes or the mappings for a specific interface.

show classofservice ip-precedence-mapping [*interface*]

Syntax Descriptions

Parameter	Description
interface	The port number. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Command Modes

Privileged Exec

Examples

The following command displays the global IP precedence mappings.

```
(switch) #show classofservice ip-precedence-mapping

 IP Precedence     Traffic Class
 -------------     -------------
       0                 3
       1                 1
       2                 2
       3                 4
       4                 5
```

5	6
6	7
7	8

Related Commands

Command	Description
classofservice ip-precedence-mapping	Maps an IP-precedence value to an internal traffic class for an interface (in Interface Config mode) or for all interfaces (in Global Config Mode).

show classofservice trust

Use this command to display the trust mode setting for a specific interface. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

show classofservice trust [*interface*]

Syntax Descriptions

Parameter	Description
interface	The port number.

Command Modes

Privileged Exec

Examples

The following example shows the output of this command when 802.1p is trusted.

```
(switch) #show classofservice trust
```

```
Class of Service Trust Mode: Dot1P
```

When IP precedence or DSCP is trusted, the following fields also display:

Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

Related Commands

Command	Description
classofservice trust	Sets the class of service trust mode of an interface.

show interfaces cos-queue

Use this command to display the global class-of-service queue configuration or the configured for a specified interface.

show interfaces cos-queue [*interface*]

Syntax Descriptions

Parameter	Description
interface	The port number.

Command Modes

Privileged Exec

Examples

The following example shows output from the command when no interface is specified.

```
(switch) #show interfaces cos-queue

Global Configuration
Interface Shaping Rate......................... 0

Queue Id   Min. Bandwidth   Scheduler Type
```

```
--------    --------------    --------------
1           20                Strict
2           20                Strict
3           20                Strict
4           10                Strict
5           10                Strict
6           10                Strict
7           5                 Strict
8           5                 Strict
```

Queue Id	An interface supports n queues numbered 1 to 8.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.

Related Commands

Command	Description
cos-queue min-bandwidth	Specifies the minimum transmission bandwidth guarantee for each interface queue.
cos-queue wrr	Activates the weighted scheduler mode for each specified queue.
traffic-shape	Specifies the maximum transmission bandwidth limit on egress for the interface as a whole.

10

IP Configuration

This chapter describes how to use the CLI to configure switch IPv4 and IPv6 addresses and the DNS feature.

It contains the following sections:

- **IP Addresses**
- **DNS**

IP Addresses

You can use the commands described in this section to view and configure IPv4 and IPv6 addresses for the management interface and to configure DHCP client settings.

clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management VLAN.

```
clear arp-switch
```

Command Modes

Privileged Exec

Related Commands

Command	Description
show arp switch	Displays the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port.

clear network ipv6 dhcp statistics

Use this command to clear the DHCPv6 client statistics on the network management interface.

```
clear network ipv6 dhcp statistics
```

Command Modes

Privileged Exec

Related Commands

Command	Description
show network ipv6 dhcp statistics	Displays the statistics of the DHCPv6 client running on the network management interface.

dhcp client vendor-id-option

Use this command to enable the DHCP Option-60 (i.e., the vendor class) option. Use the `no` form of the command to disable it.

```
dhcp client vendor-id-option
```

```
no dhcp client vendor-id-option
```

Command Modes

Global Config

Related Commands

Command	Description
dhcp client vendor-id-option-string	Sets the vendor ID option string that is sent in DHCP packets for option-60 sent.
show dhcp client vendor-id-option	Shows whether the switch sends the vendor ID option string as option-60 in DHCP client packets and displays the contents of the string.

dhcp client vendor-id-option-string

Use this command to set the vendor ID option string for use as option-60 in DHCP client packets sent by the switch. Use the no option to delete the vendor ID option string.

dhcp client vendor-id-option-string *string*

no dhcp client vendor-id-option string

Syntax Descriptions

Parameter	Description
string	The vendor-option string to be included in DHCP packets.

Command Modes

Global Config

Related Commands

Command	Description
dhcp client vendor-id-option	Enables the DHCP Option-60 (vendor class option).
show dhcp client vendor-id-option	Shows whether the switch sends the vendor ID option string as option-60 in DHCP client packets and displays the contents of the string.

network ipv6 address

Use this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration, and enable/disable DHCPv6 client protocol information for the management interface. Multiple IPv6 addresses can be configured on the management interface.

Use the `no` form of the command to remove all configured IPv6 prefixes. Use the `no` form with the **address** option to remove the manually configured IPv6 global address on the network port interface. Use the `no` form with the **autoconfig** option to disable the stateless global address autoconfiguration on the network port. Use the `no` form with the **dhcp** option to disable the DHCPv6 client protocol.

network ipv6 address {*address/prefix-length* **[eui64**]| **autoconfig** | **dhcp**}

no network ipv6 address {*address/prefix-length* [**eui64**]| **autoconfig** | **dhcp**}

Syntax Descriptions

Parameter	Description
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	The IPv6 address is formatted in EUI64 format.
autoconfig	Configures the stateless global address autoconfiguration capability.
dhcp	Configures the switch to use DHCPv6 client protocol to obtain its IPv6 address.

Command Modes

Privileged Exec

Examples

The following example enables DHCPv6.

```
(switch) #network ipv6 address dhcp
```

The following example enables stateless global address autoconfiguration.

```
(switch) #network ipv6 address autoconfig
```

The following example configures an IPv6 address.

```
(switch) #network ipv6 address 3ffe:1900:4545:3:200:f8ff:fe21:67cf/24
```

Related Commands

Command	Description
network ipv6 gateway	Configures the IPv6 gateway (i.e., default router) on the management interface.
show network	Displays the configuration settings associated with the switch management interface.

network ipv6 enable

Use this command to enable IPv6 operation on the management interface. Use the `no` form of the command to disable it.

network ipv6 enable

no network ipv6 enable

Default

IPv6 management is enabled.

Command Modes

Privileged Exec

Related Commands

Command	Description
network ipv6 address	Manually configures IPv6 global address.
network ipv6 gateway	Configures IPv6 gateway (i.e. default routers) on the management interface.
network ipv6 neighbor	Adds static IPv6 neighbor entry.
show network	Displays the configuration settings associated with the switch's management interface.

network ipv6 gateway

Use this command to configure IPv6 gateway (i.e., default routers) for the management interface. Use the **no** form of the command to remove the IPv6 gateway.

network ipv6 gateway ***gateway-address***

no network ipv6 gateway

Syntax Descriptions

Parameter	Description
gateway-address	The IPv6 default router address.

Command Modes

Privileged Exec

Related Commands

Command	Description
network ipv6 address	Manually configures IPv6 global address.
show network	Displays the configuration settings associated with the switch management interface.

network ipv6 neighbor

Use this command to add static IPv6 neighbor entry. Use the **no** form of the command to delete a static entry.

network ipv6 neighbor ***ipv6-address mac-address***

network ipv6 neighbor ***ipv6-address mac-address***

Syntax Descriptions

Parameter	Description
ipv6-address	The neighbor’s global IPv6 address.
mac-address	The neighbor’s MAC address.

Command Modes

Privileged Exec

Related Commands

Command	Description
show network ndp	Displays system network IPv6 neighbor entries.

network parms

Use this command to set the IPv4 address, subnet mask, and gateway for the switch. The IP address and the gateway must be in the same subnet.

network parms *ip-address netmask* [*gateway*]

Syntax Descriptions

Parameter	Description
ip-address	The IPv4 address.
netmask	The network mask.
gateway	The default gateway IP address.

Defaults

- Default IP address: 192.168.1.254
- Default mask: 255.255.255.0
- Default gateway: 192.168.1.1

Command Modes

Privileged Exec

Related Commands

Command	Description
show network	Displays the configuration settings associated with the switch management interface.

network protocol

Use this command to specify the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the **bootp** parameter, the switch periodically sends requests to a BOOTP server until a response is received. If you use the **dhcp** parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the **none** parameter, you must configure the network information for the switch manually.

```
network protocol {none | bootp | dhcp}
```

Syntax Descriptions

Parameter	Description
none	Disables DHCP and BOOTP. If none is specified, you can use the **network parms** command to configure IP information for the switch.
bootp	Enables BOOTP.
dhcp	Enables DHCP.

Default

DHCP is enabled.

Command Modes

Privileged Exec

Related Commands

Command	Description
network parms	Set the IP address, subnet mask and gateway IPv4 address for the switch when the switch is not configured to use DHCP or BOOTP to acquire its address.
network ipv6 enable	Enables IPv6 operation on the management interface.
show network	Displays the configuration settings associated with the switch management interface.

ping

Use this command to determine whether a particular IPv4 computer/host is active on the network. Ping provides a synchronous response when initiated from the CLI and web interfaces.

ping {*ip-address* | *hostname*} [**count** *count*][**interval** *interval*][**size** *size*]

Syntax Descriptions

Parameter	Description
ip-address	The IP address of the host to ping.
hostname	The hostname to ping. The DNS service must be enabled to lookup the hostname.
count	The number of ping packets (ICMP Echo requests) to send to the address. The range is 1–15 requests.
interval	The time between Echo Requests. The range is 1–60 seconds.
size	the size, in bytes, of the payload. The range is 0–65507 bytes.

Defaults

- *count*—1
- *interval*—3 seconds
- *size*—0 bytes

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #ping yahoo.com count 3 interval 2 size 1024
 Pinging yahoo.com with 1024 bytes of data:

Reply From 69.147.125.65: icmp_seq = 0. time= 260 msec.
Reply From 69.147.125.65: icmp_seq = 1. time= 260 msec.
Reply From 69.147.125.65: icmp_seq = 2. time= 260 msec.

----yahoo.com PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 260/260/260
```

Related Commands

Command	Description
ping ipv6	Determines whether another computer is on the network.

ping ipv6

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and web interfaces.

ping ipv6 {*ipv6-global-address* | *hostname* | **interface network** *link-local-address*} {[**size** *datagram-size*]}

Syntax Descriptions

Parameter	Description
ipv6-global-address	Specifies and IPv6 global address of the interface to ping.

Parameter	Description
hostname	The hostname of the IPv6 station on the network. Ensure that the DNS services is enabled on the switch to perform hostname lookup.
interface	Use this keyword to specify a link-local address.
network	If using the interface keyword, specify this keyword followed by the link-local IP address.
link-local-address	If using the interface keyword, specify the link-local part of the IPv6 address to ping.
datagram size	The size of the datagram to send. The range is 0–65507 bytes.

Default

datagram-size—0 bytes

Command Modes

Privileged Exec

Usage Guidelines

To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN, as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

You can utilize the ping command over the network port when using an IPv6 global address *ipv6-global-address* | *hostname*. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping request is routed out the network port properly.

Examples

The following shows sample output for the command.

```
(switch) #ping ipv6 3ffe:1900:4545:3:200:f8ff:fe21:67cf

Send count=3, Receive count=3 from 3ffe:1900:4545:3:200:f8ff:fe21:67cf
Average round trip time = 1.00 ms
```

Related Commands

Command	Description
ping	Determines whether another IPv4 computer/host is on the network.

renew dhcp network-port

Use this command to renew the IP address on the network management interface by using DHCP.

renew dhcp network-port

Command Modes

Privileged Exec

Related Commands

Command	Description
show network	Displays the configuration settings associated with the switch management interface.

show arp switch

Use this command to display the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port.

show arp switch

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(Switch) #show arp switch

    MAC Address          IP Address      Interface
------------------- ---------------- ------------
00:00:0C:07:AC:2A   10.131.16.1      Management
00:1A:A0:31:A9:6A   10.131.17.73     Management
```

```
00:1C:23:00:83:40   10.131.16.59     Management
```

Related Commands

Command	Description
show network	Displays the configuration settings associated with the switch management interface.
clear arp-switch	Clears the contents of the switch Address Resolution Protocol (ARP) table that contains entries learned through the Management VLAN.

show dhcp client vendor-id-option

Use this command to show whether the switch sends the vendor ID option string as option-60 in DHCP client packets, and to view the contents of the string.

show dhcp client vendor-id-option

Command Modes

Global Config

Examples

The following shows sample output for the command.

```
(Switch) #show dhcp client vendor-id-option

DHCP Client Vendor Identifier Option........... Enabled
DHCP Client Vendor Identifier Option String.... SF 200E-24P
```

Related Commands

Command	Description
dhcp client vendor-id-option	Sets the vendor ID option string for use as option-60 in DHCP client packets sent by the switch.
dhcp client vendor-id-option-string	Sets the vendor ID option string for use as option-60 in DHCP client packets sent by the switch.

show dhcp client timezone-option

Use this command to show whether the switch has received its timezone information from a DHCP server and the timezone option format in which it was provided.

show dhcp client timezone-option

Command Modes

Global Config

Examples

The following shows sample output for the command.

```
(Switch) #show dhcp client timezone-option

DHCP TimeZone Option........................... TZ-POSIX
Is TimeZone Info Received...................... FALSE
```

Related Commands

Command	Description
clock timezone config dhcp	Sets the clock operational data with the time zone details received from DHCP server.

show network

Use this command to display the configuration settings associated with the switch's management interface. The management interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's management interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The management interface is always considered to be up, whether or not any member ports are up; therefore, the show network command will always show **Interface Status** as **Up**.

show network

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show network

Interface Status............................... Always Up
IP Address..................................... 10.131.11.166
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.131.11.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................ fe80::2ab:cdff:fe14:2e4e/64
Burned In MAC Address.......................... 00:AB:CD:14:2E:4E
Configured IPv4 Protocol....................... DHCP
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Management VLAN ID............................. 1
```

Related Commands

Command	Description
network parms	Sets the IP address, subnet mask and gateway of the device.
show network ndp	Displays the NDP cache information for the management interface.

show network ipv6 dhcp statistics

Use this command to display the statistics of the DHCPv6 client running on the network management interface.

show network ipv6 dhcp statistics

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show network ipv6 dhcp statistics

DHCPv6 Client Statistics
-------------------------
DHCPv6 Advertisement Packets Received.................... 1
DHCPv6 Reply Packets Received............................ 1
Received DHCPv6 Advertisement Packets Discarded.......... 0
Received DHCPv6 Reply Packets Discarded.................. 0
DHCPv6 Malformed Packets Received........................ 0
Total DHCPv6 Packets Received............................ 2
DHCPv6 Solicit Packets Transmitted....................... 9
DHCPv6 Request Packets Transmitted....................... 1
DHCPv6 Renew Packets Transmitted......................... 0
DHCPv6 Rebind Packets Transmitted........................ 0
DHCPv6 Release Packets Transmitted....................... 0
Total DHCPv6 Packets Transmitted......................... 10
```

DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.

DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the network interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the network interface.
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the network interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets.

Related Commands

Command	Description
clear network ipv6 dhcp statistics	Clears the DHCPv6 client statistics on the network management interface.
show network	Displays the configuration settings associated with the switch's management interface.
network protocol	Specifies the network configuration protocol to be used.

show network ndp

Use this command to display the Neighbor Discovery Protocol (NDP) cache information for the management interface.

```
show network ndp
```

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show network ndp

                                                            Neighbor Age
IPv6 Address                         MAC Address       isRtr State    Update
d
------------------------------------ ----------------- ----- -------- ------
fe80::20f:feff:fe03:8d9a             00:0f:fe:03:8d:9a False Stale      1146
```

IPv6 Address	The IPv6 address of the interface.
MAC Address	The MAC Address used.
Neighbor State	The state of the neighbor cache entry. Possible values are: Reachable, Delay.
Age Updated	The time in seconds that has elapsed since an entry was added to the cache.

Related Commands

Command	Description
show network	Displays the configuration settings associated with the switch's management interface.

DNS

The switch supports IPv4 DNS client functionality. When enabled as a DNS client, the switch provides a hostname lookup service to other applications on the switch such as ping, RADIUS, syslog, Auto Configuration, and TFTP. You can add and remove static mappings of domain names to IP addresses. You can also assign hostnames to IP addresses for hosts on the network.

This section describes the commands you use to configure DNS functionality and DNS servers.

clear host

Use this command to delete dynamic entries from the hostname-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

clear host {*name* | **all**}

Syntax Descriptions

Parameter	Description
name	The hostname.
all	Clears all hostnames from the DNS cache.

Command Modes

Privileged Exec

Related Commands

Command	Description
ip host	Defines static hostname-to-IPv4 address mapping in the host cache.
ipv6 host	Defines static hostname-to-IPv6 address mapping in the host cache.
show hosts	Displays the default domain name, a list of name server hosts, the static and the cached list of hostnames and addresses.

ip domain lookup

Use this command to enable the DNS client. Use the `no` form of the command to disable the DNS client.

ip domain lookup

no ip domain lookup

Default

DNS client is enabled.

Command Modes

Global Config

Related Commands

Command	Description
ip domain name	Defines a default domain name that the software uses to complete unqualified hostnames (names with a domain name).
ip name server	Configures the available name servers.

ip domain name

Use this command to define a default domain name that the software uses to complete unqualified hostnames (names with a domain name). To delete the default domain name, use the `no` form of this command.

ip domain-name *name*

no ip domain-name

Syntax Descriptions

Parameter	Description
name	The domain name used to complete an unqualified hostname. This value can be from 1 to 255 characters and should not include an initial period.

Default

No default domain name is configured in the system.

Command Modes

Global Config

Examples

The following example defines a default domain name as yahoo.com.

```
switch(config)#ip domain-name yahoo.com
```

Related Commands

Command	Description
ip domain lookup	Enables the DNS client.
ip name server	Configures the available name servers.

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. Use the **no** form of the command to return to default.

ip domain retry *number*

no ip domain retry

Syntax Descriptions

Parameter	Description
number	The number of times to retry sending a DNS query to the DNS server. The range is 0–100.

Default

number—2

Command Modes

Global Config

Related Commands

Command	Description
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.

Command	Description
ip name server	Configures the available name servers.

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. Use the `no` form of the command to return to default.

ip domain timeout *seconds*

no ip domain timeout

Syntax Descriptions

Parameter	Description
seconds	The time to wait for a response to a DNS query. The range is 0–3600 seconds.

Default

seconds—3

Command Modes

Global Config

Related Commands

Command	Description
ip domain retry	Specifies the number of times to retry sending Domain Name System (DNS) queries.
ip name server	Configures the available name servers.

ip host

Use this command to define static hostname-to-address mapping in the host cache. Use the `no` form of the command to remove the mapping.

ip host *hostname ip-address*

no ip host *hostname*

Syntax Descriptions

Parameter	Description
hostname	The hostname.
ip-address	The IP address of the host.

Command Modes

Global Config

Related Commands

Command	Description
ipv6 host	Defines static hostname-to-IPv6 address mapping in the host cache.
show hosts	Displays the default domain name, a list of name server hosts, the static and the cached list of hostnames and addresses.

ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The preference of the servers is determined by the order they are entered. Use the `no` form of the command to remove a name server.

ip name-server *server-address1* [*server-address2…server-address8*]

no ip name-server *server-address1* [*server-address2…server-address8*]

Syntax Descriptions

Parameter	Description
server-address1… server-address8	Specify from 1 to 8 IPv4 or IPv6 DNS name server addresses, each separated by a space.

Command Modes

Global Config

Related Commands

Command	Description
ip domain lookup	Enables the DNS client.
ip domain retry	Specifies the number of times to retry sending Domain Name System (DNS) queries.
ip domain name	Defines a default domain name that the software uses to complete unqualified hostnames (names with a domain name).

ipv6 host

Use this command to define static hostname-to-IPv6 address mapping in the host cache. The *name* is hostname, and *v6 address* is the IPv6 address of the host. Use the `no` form of the command to remove the mapping.

ipv6 host ***hostname ip-address***

no ipv6 host ***hostname***

Syntax Descriptions

Parameter	Description
hostname	The IPv6 hostname.
ip-address	The IPv6 address of the host.

Command Modes

Global Config

Related Commands

Command	Description
ip host	Defines static hostname-to-IPv4 address mapping in the host cache.
show hosts	Displays the default domain name, a list of name server hosts, the static and the cached list of hostnames and addresses.

show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of hostnames and addresses. *name* ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

show hosts

Command Modes

Privileged Exec

Examples

The following example shows the output for this command.

```
(Switch) #show hosts

hostname....................................... host1
Default domain................................. Domain name is not configured
Default domain list............................ Domain Name List is not configured
Domain Name Lookup............................. Enabled
Number of retries.............................. 2
Retry timeout period........................... 3
Name servers (Preference order)................ 10.131.138.20

Configured hostname-to-address mapping:

 Host                             Addresses
---------------------               ----------------------
host1                             10.131.11.7
host2                             10.131.11.9


 Host                 Total   Elapsed   Type        Addresses
```

```
-------              -------  -------    ----       -----------
www-real.wa1.b.yahoo.com  60      4       IP        209.131.36.158
www.google.com           65171   36       Canonical  www.l.google.com
www.l.google.com         112     36       IP        74.125.127.105
www.l.google.com         112     36       IP        74.125.127.106
www.l.google.com         112     36       IP        74.125.127.147
www.l.google.com         112     36       IP        74.125.127.99
www.l.google.com         112     36       IP        74.125.127.103
www.l.google.com         112     36       IP        74.125.127.104
www.wa1.b.yahoo.com      60       4       Canonical  www-real.wa1.b.yahoo.com
www.yahoo.com            68      19       Canonical  www.wa1.b.yahoo.com
```

Related Commands

Command	Description
ip host	Defines static hostname-to-IPv4 address mapping in the host cache.
ipv6 host	Defines static hostname-to-IPv6 address mapping in the host cache.
ip name server	Configures the available name servers.

11

SNMP

This chapter describes how to use the CLI commands to configure the Simple Network Management Protocol (SNMP) on the switch.

snmp-server community

This command adds and names a new SNMP community. A community name is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level (read or write).

NOTE Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

The maximum number of communities that can be configured is 8.

Use the `no` form of the command to remove this community name from the table.

snmp-server community *name* {**ro** | **rw**} [**ipaddress** *ip-address*]

no snmp-server community *name*

Syntax Descriptions

Parameter	Description
name	The name to assign to the community, up to 16 case-sensitive characters.
ro | rw	ro—Read Only access. rw—Read/Write access.
ipaddress	The IP address that users must have to gain SNMP access through this community. If no value is specified, access is permitted from any IP address.

Command Modes

Global Config

Related Commands

Command	Description
show snmp	Displays SNMP community information.

snmp-server enable

Use this command to enable the SNMP agent on the switch. Use the `no` form of the command to disable it.

```
snmp-server enable
no snmp-server enable
```

Default

The SNMP agent is disabled.

Command Modes

Global Config

Related Commands

Command	Description
snmp-server engineID local	Specifies the Simple Network Management Protocol (SNMP) engine ID on the switch.

snmp-server enable traps authentication

Use this command in Global Config mode to enable the switch to send Simple Network Management Protocol traps when authentication fails. To disable SNMP failed authentication traps, use the `no` form of this command.

```
snmp-server enable traps authentication
no snmp-server enable traps authentication
```

Default

These traps are enabled.

Command Modes

Global Config

Related Commands

Command	Description
show trapflags	Displays trap conditions.

snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. Use the `no` form of the command to disable it.

```
snmp-server enable traps linkmode

no snmp-server enable traps linkmode
```

Default

These traps are enabled.

Command Modes

Global Config

Related Commands

Command	Description
show trapflags	Displays trap conditions.

snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session. Use the `no` form of the command to disable it.

```
snmp-server enable traps multiusers
```

```
no snmp-server enable traps multiusers
```

Default

These traps are enabled.

Command Modes

Global Config

Related Commands

Command	Description
show trapflags	Displays trap conditions.

snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification trap. Use the `no` form of the command to disable it.

```
snmp-server enable traps stpmode
```

```
no snmp-server enable traps stpmode
```

Default

These traps are enabled.

Command Modes

Global Config

Related Commands

Command	Description
show trapflags	Displays trap conditions.

snmp-server host traps

Use this command to specify a host that will receive SNMP version 1 and 2 notifications (traps). To stop a host from receiving notifications, use the `no` form of this command.

snmp-server host {*ip-address* | *hostname*} *community* **traps** [**v1** | **v2**][**dpport**]

no snmp-server host *ip-address* **traps**

Syntax Descriptions

Parameter	Description
ip-address | hostname	The IP address of the host. Or, a hostname from 1-158 characters.
community	The community name that determines the set of notifications that the host receives. The range 1-25 characters.
v1 | v2	The SNMP version that the host supports.
udpport	The UDP port number to use to communicate with the host. The default is 162. The range is 1025-65535.

Command Modes

Global Config

Related Commands

Command	Description
snmp-server community	Adds (and names) a new SNMP community.

Command	Description
show snmp details	Displays the SNMP client and community details.

show snmp

This command displays SNMP client and community details.

show snmp

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
(Switch) #show snmp
SNMP server disabled
Community-String           Community-Access                    IP Address
--------------------        ----------------                   ----------------
community1                  Read/Write                         10.131.11.12

Traps are enabled.

Version 1,2 notifications
Target Address     Type      Community      Version     UDP     TO       Retries
                                                        Port    Sec
----------------   -------   -------------- -------     ------  ---      -----

Version 3 notifications
Target Address   Type      Username         Security     UDP     TO   Retries
                                            Level        Port    Sec
--------------   -------  ----------------- -------      ------  ---  -----
192.168.100.55   Trap    admin              NoAuth-N     162     15   3
=====================================================================================
```

snmp-server engineID local

Use this command to specify the Simple Network Management Protocol (SNMP) engine ID on the switch. Use the `no` form of this command to reset the engine ID to a default value that is created automatically from the switch MAC address.

snmp-server engineID local ***engineid-string***

no snmp-server engineID local

Syntax Descriptions

Parameter	Description
engineid-string	The character string that identifies the engine ID. The range is 6–32 characters. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

Command Modes

Global Config

Examples

The following example configures the Engine ID automatically.

```
switch(config)# snmp-server engineID local default
```

Related Commands

Command	Description
snmp-server community	Adds (and names) a new SNMP community.
show snmp engineid	Displays the SNMP engine ID for the switch.

snmp-server user

Use this command to configure a new SNMP Version 3 user. To delete a user, use the **no** form of this command.

NOTE If the SNMP local engine ID is changed, configured users will no longer be able to connect and will need to be reconfigured.

snmp-server user *username* {**read** | **write**}[**remote** *engine-idstring*][{**auth-md5** *password* | **auth-md5-key** *md5-key* | **auth-sha** *password* | **auth-sha-key** *sha-key*}][{**priv-des** *password* | **priv-des-key** *des-key*] [**priv-aes** *password* | **priv-aes-key** *aes-key*}]**no snmp-server user** *username* [**remote** *engineid-string*]

Syntax Descriptions

Parameter	Description
engine-idstring	The engine ID of the remote SNMP entity to which the user belongs.
username	The name of the user on the host that connects to the agent. The range is 1–30 characters.
auth-md5	The HMAC-MD5-96 authentication level.
password	A password. The range is 1–32 characters.
auth-md5-key	The HMAC-MD5-96 authentication level. Enter a pregenerated MD5 key.
md5-key	Character string, length 32 hex characters.
auth-sha	The HMAC-SHA-96 authentication level.
password	A password. The range is 1–32 characters.
auth-sha-key	The HMAC-SHA-96 authentication level. Enter a pregenerated SHA key.
sha-key	Character string, length 48 characters.
priv-des	The CBC-DES Symmetric Encryption privacy level. Enter a password.
password	A password. The range is 1–32 characters.
priv-des-key	The CBC-DES Symmetric Encryption privacy level. The user should enter a pregenerated key.
des-key	The pregenerated DES encryption key.
priv-aes	The AES Symmetric Encryption privacy level. Enter a password.
password	A password. The range is 1–32 characters.
priv-aes-key	The AES Symmetric Encryption privacy level. The user should enter a pregenerated key.
aes-key	The pregenerated AES encryption key.

Command Modes

Global Config

Related Commands

Command	Description
snmp-server v3-host	Specifies the recipient of Simple Network Management Protocol Version 3 notifications.

snmp-server v3-host

Use this command to specify the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the `no` form of this command.

snmp-server v3-host {*ip-address* | *hostname*} *username* **traps** [**noauth** | **auth** | **priv**][**udpport** *port*]

no snmp-server v3-host {*ip-address* | *hostname*} **traps**

Syntax Descriptions

Parameter	Description
ip-address	The IP address of the host (i.e., the targeted recipient).
Hostname	The name of the host. The range is 1–158 characters.
username	The user name used to generate the notification. (30 characters maximum.)
traps	Indicates that SNMP traps are sent to this host.
Noauth	Specifies sending of a packet without authentication.
Auth	Specifies authentication of a packet without encrypting it.
Priv	Specifies authentication and encryption of a packet.
port	The UDP port of the host to use. The range is 1025–65535. The default is 162.

Command Modes

Global Config

Related Commands

Command	Description
snmp-server user	Configures a new SNMP Version 3 user.

snmp trap link-status all

This command enables link status traps for all interfaces. Use the `no` form of the command to disables link status traps for all interfaces.

```
snmp trap link-status all
no snmp trap link-status all
```

Command Modes

Global Config

Related Commands

Command	Description
snmp trap link-status	Enables link status traps by interface.

snmp trap link-status

This command enables link status traps by interface. Use the `no` form of the command to disables link status traps by interface.

```
snmp trap link-status
no snmp trap link-status
```

Default

Link status traps are enabled on all interfaces.

Command Modes

Interface Config

Related Commands

Command	Description
snmp trap link-status all	Enables link status traps by interface.

show snmp engineid

This command displays the SNMP engine ID for the switch.

show snmp engineid

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show snmp engineid
Local SNMP engineID : 000000630300abcd142e4e0000000000
```

Related Commands

Command	Description
snmp-server engineID local	Specifies the Simple Network Management Protocol (SNMP) engine ID on the switch.

show snmp users

Use this command to display the configuration of users.

show smnp users [*username*]

Syntax Descriptions

Parameter	Description
username	The name of the user. If no user name is specified, configuration information for all users displays.

Command Modes

Privileged EXEC

Examples

The following shows sample output for the command.

```
(switch) #show snmp users

Name          Access Mode     Auth Priv
                              Meth Meth     Remote Engine ID
------------- --------------- ---- -------  -------------------------
joew          Read/Write      MD5           000000630300abcd142e4e0000000000
cisco         Read/Write                    000000630300abcd142e4e00000000
00
```

Name	The name the user enters to login using SNMP.
Access Mode	Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). (The default username **cisco** has Read/Write access.)
Auth Meth	The authentication protocol used for the specified user. (The default username **cisco** is not configured with an authentication method.) The authentication method might be configured to be MD5 or SHA.
Priv Meth	The privacy method used for the SNMP user. The factory default user, **cisco**, is not configured with a privacy method. The privacy method might be AES or DES Symmetric Encryption.
Remote Engine ID	The engine ID of the remote SNMP entity to which the user belongs.

Related Commands

Command	Description
snmp-server user	Configures a new SNMP Version 3 user.

show trapflags

This command displays trap conditions.

show trapflags

Command Modes

Privileged Exec

Examples

The following shows sample output for the command.

```
(switch) #show trapflags

Authentication Flag........................... Enable
Link Up/Down Flag............................. Enable
Multiple Users Flag........................... Enable
Spanning Tree Flag............................ Enable
```

Authentication Flag	Indicates whether traps are sent when an SNMP user fails to authenticate to the switch. The default is Enable.
Link Up/Down Flag	Indicates whether link status traps will be sent. The default is Enable.
Multiple Users Flag	Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port). The default is Enable.
Spanning Tree Flag	Indicates whether spanning tree traps are sent. The default is Enable.

Related Commands

Command	Description
snmp-server enable traps authentication	Enables an Authentication Fail trap.
snmp-server enable traps linkmode	Enables Link Up/Down traps for the entire switch.

Command	Description
snmp-server enable traps multiusers	Enables Multiple User traps.
snmp-server enable traps stpmode	Enables the sending of new root traps and topology change notification trap.