CHAPTER 2

Cisco IOS Commands for the Catalyst 4500 Series Switches

This chapter contains an alphabetical listing of Cisco IOS commands for the Catalyst 4500 series switches. For information about Cisco IOS commands that are not included in this publication, refer to Cisco IOS Release 12.2 configuration guides and command references at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_product_indices_list.html

#macro keywords

To specify the help string for the macro keywords, use the **#macro keywords** command.

#macro keywords [**keyword1**] [**keyword2**] [**keyword3**]

Syntax Description

keyword 1	(Optional) Specifies a keyword that is needed while applying a macro to an interface.
keyword 2	(Optional) Specifies a keyword that is needed while applying a macro to an interface.
keyword 3	(Optional) Specifies a keyword that is needed while applying a macro to an interface.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

If you do not specify the mandatory keywords for a macro, the macro is to be considered invalid and fails when you attempt to apply it. By entering the **#macro keywords** command, you will receive a message indicating what you need to include to make the syntax valid.

Examples

This example shows how to specify the help string for keywords associated with a macro named test:

```
Switch(config)# macro name test
macro name test
Enter macro commands one per line. End with the character '@'.
#macro keywords $VLAN $MAX
swichport
@

Switch(config)# int gi1/1
Switch(config-if)# macro apply test ?
  WORD  Keyword to replace with a value e.g $VLAN, $MAX   << It is shown as help
  <cr>
```

Related Commands

Command	Description
macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.

aaa accounting dot1x default start-stop group radius

To enable accounting for 802.1X authentication sessions, use the **aaa accounting dot1x default start-stop group radius** command. To disable accounting, use the **no** form of this command.

aaa accounting dot1x default start-stop group radius

no aaa accounting dot1x default start-stop group radius

Syntax Description

This command has no arguments or keywords.

Defaults

Accounting is disabled.

Command Modes

Global configuration mode

Usage Guidelines

802.1X accounting requires a RADIUS server.

This command enables the Authentication, Authorization, and Accounting (AAA) client's accounting feature to forward 802.1X update and watchdog packets from the 802.1X supplicant (workstation client) to the authentication (RADIUS) server. (Watchdog packets are defined as EAPOL-LOGON, EAPOL-LOGOFF, and EAPOL-INTERIM messages.) Successful authentication and authorization of the supplicant by the authentication server is required before these packets are considered valid and are forwarded. When the client is reauthenticated, an interim-update accounting notice is sent to the accounting server.

Examples

This example shows how to configure 802.1X accounting:

```
Switch(config)# aaa accounting dot1x default start-stop group radius
```

Note The RADIUS authentication server must be properly configured to accept and log update or watchdog packets from the AAA client.

Related Commands

Command	Description
aaa accounting system default start-stop group radius	Receives the session termination messages after the switch reboots.

aaa accounting system default start-stop group radius

To receive the session termination messages after the switch reboots, use the **aaa accounting system default start-stop group radius** command. To disable accounting, use the **no** form of this command.

aaa accounting system default start-stop group radius

no aaa accounting system default start-stop group radius

Syntax Description

This command has no arguments or keywords.

Defaults

Accounting is disabled.

Command Modes

Global configuration mode

Usage Guidelines

802.1X accounting requires the RADIUS server.

This command enables the AAA client's accounting feature to forward 802.1X update and watchdog packets from the 802.1X supplicant (workstation client) to the authentication (RADIUS) server. (Watchdog packets are defined as EAPOL-LOGON, EAPOL-LOGOFF, and EAPOL-INTERIM messages.) Successful authentication and authorization of the supplicant by the authentication server is required before these packets are considered valid and are forwarded. When the client is reauthenticated, an interim-update accounting notice is sent to the accounting server.

Examples

This example shows how to generate a logoff after a switch reboots:

```
Switch(config)# aaa accounting system default start-stop group radius
```

Note The RADIUS authentication server must be properly configured to accept and log update or watchdog packets from the AAA client.

Related Commands

Command	Description
aaa accounting dot1x default start-stop group radius	Enables accounting for 802.1X authentication sessions.

access-group mode

To specify the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict mode), use the **access-group mode** command. To return to preferred port mode, use the **no** form of this command.

access-group mode {**prefer** {**port** | **vlan**} | **merge**}

no access-group mode {**prefer** {**port** | **vlan**} | **merge**}

Syntax Description

prefer port	Specifies that the PACL mode take precedence if PACLs are configured. If no PACL features are configured on the port, other features applicable to the interface are merged and applied on the interface.
prefer vlan	Specifies that the VLAN-based ACL mode take precedence. If no VLAN-based ACL features are configured on the port's VLAN, the PACL features on the port are applied.
merge	Merges applicable ACL features before they are programmed into the hardware.

Defaults

PACL override mode

Command Modes

Interface configuration mode

Usage Guidelines

On the Layer 2 interface, prefer port, prefer VLAN, and merge modes are supported. A Layer 2 interface can have one IP ACL applied in either direction (one inbound and one outbound).

Examples

This example shows how to make the PACL mode on the switch take effect:

```
(config-if)# access-group mode prefer port
```

This example shows how to merge applicable ACL features:

```
(config-if)# access-group mode merge
```

Related Commands

Command	Description
show access-group mode interface	Displays the ACL configuration on a Layer 2 interface.
show ip interface (refer to Cisco IOS documentation)	Displays the IP interface configuration.
show mac access-group interface	Displays the ACL configuration on a Layer 2 interface.

access-list hardware capture mode

To select the mode of capturing control packets, use the **access-list hardware capture mode** command.

access-list hardware capture mode {**global** | **vlan**}

Syntax Description

global	Specifies the capture of control packets globally on all VLANs.
vlan	Specifies the capture of control packets on a specific VLAN.

Defaults

The control packets are globally captured.

Command Modes

Global configuration mode

Usage Guidelines

Before configuring the capture mode, it is best to examine and modify your configuration to globally disable features such as DHCP snooping or IGMP snooping, and instead enable them on specific VLANs.

When changing to path managed mode, be aware that control traffic may be bridged in hardware or dropped initially until the per-vlan CAM entries are programmed in hardware.

You must ensure that any access control configuration on a member port or VLAN does not deny or drop the control packets from being forwarded to the CPU for the features which are enabled on the VLAN. If control packets are not permitted then the specific feature does not function.

Examples

This example shows how to configure the switch to capture control packets on VLANs that are configured to enable capturing control packets:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware capture mode vlan
Switch(config)# end
Switch#
```

This example shows how to configure the switch to capture control packets globally across all VLANs (using a static ACL):

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware capture mode global
Switch(config)# end
Switch#
```

This example shows another way to configure the switch to capture control packets globally across all VLANs:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no access-list hardware capture mode vlan
Switch(config)# end
Switch#
```

access-list hardware entries

To designate how ACLs are programmed into the switch hardware, use the **access-list hardware entries** command.

access-list hardware entries {**packed** | **scattered**}

Syntax Description

packed	Directs the software to use the first entry with a matching mask when selecting an entry from the ACL TCAM for programming the ACEs in an ACL.
scattered	Directs the software to use the first entry with a free mask when selecting an entry from the ACL TCAM for programming the ACEs in an ACL.

Defaults

The ACLs are programmed as packed.

Command Modes

Global configuration mode

Usage Guidelines

Two types of hardware resources are used when ACLs are programmed: entries and masks. If one of these resources is consumed, no additional ACLs can be programmed into the hardware. If the masks are consumed, but the entries are available, change the programming algorithm from **packed** to **scattered** to make the masks available. This action allows additional ACLs to be programmed into the hardware.

The goal is to use TCAM resources more efficiently; that is, to minimize the number of masks per ACL entries. To compare TCAM utilization when using the **scattered** or **packed** algorithms, use the **show platform hardware acl statistics utilization brief** command. To change the algorithm from **packed** to **scattered**, use the **access-list hardware entries** command.

Examples

This example shows how to program ACLs into the hardware as packed. After they are programmed, you will need 89 percent of the masks to program only 49 percent of the ACL entries.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware entries packed
Switch(config)# end
Switch#
01:15:34: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
Entries/Total(%)  Masks/Total(%)
                                       -----------------  ---------------
            Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   460 /  512 ( 89)
            Input  Acl(PortOrVlan)      6 / 4096 (  0)     4 /  512 (  0)
            Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)

            L4Ops: used 2 out of 64
```

```
Switch#
```

This example shows how to reserve space (scatter) between ACL entries in the hardware. The number of masks required to program 49 percent of the entries has decreased to 49 percent.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware entries scattered
Switch(config)# end
Switch#
01:39:37: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
Entries/Total(%)  Masks/Total(%)
                                       -----------------  ---------------
            Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   252 /  512 ( 49)
            Input  Acl(PortOrVlan)      6 / 4096 (  0)     5 /  512 (  0)
            Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)

            L4Ops: used 2 out of 64
Switch#
```

access-list hardware region

To modify the balance between TCAM regions in hardware, use the **access-list hardware region** command.

access-list hardware region {**feature** | **qos**} {**input** | **output**} **balance** {*bal-num*}

Syntax Description

feature	Specifies adjustment of region balance for ACLs.
qos	Specifies adjustment of region balance for QoS.
input	Specifies adjustment of region balance for input ACL and QoS.
output	Specifies adjustment of region balance for output ACL and QoS.
balance *bal-num*	Specifies relative sizes of the PandV and PorV regions in the TCAM; valid values are between 1 and 99.

Defaults

The default region balance for each TCAM is 50.

Command Modes

Global configuration mode

Usage Guidelines

PandV is a TCAM region containing entries which mask in both the port and VLAN tag portions of the flow label.

PorV is a TCAM region containing entries which mask in either the port or VLAN tag portion of the flow label, but not both.

A balance of 1 allocates the minimum number of PandV region entries and the maximum number of PorV region entries. A balance of 99 allocates the maximum number of PandV region entries and the minimum number of PorV region entries. A balance of 50 allocates equal numbers of PandV and PorV region entries in the specified TCAM.

Balances for the four TCAMs can be modified independently.

Examples

This example shows how to enable the MAC notification trap when a MAC address is added to a port:

```
Switch# configure terminal
Switch(config)# access-list hardware region feature input balance 75
Switch(config)#
```

action

To specify an action to be taken when a match occurs in a VACL, use the **action** command. To remove an action clause, use the **no** form of this command.

action {**drop** | **forward**}

no action {**drop** | **forward**}

Syntax Description

drop	Sets the action to drop packets.
forward	Sets the action to forward packets to their destination.

Defaults

This command has no default settings.

Command Modes

VLAN access-map mode

Usage Guidelines

In a VLAN access map, if at least one ACL is configured for a packet type (IP or MAC), the default action for the packet type is **drop** (deny).

If an ACL is not configured for a packet type, the default action for the packet type is **forward** (permit).

If an ACL for a packet type is configured and the ACL is empty or undefined, the configured action will be applied to the packet type.

Examples

This example shows how to define a drop action:

```
Switch(config-access-map)# action drop
Switch(config-access-map)#
```

This example shows how to define a forward action:

```
Switch(config-access-map)# action forward
Switch(config-access-map)#
```

Syntax Description

Command	Description
match	Specifies a match clause by selecting one or more ACLs for a VLAN access-map sequence.
show vlan access-map	Displays the contents of a VLAN access map.
vlan access-map	Enters VLAN access-map command mode to create a VLAN access map.

active

To enable the destination profile, use the **active** command.

active

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

cfg-call-home-profile

Usage Guidelines

By default the profile is enabled upon creation.

Examples

This example shows how to enable the destination profile:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# active
```

Related Commands

Command	Description
destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

ancp client port identifier

To create a mapping for an ANCP client to identify an interface on which ANCP should start or stop a multicast stream, use the **ancp client port identifier** command.

ancp client port identifier *identifying name* **vlan** *vlan number* **interface** *interface*

Syntax Description

identifier name	Identifier used by the ANCP server to specify an interface member of a VLAN.
vlan number	VLAN identifier.
interface	Interface member of this VLAN.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

The ANCP server can use either the DHCP option 82 circuit ID or an identifier created with this commandto identify the port. Use only one of the two methods; do not interchange them. If you use the DHCP option 82, the port identifier used by the ANCP server should be (in hex) 0x01060004[vlan][intf]. For example, VLAN 19 and interface Fast Ethernet 2/3 will provide 0x0106000400130203. If you use the port identifier, however, use the exact string provided on the CLI.

Note This command is available only after you set the box in ANCP client mode with the **ancp mode client** configuration command.

Examples

This example shows how to identify interface FastEthernet 7/3 on VLAN 10 with the string NArmstrong:

```
Switch# ancp client port identifier NArmstrong vlan 10 interface FastEthernet 7/3
```

Related Commands

Command	Description
ancp mode client	Sets the router to become an ANCP client.

ancp client server

To set the IP address of the remote ANCP server, use the **ancp client server** command.

ancp client server *ipaddr of server* **interface** *interface*

Syntax Description

ipaddr of server	IP address of the ANCP server the client must connect with TCP.
interface	Interface to use for the connection.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

The interface can be the direct interface connected towards the ANCP server (if only one) or a loopback interface if several interfaces are available for connecting to the server and proper routing is set. (An IP address must be configured on this interface and it should not be in shutdown state.) Along with the **ancp mode client** command, the **ancp client server** command is required in order to activate the ANCP client. Once you enter this command, the ANCP client tries to connect to the remote server.

Examples

This example shows how to indicate to the ANCP client the IP address of the ANCP server it needs to connect to:

```
Switch# ancp client server 10.1.2.31 interface FastEthernet 2/1
```

Related Commands

Command	Description
ancp mode client	Sets the router to become an ANCP client.

ancp mode client

To set the router to become an ANCP client, use the **ancp mode client** command.

ancp mode client

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

To fully activate ANCP, the administrator must also set the ANCP server IP address to which the ANCP client must connect.

Examples

This example shows how to set the router to become an ANCP client:

```
Switch# ancp mode client
```

Related Commands

Command	Description
ancp client server	Displays multicast streams activated by ANCP.

apply

To implement a new VLAN database, increment the configuration number, save the configuration number in NVRAM, and propagate the configuration number throughout the administrative domain, use the **apply** command.

apply

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

VLAN configuration mode

Usage Guidelines

The **apply** command implements the configuration changes that you made after you entered VLAN database mode and uses them for the running configuration. This command keeps you in VLAN database mode.

You cannot use this command when the switch is in the VTP client mode.

You can verify that the VLAN database changes occurred by entering the **show vlan** command from privileged EXEC mode.

Examples

This example shows how to implement the proposed new VLAN database and to recognize it as the current database:

```
Switch(config-vlan)# apply
Switch(config-vlan)#
```

Related Commands

Command	Description
exit (refer to Cisco IOS documentation)	Closes an active terminal session by logging off the switch.
reset	Leaves the proposed new VLAN database but remains in VLAN configuration mode and resets the proposed new database to be identical to the VLAN database currently implemented.
show vlan	Displays VLAN information.
shutdown vlan (refer to Cisco IOS documentation)	Shuts down VLAN switching.
vtp (global configuration mode)	Modifies the name of a VTP configuration storage file.

arp access-list

To define an ARP access list or add clauses at the end of a predefined list, use the **arp access-list** command.

arp access-list *name*

Syntax Description

name	Specifies the access control list name.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Examples

This example shows how to define an ARP access list named static-hosts:

```
Switch(config)# arp access-list static-hosts
Switch(config)#
```

Related Commands

Command	Description
deny	Denies an ARP packet based on matches against the DHCP bindings.
ip arp inspection filter vlan	Permits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and applies it to a VLAN.
permit	Permits an ARP packet based on matches against the DHCP bindings.

attach module

To remotely connect to a specific module, use the **attach module** configuration command.

attach module *mod*

Syntax Description

mod	Target module for the command.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command applies only to the Access Gateway Module on Catalyst 4500 series switches.

The valid values for *mod* depend on the chassis that are used. For example, if you have a Catalyst 4506 chassis, valid values for the module are from 2 to 6. If you have a 4507R chassis, valid values are from 3 to 7.

When you execute the **attach module** *mod* command, the prompt changes to Gateway#.

This command is identical in the resulting action to the **session module** *mod* and the **remote login module** *mod* commands.

Examples

This example shows how to remotely log in to an Access Gateway Module:

```
Switch# attach module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

Related Commands

Command	Description
remote login module	Remotely connects to a specific module.
session module	Logs in to the standby supervisor engine using a virtual console.

authentication control-direction

To change the port control to unidirectional or bidirectional, use the **authentication control-direction** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication control-direction {**both** | **in**}

no authentication control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default

both

Command Modes

Interface configuration mode

Usage Guidelines

The **authentication control-direction** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(50)SG and later releases:

dot1x control-direction {**both** | **in**}

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports.

IEEE 802.1X controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. IEEE 802.1X authenticates each user device that connects to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device authenticates, 802.1X access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device connects. After authentication succeeds, normal traffic can pass through the port.

- Unidirectional state—When you configure a port as unidirectional with the **dot1x control-direction** interface configuration command, the port changes to the spanning-tree forwarding state.

  When the unidirectional controlled port is enabled, the connected host is in sleeping mode or power-down state. The host does not exchange traffic with other devices in the network. If the host connected to the unidirectional port that cannot send traffic to the network, the host can only receive traffic from other devices in the network.

- Bidirectional state—When you configure a port as bidirectional with the **dot1x control-direction** interface configuration command, the port is access-controlled in both directions. In this state, the switch port sends only EAPOL.

Using the **both** keyword or using the **no** form of this command changes the port to its bidirectional default setting.

Setting the port as bidirectional enables 802.1X authentication with Wake-on-LAN (WoL).

You can verify your settings by entering the **show authentication** privileged EXEC command.

Examples

The following example shows how to enable unidirectional control:

```
Switch(config-if)# authentication control-direction in
Switch(config-if)#
```

The following example shows how to enable bidirectional control:

```
Switch(config-if)# authentication control-direction both
Switch(config-if)#
```

The following example shows how to return to the default settings:

```
Switch(config-if)# no authentication control-direction
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication critical recovery delay

To configure the 802.1X critical authentication parameters, use the **authentication critical recovery delay** command in global configuration mode. To return to the default settings, use the **no** form of this command.

authentication critical recovery delay *milliseconds*

no authentication critical recovery delay

Syntax Description

milliseconds	Specifies the recovery delay period in milliseconds to wait to reinitialize a critical port when an unavailable RADIUS server becomes available. The rang is 1 to 10000 milliseconds.

Command Default

10000 milliseconds

Command Modes

Global configuration mode

Usage Guidelines

The **authentication critical recovery delay** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(50)SG and later releases:

dot1x critical recovery delay *milliseconds*

You can verify your settings by entering the **show authentication** privileged EXEC command.

Examples

This example shows how to set the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available:

```
Switch(config)# authentication critical recovery delay 1500
Switch(config)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication event

To configure the actions for authentication events, use the **authentication event** interface configuration command. To return to the default settings, use the **no** form of this command.

authentication event fail [**retry** *count*] **action** [**authorize vlan** *vlan* | **next-method**}

authentication event server {**alive action reinitialize** | **dead action authorize [vlan** *vlan*] | **voice** | **dead action reinitialize [vlan** *vlan*]}}

authentication event no-response action authorize vlan *vlan*]}

no authentication event {**fail**} | {**server** {**alive** | **dead**}} | {**no-response**}

Syntax Description

fail	Specifies the behavior when an authentication fails due to bad user credentials.
retry *count*	(Optional) Specifies the number of times to retry failed authentications. Range is 0 to 5. Default is 2.
fail action authorize vlan *vlan*	When authentication fails due to wrong user credentials, authorizes the port to a particular VLAN.
fail action next-method	Specifies that the required action for an authentication event moves to the next authentication method.
server alive action reinitialize	Configures the authentication, authorization, and accounting (AAA) server alive actions as reinitialize all authorized clients for authentication events.
server dead action authorize [vlan *vlan* **| voice**	Configures the AAA server dead actions to authorize data or voice clients for the authentication events.
server dead action reinitialize vlan *vlan*	Configures the AAA server dead actions to reinitialize all authorized data clients for authentication events.
no-response action authorize	When the client does not support 802.1x, authorizes the port to a particular VLAN.

Command Default

The default settings are as follows:

- The *count* is 2 by default.
- The current authentication method is retried indefinitely (and fails each time) until the AAA server becomes reachable.

Command Modes

Interface configuration mode

Usage Guidelines

The **authentication event fail** command replaces the following 802.1X commands, which are deprecated in Cisco IOS Release 12.2(50)SG and later releases:

- [**no**] **dot1x auth-fail max-attempts** *count*
- [**no**] **dot1x auth-fail vlan** *vlan*

The **authentication event fail** command is supported only for 802.1X to signal authentication failures. By default, this failure type causes the authentication method to be retried. You can configure either to authorize the port in the configured VLAN or to failover to the next authentication method. Optionally, you can specify the number of authentication retries before performing this action.

The **authentication event server** command replaces the following 802.1X commands, which are deprecated in Cisco IOS Release 12.2(50)SG and later releases:

- [**no**] **dot1x critical**
- [**no**] **dot1x critical vlan** *vlan*
- [**no**] **dot1x critical recover action initialize**

The **authentication event server** command specifies the behavior when the AAA server becomes unreachable, ports are authorized in the specified VLAN.

The **authentication server alive action** command specifies the action to be taken once the AAA server becomes reachable again.

You can verify your settings by entering the **show authentication** privileged EXEC command.

The **authentication event no-response** command replaces the following 802.1X command, which is deprecated in Cisco IOS Release 12.2(50)SG and later releases:

- [**no**] **dot1x guest-vlan** *vlan*

The **authentication event no-response** command specifies the action to be taken when the client does not support 802.1X.

Examples

The following example shows how to specify that when an authentication fails due to bad user credentials, the process advances to the next authentication method:

```
Switch(config-if)# authentication event fail action next-method
Switch(config-if)#
```

The following example shows how to specify the AAA server alive actions as reinitialize all authorized clients for authentication events:

```
Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)#
```

The following example shows how to specify the AAA server dead actions that authorize the port for authentication events:

```
Switch(config-if)# authentication event server dead action authorize
Switch(config-if)#
```

The following example shows how to specify the conditions when a client doesn't support 802.1X to authorize the port for authentication events:

```
Switch(config-if)# authentication event authentication event no-response action authorize
vlan 10
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication fallback

To enable WebAuth fallback and to specify the fallback profile to use when failing over to WebAuth, use the **authentication fallback** interface command. To return to the default setting, use the **no** form of this command.

authentication fallback *profile*

Syntax Description

profile	Name to use when failing over to WebAuth (maximum of 200 characters).

Command Default

Disabled

Command Modes

Interface configuration mode

Usage Guidelines

By default, if 802.1X times out and if MAB fails, WebAuth is enabled.

The **authentication fallback** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(50)SG and later releases:

[no] dot1x fallback profile

The Webauth fallback feature allows you to have those clients that do not have an 802.1X supplicant and are not managed devices to fall back to the WebAuth method.

You can verify your settings with the **show authentication** privileged EXEC command.

Examples

This example shows how to enable WebAuth fallback and specify the fallback profile to use when failing over to WebAuth:

```
Switch(config-if)# authentication fallback fallbacktest1
Switch(config-if)#
```

This example shows how to disable WebAuth fallback:

```
Switch(config-if)# no authentication fallback fallbacktest1
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication host-mode

To define the classification of a session that will be used to apply the access-policies in host-mode configuration, use the **authentication host-mode** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

authentication host-mode {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**]

[**no**] **authentication host-mode** {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**]

Syntax Description

single-host	Specifies the session as an interface session, and allows one client on the port only. This is the default host mode when enabling 802.1X.
multi-auth	Specifies the session as a MAC-based session. Any number of clients are allowed on a port in data domain and only one client in voice domain, but each one is required to authenticate separately.
multi-domain	Specifies the session based on a combination of MAC address and domain, with the restriction that only one MAC is allowed per domain.
multi-host	Specifies the session as an interface session, but allows more than one client on the port.
open	(Optional) Configures the host-mode with open policy on the port.

Command Default

This command has no default settings.

Command Modes

Interface configuration mode

Usage Guidelines

Single-host mode classifies the session as an interface session (for example, one MAC per interface). Only one client is allowed on the port, and any policies that are downloaded for the client are applied to the whole port. A security violation is triggered if more than one client is detected.

Multi-host mode classifies the session as an interface session, but the difference with this host-mode is that it allows more than one client to attach to the port. Only the first client that is detected on the port will be authenticated and the rest will inherit the same access as the first client. The policies that are downloaded for the first client will be applied to the whole port.

Multi-domain mode classifies the session based on a combination of MAC address and domain, with the restriction that only one MAC is allowed per domain. The domain in the switching environment refers to the VLAN, and the two supported domains are the DATA domain and the voice domain. Only one client is allowed on a particular domain. So, only two clients (MACs) per port are supported. Each one is required to authenticate separately. Any policies that are downloaded for the client will be applied for that client's MAC/IP only and will not affect the other on the same port. The clients can be authenticated using different methods (such as 802.1X for PC, MAB for IP phone, or vice versa). No restriction exists on the authentication order.

The only caveat with the above statement is that web-based authentication is only available for data devices because a user is probably operating the device and HTTP capability exists. Also, if web-based authentication is configured in MDA mode, the only form of enforcement for all types of devices is downloadable ACLs (dACL). The restriction is in place because VLAN assignment is not supported for web-based authentication. Furthermore, if you use dACLs for data devices and not for voice devices, when the user's data falls back to webauth, voice traffic is affected by the ACL that is applied based on the fallback policy. Therefore if webauth is configured as a fallback on an MDA enabled port, dACL is the only supported enforcement method.

Multi-auth mode classifies the session as a MAC-based. No limit exists for the number of clients allowed on a port data domain. Only one client is allowed in a voice domain and each one is required to authenticate separately. Any policies that are downloaded for the client are applied for that client's MAC or IP only and do not affect others on the same port.

The optional pre-authentication open access mode allows you to gain network access before authentication is performed.This is primarily required for the PXE boot scenario, but not limited to just that use case, where a device needs to access the network before PXE times out and downloads a bootable image possibly containing a supplicant.

The configuration related to this feature is attached to the host-mode configuration whereby the host-mode itself is significant for the control plane, while the open access configuration is significant for the data plane. Open-access configuration has absolutely no bearing on the session classification. The host-mode configuration still controls this. If the open-access is defined for single-host mode, the port still allows only one MAC address. The port forwards traffic from the start and is only restricted by what is configured on the port. Such configurations are independent of 802.1X. So, if there is **no** form of access-restriction configured on the port, the client devices have full access on the configured VLAN.

You can verify your settings with the **show authentication** privileged EXEC command.

Examples

This example shows how to define the classification of a session that are used to apply the access-policies using the host-mode configuration:

```
Switch(config-if)# authentication host-mode single-host
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication open

To enable open access on this port, use the **authentication open** command in interface configuration mode. To disable open access on this port, use the **no** form of this command.

authentication open

no authentication open

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration mode

Usage Guidelines

Open Access allows clients or devices to gain network access before authentication is performed.

You can verify your settings with the **show authentication** privileged EXEC command.

This command overrides the **authentication host-mode** *session-type* **open** global configuration mode command for the port only.

This command operates per-port rather than globally.

Examples

The following example shows how to enable open access to a port:

```
Switch(config-if)# authentication open
Switch(config-if)#
```

The following example shows how to enable open access to a port:

```
Switch(config-if)# no authentication open
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication order

To specify the order in which authentication methods should be attempted for a client on an interface, use the **authentication order** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

authentication order *method1* [*method2*] [*method3*]

no authentication order

Syntax Description

method1	Authentication method to be attempted. The valid values are as follows: • **dot1x**—Adds the dot1x authentication method. • **mab**—Adds the MAB authentication method. • **webauth**—Adds the WebAuth authentication method.
method2 *method3*	(Optional) Authentication method to be attempted. The valid values are as follows: • **dot1x**—Adds the dot1x authentication method. • **mab**—Adds the MAB authentication method. • **webauth**—Adds the WebAuth authentication method.

Command Default

The default order is dot1x, MAB, then WebAuth.

Command Modes

Interface configuration mode

Usage Guidelines

Once you enter the **authentication order** command, only those methods explicitly listed will run. Each method may be entered only once in the run list and no methods may be entered after you enter the **webauth** keyword.

Authentication methods are applied in the configured (or default) order until authentication succeeds. For authentication fails, failover to the next authentication method occurs (subject to the configuration of authentication event handling).

You can verify your settings with the **show authentication** privileged EXEC command.

Examples

The following example shows how to specify the order in which authentication methods should be attempted for a client on an interface:

```
Switch(config-if)# authentication order mab dot1x webauth
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication periodic

To enable reauthentication for this port, use the **authentication periodic** command in interface configuration mode. To disable reauthentication for this port, use the **no** form of this command.

authentication periodic

no authentication periodic

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration mode

Usage Guidelines

The reauthentication period can be set using the **authentication timer** command.

You can verify your settings by entering the **show authentication** privileged EXEC command.

Examples

The following example shows how to enable reauthentication for this port:

```
Switch(config-if)# authentication reauthentication
Switch(config-if)#
```

The following example shows how to disable reauthentication for this port:

```
Switch(config-if)# no authentication reauthentication
Switch(config-if)#
```

Related Commands

Command	Description
authentication timer	Configures the authentication timer.
show authentication	Displays Authentication Manager information.

authentication port-control

To configure the port-control value, use the **authentication port-control** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication port-control [**auto** | **force-authorized** | **force-unauthorized**]

no authentication port-control

Syntax Description

auto	(Optional) Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state.
force-authorized	(Optional) Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	(Optional) Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Command Default

force-authorized

Command Modes

Interface configuration mode

Usage Guidelines

The following guidelines apply to Ethernet switch network modules:

- The 802.1X protocol is supported on Layer 2 static-access ports.
- You can use the **auto** keyword only if the port is not configured as one of the following types:
  - Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
  - EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error message appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
  - Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

You can verify your settings with the **show authentication** privileged EXEC command.

The **auto** keyword allows you to send and receive only Extensible Authentication Protocol over LAN (EAPOL) frames through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the system through the client's MAC address.

Examples

The following example shows that the authentication status of the client PC will be determined by the authentication process:

```
Switch(config-if)# authentication port-control auto
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication priority

To specify the priority of authentication methods on an interface, use the **authentication priority** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

authentication priority *method1* [*method2*] [*method3*]

no authentication priority

Syntax Description

method1	Authentication method to be attempted. The valid values are as follows: • **dot1x**—Adds the dot1x authentication method. • **mab**—Adds the MAB authentication method. • **webauth**—Adds the Webauth authentication method.
method2 *method3*	(Optional) Authentication method to be attempted. The valid values are as follows: • **dot1x**—Adds the dot1x authentication method. • **mab**—Adds the MAB authentication method. • **webauth**—Adds the Webauth authentication method.

Command Default

The default order is dot1x, MAB, then webauth.

Command Modes

Interface configuration mode

Usage Guidelines

Configuring priorities for authentication methods allows a higher priority method (not currently running) to interrupt an authentication in progress with a lower priority method. Alternatively, if the client is already authenticated, an interrupt from a higher priority method can cause a client, which was previously authenticated using a lower priority method, to reauthenticate.

The default priority of a method is equivalent to its position in the order of execution list. If you do not configure a priority, the relative priorities (highest first) are dot1x, MAB and then webauth. If you enter the **authentication order** command, the default priorities are the same as the configured order.

You can verify your settings with the **show authentication** privileged EXEC command.

Examples

The following example shows how to specify the priority in which authentication methods should be attempted for a client on an interface:

```
Switch(config-if)# authentication priority mab dot1x webauth
Switch(config-if)#
```

Related Commands

Command	Description
authentication order	Specifies the order in which authentication methods should be attempted for a client on an interface.
show authentication	Displays Authentication Manager information.

authentication timer

To configure the authentication timer, use the **authentication timer** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

authentication timer {{**inactivity** *value*} | {**reauthenticate** {**server** | *value*}} | {**restart** *value*}}

no authentication timer {{**inactivity** *value*} | {**reauthenticate** *value*} | {**restart** *value*}}

Syntax Description

inactivity *value*	Specifies the amount of time in seconds that a host is allowed to be inactive before being authorized. Range is 1 to 65535. Default is Off. **Note** The inactivity value should be less than the reauthenticate timer value, but configuring the inactivity value higher than the reauthenticate timer value is not considered an error.
reauthenticate server	Specifies that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as Session-Timeout (RADIUS Attribute 27).
reauthenticate *value*	Specifies the amount of time in seconds after which an automatic reauthentication is initiated. Range is 1 to 65535. Default is 3600.
restart *value*	Specifies the amount of time in seconds after which an attempt is made to authenticate an unauthorized port. Range is 1 to 65535. Default is Off.

Command Default

The default settings are as follows:

- **inactivity** *value*—Off.
- **reauthenticate** *value*—3600
- **restart** *value*—Off

Command Modes

Interface configuration mode

Usage Guidelines

Reauthentication only occurs if it is enabled on the interface.

Note You should change the default values of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.

During the inactivity period, the Ethernet switch network module does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number less than the default.

The **reauthenticate** keyword affects the behavior of the Ethernet switch network module only if you have enabled periodic reauthentication with the **authentication reauthentication** global configuration command.

Examples

The following example shows how to specify that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as Session-Timeout (RADIUS Attribute 27):

```
Switch(config-if)# authentication timer reauthenticate server
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication violation

Use the **authentication violation** interface configuration command to configure the violation mode: restrict, shutdown, and replace.

In single-host mode, a security violation is triggered when more than one device are detected on the data vlan. In multidomain authentication mode, a security violation is triggered when more than one device are detected on the data or voice VLAN.

Security violation cannot be triggered in multiplehost or multiauthentication mode.

authentication violation { **restrict** | **shutdown** | **replace**}

no authentication violation {**restrict** | **shutdown** | **replace**}

Syntax Description

restrict	Generates a syslog error when a violation error occurs.
shutdown	Error disables the [virtual] port on which an unexpected MAC address occurs.
replace	Replaces the existing host with the new host, instead of errordisabling or restricting the port.

Defaults

Shut down the port. If the **restrict** keyword is configured, the port does not shutdown.

Command Modes

Interface configuration

Usage Guidelines

When a new host is seen in single or multiple- domain modes, **replace** mode tears down the old session and authenticates the new host.

Examples

This example shows how to configure violation mode shutdown on a switch:

```
Switch# configure terminal
Switch(config)# authentication violation shutdown
```

A port is error-disabled when a security violation triggers on shutdown mode. The following syslog messages displays:

```
%AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface <interface name>, new
MAC address <mac-address> is seen.
%PM-4-ERR_DISABLE: security-violation error detected on <interface name>, putting
<interface name> in err-disable state
```

Related Commands

Command	Description
authentication control-direction	Configures the port mode as unidirectional or bidirectional.
authentication event	Sets the action for specific authentication events.

Command	Description
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
show authentication	Displays information about authentication manager events on the switch.

auto qos classify

To generate a QoS configuration for an untrusted interface, use the **auto qos classify** interface command.

auto qos classify

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Usage Guidelines

This command generates a QoS configuration for untrusted interfaces. It places a service-policy to classify the traffic coming from untrusted desktops or devices and marks them accordingly. The service-policies generated do not police.

Global Level Commands Generated

The global templates are defined in A, B, C.

A. Template for ACLs and application classes used by the **auto qos classify** command.

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
      permit udp any any range 16384 32767
    ip access-list extended AutoQos-4.0-ACL-Signaling
      permit tcp any any range 2000 2002
      permit tcp any any range 5060 5061
            permit udp any any range 5060 5061
    ip access-list extended AutoQos-4.0-ACL-Transactional-Data
      permit tcp any any eq 443
      permit tcp any any eq 1521
      permit udp any any eq 1521
      permit tcp any any eq 1526
      permit udp any any eq 1526
      permit tcp any any eq 1575
      permit udp any any eq 1575
      permit tcp any any eq 1630
      permit udp any any eq 1630
    ip access-list extended AutoQos-4.0-ACL-Bulk-Data
      permit tcp any any eq ftp
      permit tcp any any eq ftp-data
      permit tcp any any eq 22
permit tcp any any eq smtp
      permit tcp any any eq 465
      permit tcp any any eq 143
      permit tcp any any eq 993
      permit tcp any any eq pop3
      permit tcp any any eq 995
      permit tcp any any eq 1914
    ip access-list extended AutoQos-4.0-ACL-Scavenger
      permit tcp any any eq 1214
      permit udp any any eq 1214
      permit tcp any any range 2300 2400
      permit udp any any range 2300 2400
```

```
   permit tcp any any eq 3689
   permit udp any any eq 3689
   permit tcp any any range 6881 6999
   permit tcp any any eq 11999
   permit tcp any any range 28800 29100
 ip access-list extended AutoQos-4.0-ACL-Default
   permit ip any any

class-map match-any AutoQos-4.0-VoIP-Data
        match dscp ef
        match cos 5
      class-map match-all AutoQos-4.0-VoIP-Data-Cos
        match cos 5
      class-map match-any AutoQos-4.0-VoIP-Signal
        match dscp cs3
        match cos 3
      class-map match-all AutoQos-4.0-VoIP-Signal-Cos
        match cos 3
class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
        match access-group name AutoQos-4.0-ACL-Multimedia-Conf
class-map match-all AutoQos-4.0-Signaling-Classify
  match access-group name AutoQos-4.0-ACL-Signaling
class-map match-all AutoQos-4.0-Transaction-Classify
  match access-group name AutoQos-4.0-ACL-Transactional-Data
class-map match-all AutoQos-4.0-Bulk-Data-Classify
  match access-group name AutoQos-4.0-ACL-Bulk-Data
class-map match-all AutoQos-4.0-Scavenger-Classify
  match access-group name AutoQos-4.0-ACL-Scavenger
      class-map match-all AutoQos-4.0-Default-Classify
  match access-group name AutoQos-4.0-ACL-Default
```

AutoQos-4.0-VoIP-Data-Cos and AutoQos-4.0-VoIP-Signal-Cos are needed to handle instances when you connect an IP phone to an interface and call the **auto qos voip cisco-phone** command on that interface. In this situation, the input service policy on the interface must match VoIP and signaling packets solely on their CoS markings. This is because switching ASICs on Cisco IP Phones are limited to only remarking the CoS bits of VoIP and the signaling traffic. Matching DSCP markings results in a security vulnerability because a user whose PC was connected to an IP phone connected to a switch would be able to remark DSCP markings of traffic arising from their PC to dscp ef using the NIC on their PC. This causes incorrect placement of non real-time traffic in the priority queue in the egress direction.

B. Template for the **auto qos classify** command input service-policy

```
policy-map AutoQos-4.0-Classify-Input-Policy
  class AutoQos-4.0-Multimedia-Conf-Classify
     set dscp af41
     set cos 4
     set qos-group 34
   class AutoQos-4.0-Signaling-Classify
     set dscp cs3
     set cos 3
     set qos-group 16
   class AutoQos-4.0-Transaction-Classify
     set dscp af21
     set cos 2
           set qos-group 18
   class AutoQos-4.0-Bulk-Data-Classify
     set dscp af11
     set cos 1
     set qos-group 10
   class AutoQos-4.0-Scavenger-Classify
     set dscp cs1
     set cos 1
     set qos-group 8
```

```
      class AutoQos-4.0-Default-Classify
        set dscp default
        set cos 0
```

C. Template for egress queue classes along with the SRND4 output policy that uses the egress classes to allocate 8 queues. This template is required by all SRND4 commands:

```
    class-map match-all AutoQos-4.0-Priority-Queue
      match qos-group 32
    class-map match-all AutoQos-4.0-Control-Mgmt-Queue
      match qos-group 16
    class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
      match qos-group 34
    class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
      match qos-group 26
    class-map match-all AutoQos-4.0-Trans-Data-Queue
      match qos-group 18
    class-map match-all AutoQos-4.0-Bulk-Data-Queue
            match qos-group 10
    class-map match-any AutoQos-4.0-Scavenger-Queue
      match qos-group 8
      match dscp cs1
```

Because **police** commands executed in policy map configuration mode do not allow the remarking of qos-groups for traffic flows that exceed defined rate limits, you must configure AutoQos-4.0-Scavenger-Queue to match either qos-group 7 or dscp af11. When you enter the **auto qos classify** police command, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos-group classification because qos-groups cannot be remarked as an exceed action. However, because AutoQos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, remarked packets fall into it, despite retaining their original qos-group labels.

```
       policy-map AutoQos-4.0-Output-Policye
      bandwidth remaining percent 1
   class AutoQos-4.0-Priority-Queue
      priority
      police cir percent 30 bc 33 ms
               conform-action transmit exceed-action drop
   class AutoQos-4.0-Control-Mgmt-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Conf-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Stream-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Trans-Data-Queue
      bandwidth remaining percent 10
      dbl
   class AutoQos-4.0-Bulk-Data-Queue
      bandwidth remaining percent 4
      dbl
   class class-default
      bandwidth remaining percent 25
            dbl
```

Interface Level Commands Generated

For Fa/Gig Ports:

```
Switch(config-if)# service-policy input AutoQos-4.0-Classify-Input-Policy
                  service-policy output AutoQos-4.0-Output-Policy
```

Examples

This example shows how to generate a QoS configuration for the untrusted interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos classify
```

Related Commands

Command	Description
auto qos trust	Generate QoS configurations for trusted interfaces.
auto qos voip cisco-softphone	Generate QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and marks police traffic coming from such interfaces.

auto qos classify police

To police traffic form an untrusted interface, use the **auto qos classify police** interface command.

auto qos classify police

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Usage Guidelines

This command generates a QoS configuration for untrusted interfaces. It places a service-policy to classify the traffic arriving from these untrusted desktops or devices and marks them accordingly. The generated service-policies police and either mark-down or drop packets.

Global Level Commands Generated

Auto QoS srn4 commands, once applied to an interface, generate one or more of the following templates (A, B, and C) at the global configuration level. Typically, a command generates a series of class-maps that either match on ACLs or on DSCP or CoS values to differentiate traffic into application classes. An input policy is generated that matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is merely a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress-queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each one of these eight egress-queue class-maps.

The commands generate the following templates as needed. For example, on initial use of the a new command, global configurations that define the eight queue egress service-policy are generated (template C, below). Subsequently, **auto qos** commands applied to other interfaces do not generate templates for egress queuing because all **auto qos** commands rely on the same eight queue model after migration, and they will have already been generated from the first use of the command.

The global templates are defined in A, B, C.

A. Template for ACLs and application classes used by the **auto qos classify police** command

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
  permit udp any any range 16384 32767
ip access-list extended AutoQos-4.0-ACL-Signaling
  permit tcp any any range 2000 2002
  permit tcp any any range 5060 5061
        permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-ACL-Transactional-Data
  permit tcp any any eq 443
  permit tcp any any eq 1521
  permit tcp any any eq 1521
  permit udp any any eq 1521
  permit tcp any any eq 1526
  permit udp any any eq 1526
  permit tcp any any eq 1575
  permit udp any any eq 1575
```

```
      permit tcp any any eq 1630
      permit udp any any eq 1630
    ip access-list extended AutoQos-4.0-ACL-Bulk-Data
      permit tcp any any eq ftp
      permit tcp any any eq ftp-data
      permit tcp any any eq 22
permit tcp any any eq smtp
      permit tcp any any eq 465
      permit tcp any any eq 143
      permit tcp any any eq 993
      permit tcp any any eq pop3
      permit tcp any any eq 995
      permit tcp any any eq 1914
    ip access-list extended AutoQos-4.0-ACL-Scavenger
      permit tcp any any eq 1214
      permit udp any any eq 1214
      permit tcp any any range 2300 2400
      permit udp any any range 2300 2400
      permit tcp any any eq 3689
      permit udp any any eq 3689
      permit tcp any any range 6881 6999
      permit tcp any any eq 11999
      permit tcp any any range 28800 29100
    ip access-list extended AutoQos-4.0-ACL-Default
      permit ip any any

   class-map match-any AutoQos-4.0-VoIP-Data
           match dscp ef
           match cos 5
         class-map match-all AutoQos-4.0-VoIP-Data-Cos
           match cos 5
         class-map match-any AutoQos-4.0-VoIP-Signal
           match dscp cs3
           match cos 3
         class-map match-all AutoQos-4.0-VoIP-Signal-Cos
           match cos 3
   class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
           match access-group name AutoQos-4.0-ACL-Multimedia-Conf
   class-map match-all AutoQos-4.0-Signaling-Classify
     match access-group name AutoQos-4.0-ACL-Signaling
   class-map match-all AutoQos-4.0-Transaction-Classify
     match access-group name AutoQos-4.0-ACL-Transactional-Data
   class-map match-all AutoQos-4.0-Bulk-Data-Classify
     match access-group name AutoQos-4.0-ACL-Bulk-Data
   class-map match-all AutoQos-4.0-Scavenger-Classify
     match access-group name AutoQos-4.0-ACL-Scavenger
         class-map match-all AutoQos-4.0-Default-Classify
     match access-group name AutoQos-4.0-ACL-Default
```

AutoQos-4.0-VoIP-Data-Cos and AutoQos-4.0-VoIP-Signal-Cos are needed to handle the case in which a user connects an IP phone to an interface and calls the **auto qos voip cisco-phone** command on that interface. In this situation, the input service policy on the interface must match VoIP and signaling packets solely on their CoS markings because switching ASICs on Cisco IP phones are limited to only remarking the CoS bits of VoIP and signaling traffic. Matching DSCP markings would cause a security vulnerability because user whose PC was connected to an IP phone connected to a switch would be able to re-mark DSCP markings of traffic arising from their PC to dscp ef using the NIC on their PC. This places non real-time traffic in the priority queue in the egress direction.

B. Template for the input service-policy of the **auto qos classify police** command

```
    policy-map AutoQos-4.0-Classify-Police-Input-Policy
      class AutoQos-4.0-Multimedia-Conf-Classify
        set dscp af41
    set cos 4
    set qos-group 34
    police cir 5000000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Signaling-Classify
    set dscp cs3
    set cos 3
    set qos-group 16
    police cir 32000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Transaction-Classify
    set dscp af21
    set cos 2
    set qos-group 18
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
  class AutoQos-4.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 10
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
         exceed-action set-cos-transmit 1
  class AutoQos-4.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 8
    police cir 10000000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Default-Classify
    set dscp default
    set cos 0
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
```

C. Template for egress queue classes along with the SRND4 output policy that uses the egress classes to allocate eight queues. This template is required by the four SRND4 commands:

```
class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
        match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

AutoQos-4.0-Scavenger-Queue must be configured to match either qos-group 7 or dscp af11 to accomodate for the fact that police commands executed in policy map configuration mode do not allow the remarking of qos-groups for traffic flows that exceed defined rate limits. After entering the **auto qos classify police** command, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos-group classification because qos-groups cannot be remarked as an exceed action. However, because AutoQos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, remarked packets fall into it, despite retaining their original qos-group labels.

```
       policy-map AutoQos-4.0-Output-Policye
      bandwidth remaining percent 1
   class AutoQos-4.0-Priority-Queue
      priority
      police cir percent 30 bc 33 ms
               conform-action transmit exceed-action drop
   class AutoQos-4.0-Control-Mgmt-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Conf-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Stream-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Trans-Data-Queue
      bandwidth remaining percent 10
      dbl
   class AutoQos-4.0-Bulk-Data-Queue
      bandwidth remaining percent 4
      dbl
   class class-default
      bandwidth remaining percent 25
            dbl
```

Interface Level Commands Generated

For Fa/Gig Ports:

```
Switch(config-if)#
                service-policy input AutoQos-4.0-Classify-Police-Input-Policy
                service-policy output AutoQos-4.0-Output-Policy
```

Examples

This example shows how to police traffic from an untrusted interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos classify police
Switch(config-if)# do sh run interface gigabitethernet1
Interface gigabitethernet1
   auto qos classify police
    service-policy input AutoQos-4.0-Classify-Police-Input-Policy
    service-policy output AutoQos-4.0-Output-Policy
end
```

Related Commands

Command	Description
auto qos voip cisco-softphone	Generates QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and mark police traffic coming from such interfaces.
auto qos classify	Generates a QoS configuration for an untrusted interface.
auto qos srnd4	Generates QoS configurations based on solution reference network design 4.0.

auto qos srnd4

To generate QoS configurations based on solution reference network design 4.0, use the **auto qos srnd4** global command.

auto qos srnd4

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global configuration

Usage Guidelines

This command is generated when any new auto-QoS command is configured on an interface.

AutoQos SRND4 commands, when applied to an interface, generate one or more of the following templates (A and B) at the global configuration level.

Typcally, a command generates a series of class-maps that either match on ACLs or on DSCP and CoS values to differentiate traffic into application classes. An input policy is also generated, which matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is a numerical tag that allows different application classes to be treated as one unit. It has no significance outside the context of the switch in which it was set.) Furthermore, eight egress-queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of the eight egress-queue class-maps.

AutoQos srnd4 commands only generate a templates as needed. For example, the first time you use a new srnd4 command, global configurations that define the eight queue egress service-policy are generated (template B below). Subsequently, **auto qos** commands applied to other interfaces do not generate templates for egress queuing because all auto-QoS commands rely on the same eight queue models after migration, and they will have already been generated from the first use of the command.

For interfaces with auto qos voip trust enabled

—Global Level Commands Generated

The global templates are defined in A and B (below).

A. This template of application classes is used by the auto-QoS video cts, **auto qos video ip-camera**, and **auto qos trust** commands. This template class also includes the input service-policy for the **auto qos video cts**, **auto qos video ip-camera**, and **auto qos trust** commands. Because these three commands are the only ones that use AutoQos-4.0-Input-Policy, it makes sense to include that policy in the same template that defines the application classes used by the previous three commands.

```
class-map match-any AutoQos-4.0-VoIP
  match dscp ef
  match cos 5
class-map match-all AutoQos-4.0-Broadcast-Vid
  match dscp cs5
class-map match-all AutoQos-4.0-Realtime-Interact
  match dscp cs4
class-map match-all AutoQos-4.0-Network-Ctrl
  match dscp cs7
```

```
    class-map match-all AutoQos-4.0-Internetwork-Ctrl
      match dscp cs6
    class-map match-any AutoQos-4.0-Signaling
      match dscp cs3
      match cos 3
    class-map match-all AutoQos-4.0-Network-Mgmt
      match dscp cs2
    class-map match-any AutoQos-4.0-Multimedia-Conf
      match dscp af41
      match dscp af42
      match dscp af43
   class-map match-any AutoQos-4.0-Multimedia-Stream
      match dscp af31
      match dscp af32
      match dscp af33
    class-map match-any AutoQos-4.0-Transaction-Data
      match dscp af21
      match dscp af22
      match dscp af23
    class-map match-any AutoQos-4.0-Bulk-Data
      match dscp af11
      match dscp af12
      match dscp af13
    class-map match-all AutoQos-4.0-Scavenger
      match dscp cs1
```

The AutoQos-4.0-Signaling and AutoQos-4.0-VoIP classes must match on CoS to handle the situation when an IP phone is connected to an interface. (Cisco IP phones are only capable of re-marking CoS bits, not DSCP.)

```
policy-map AutoQos-4.0-Input-Policy
      class AutoQos-4.0-VoIP
        set qos-group 32
      class AutoQos-4.0-Broadcast-Vid
        set qos-group 32
      class AutoQos-4.0-Realtime-Interact
        set qos-group 32
      class AutoQos-4.0-Network-Ctrl
        set qos-group 16
      class AutoQos-4.0-Internetwork-Ctrl
        set qos-group 16
      class AutoQos-4.0-Signaling
        set qos-group 16
      class AutoQos-4.0-Network-Mgmt
        set qos-group 16
      class AutoQos-4.0-Multimedia-Conf
        set qos-group 34
      class AutoQos-4.0-Multimedia-Stream
        set qos-group 26
      class AutoQos-4.0-Transaction-Data
        set qos-group 18
      class AutoQos-4.0-Bulk-Data
        set qos-group 10
      class AutoQos-4.0-Scavenger
        set qos-group 8
```

B. This template for egress queue classes (along with the SRND4 output policy) allocates eight queues. This template is required by all SRND4 commands:

```
    class-map match-all AutoQos-4.0-Priority-Queue
      match qos-group 32
    class-map match-all AutoQos-4.0-Control-Mgmt-Queue
      match qos-group 16
    class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
    match qos-group 34
  class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
    match qos-group 26
  class-map match-all AutoQos-4.0-Trans-Data-Queue
    match qos-group 18
  class-map match-all AutoQos-4.0-Bulk-Data-Queue
          match qos-group 10
  class-map match-any AutoQos-4.0-Scavenger-Queue
    match qos-group 8
    match dscp cs1
```

Because the **police** commands executed in policy map configuration mode do not allow the re-marking of qos-groups for traffic flows that exceed defined rate limits, you should configure AutoQos-4.0-Scavenger-Queue to match either qos-group 7 or dscp af11. When you enter the **auto qos classify police** command, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos-group classificatio because such groups cannot be re-marked as an exceed action. However, because AutoQos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, re-marked packets fall into it, despite retaining their original qos-group labels.

```
     policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Scavenger-Queue
    bandwidth remaining percent 1
 class AutoQos-4.0-Priority-Queue
    priority
    police cir percent 30 bc 33 ms
             conform-action transmit exceed-action drop
 class AutoQos-4.0-Control-Mgmt-Queue
    bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Conf-Queue
    bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Stream-Queue
    bandwidth remaining percent 10
 class AutoQos-4.0-Trans-Data-Queue
    bandwidth remaining percent 10
    dbl
 class AutoQos-4.0-Bulk-Data-Queue
    bandwidth remaining percent 4
    dbl
 class class-default
    bandwidth remaining percent 25
          dbl
```

—Interface Level Commands Generated

For Fa/Gig Ports:

If Layer 2 interface:

```
Switch(config-if)# no service-policy input AutoQos-VoIP-Input-Cos-Policy
                  no service-policy output AutoQos-VoIP-Output-Policy
                  service-policy input AutoQos-4.0-Input-Policy
                  service-policy output AutoQos-4.0-Output-Policy
```

If Layer 3 interface:

```
Switch(config-if)# no service-policy input AutoQos-VoIP-Input-Dscp-Policy
                  no service-policy output AutoQos-VoIP-Output-Policy
                  service-policy input AutoQos-4.0-Input-Policy
                  service-policy output AutoQos-4.0-Output-Policy
```

For interfaces with auto qos voip cisco-phone enabled

—Global Level Commands Generated

The global templates defined in A and B (above).

—Interface Level Commands Generated

For Fa/Gig Ports:

```
Switch(config-if)# no qos trust device cisco-phone
                   no service-policy input AutoQos-VoIP-Input-Cos-Policy
                   no service-policy output AutoQos-VoIP-Output-Policy
                   qos trust device cisco-phone
                   service-policy input AutoQos-4.0-Cisco-Phone-Input-Policy
                   service-policy output AutoQos-4.0-Output-Policy
```

Examples

To generate QoS configurations based on solution reference network design 4.0, do the following:

```
Switch# auto qos srnd4
```

Related Commands

Command	Description
auto qos trust	Generate QoS configurations for trusted interfaces.
auto qos voip cisco-softphone	Generate QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and marks police traffic coming from such interfaces.

auto qos trust

To generate QoS configurations for trusted interfaces, use the **auto qos trust** interface command.

auto qos trust

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Usage Guidelines

Global Level Commands Generated

After you apply auto-QoS srnd4 commands to an interface, they generate one or more of the following templates (A and B) at the global configuration level. Typically, a command generates a series of class-maps that either match on ACLs or on DSCP or CoS values to differentiate traffic into application classes. An input policy is generated, which matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is simply a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Additionally, eight egress-queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of these eight class-maps.

The command only generates templates as needed. For example, on first use of a new command, global configurations that define the eight queue egress service-policy are generated. Subsequently, auto-QoS commands applied to other interfaces do not generate templates for egress queuing. This is because all auto-qos commands rely on the same eight queue models after migration, and they will have already been generated from the first use of the command.

The global templates defined in A and B.

A. Template of application classes used by the **auto qos trust** command

This template also includes the input service-policy for the **auto qos video cts**, **auto qos video ip-camera**, and **auto qos trust** commands. Because these three commands are the only ones that use the AutoQos-4.0-Input-Policy, you should include that policy in the template that defines the application classes used by the commands.

```
class-map match-any AutoQos-4.0-VoIP
  match dscp ef
  match cos 5
class-map match-all AutoQos-4.0-Broadcast-Vid
  match dscp cs5
class-map match-all AutoQos-4.0-Realtime-Interact
  match dscp cs4
class-map match-all AutoQos-4.0-Network-Ctrl
  match dscp cs7
class-map match-all AutoQos-4.0-Internetwork-Ctrl
  match dscp cs6
class-map match-any AutoQos-4.0-Signaling
  match dscp cs3
  match cos 3
class-map match-all AutoQos-4.0-Network-Mgmt
```

```
      match dscp cs2
    class-map match-any AutoQos-4.0-Multimedia-Conf
      match dscp af41
      match dscp af42
      match dscp af43
   class-map match-any AutoQos-4.0-Multimedia-Stream
      match dscp af31
      match dscp af32
      match dscp af33
    class-map match-any AutoQos-4.0-Transaction-Data
      match dscp af21
      match dscp af22
      match dscp af23
    class-map match-any AutoQos-4.0-Bulk-Data
      match dscp af11
      match dscp af12
      match dscp af13
    class-map match-all AutoQos-4.0-Scavenger
      match dscp cs1
```

The AutoQos-4.0-Signaling and AutoQos-4.0-VoIP classes must also match on CoS to handle the case when an IP phone is connected to an interface. (Cisco IP phones are only capable of remarking CoS bits, not DSCP.)

```
policy-map AutoQos-4.0-Input-Policy
      class AutoQos-4.0-VoIP
        set qos-group 32
      class AutoQos-4.0-Broadcast-Vid
        set qos-group 32
      class AutoQos-4.0-Realtime-Interact
        set qos-group 32
      class AutoQos-4.0-Network-Ctrl
        set qos-group 16
      class AutoQos-4.0-Internetwork-Ctrl
        set qos-group 16
      class AutoQos-4.0-Signaling
        set qos-group 16
      class AutoQos-4.0-Network-Mgmt
        set qos-group 16
      class AutoQos-4.0-Multimedia-Conf
        set qos-group 34
      class AutoQos-4.0-Multimedia-Stream
        set qos-group 26
      class AutoQos-4.0-Transaction-Data
        set qos-group 18
      class AutoQos-4.0-Bulk-Data
        set qos-group 10
      class AutoQos-4.0-Scavenger
        set qos-group 8
```

B. Templates for egress queue classes and the srnd4 output policy that uses the egress classes to allocate eight queues. This template is required by all srnd4 commands.

```
    class-map match-all AutoQos-4.0-Priority-Queue
      match qos-group 32
    class-map match-all AutoQos-4.0-Control-Mgmt-Queue
      match qos-group 16
    class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
      match qos-group 34
    class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
      match qos-group 26
    class-map match-all AutoQos-4.0-Trans-Data-Queue
      match qos-group 18
    class-map match-all AutoQos-4.0-Bulk-Data-Queue
```

```
        match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

Because **police** commands executed in policy map configuration mode do not allow the remarking of qos-groups for traffic flows that exceed defined rate limits, AutoQos-4.0-Scavenger-Queue must be configured to match either qos-group 7 or dscp af11. When the **auto qos classify police** command executes, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos-group classification. This is because qos-groups cannot be remarked as an exceed action. However, because AutoQos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, remarked packets will fall into it, despite retaining their original qos-group labels.

```
    policy-map AutoQos-4.0-Output-Policy
class AutoQos-4.0-Scavenger-Queue
   bandwidth remaining percent 1
class AutoQos-4.0-Priority-Queue
   priority
   police cir percent 30 bc 33 ms
            conform-action transmit exceed-action drop
class AutoQos-4.0-Control-Mgmt-Queue
   bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Conf-Queue
   bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Stream-Queue
   bandwidth remaining percent 10
class AutoQos-4.0-Trans-Data-Queue
   bandwidth remaining percent 10
   dbl
class AutoQos-4.0-Bulk-Data-Queue
   bandwidth remaining percent 4
   dbl
class class-default
   bandwidth remaining percent 25
```

Interface Level Commands Generated

For Fa/Gig Ports:

```
Switch(config-if)# service-policy input AutoQos-4.0-Input-Policy
                  service-policy output AutoQos-4.0-Output-Policy
```

Examples

This example shows how to police traffic from an untrusted interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos trust
Switch(config-if)# do sh running interface interface-id
interface FastEthernet2/1
 auto qos trust
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

Related Commands

Command	Description
auto qos voip cisco-softphone	Generates QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and mark police traffic coming from such interfaces.

Command	Description
auto qos classify	Generates a QoS configuration for an untrusted interface.
auto qos srnd4	Generates QoS configurations based on solution reference network design 4.0.

auto qos video

To generate QOS configuration for cisco-telepresence or cisco-camera interfaces (conditional trust through CDP), use the **auto qos video** interface configuration command.

auto qos video {**cts** | **ip-camera**}

Syntax Description

cts	Trust the QoS marking of Cisco Telepresence device.
ip-camera	Trust the QoS marking of Cisco video surveillance camera.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Usage Guidelines

The **auto qos video** command trusts an interface only if Cisco TelePresence is detected. Else, the port is untrusted.

Global Level Commands Generated

When auto-Qos srnd4 commands are applied to an interface, they generate one or more of the following templates at the global configuration level. Typically, a command generates a series of class-maps that either match on ACLs or on DSCP (or CoS) values to differentiate traffic into application classes. An input policy is also generated, which matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is simply a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress-queue class-maps are generated, which match the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of the eight egress-queue class-maps.

The srnd4 commsands generate the templates only as needed. For example, on first use of the new command, global configurations that define the eight queue egress service-policy are generated. Subsequently, auto-QoS commands applied to other interfaces do not generate templates for egress queuing. This is because all auto-QoS commnds rely on the same eight queue model after migration, already generated on first use of the command.

The global templates defined in A and B.

A. Template of application classes used by the **auto qos video** command

This template also includes the input service-policy for the **auto qos video cts**, **auto qos video ip-camera**, and **auto qos trust** commands. Because these three commands are the only ones that use the AutoQos-4.0-Input-Policy, we advise that you include that policy in the same template that defines the application classes used by the commands.

```
class-map match-any AutoQos-4.0-VoIP
  match dscp ef
  match cos 5
class-map match-all AutoQos-4.0-Broadcast-Vid
  match dscp cs5
class-map match-all AutoQos-4.0-Realtime-Interact
  match dscp cs4
```

```
    class-map match-all AutoQos-4.0-Network-Ctrl
      match dscp cs7
    class-map match-all AutoQos-4.0-Internetwork-Ctrl
      match dscp cs6
    class-map match-any AutoQos-4.0-Signaling
      match dscp cs3
      match cos 3
    class-map match-all AutoQos-4.0-Network-Mgmt
      match dscp cs2
    class-map match-any AutoQos-4.0-Multimedia-Conf
      match dscp af41
      match dscp af42
      match dscp af43
   class-map match-any AutoQos-4.0-Multimedia-Stream
      match dscp af31
      match dscp af32
      match dscp af33
    class-map match-any AutoQos-4.0-Transaction-Data
      match dscp af21
      match dscp af22
      match dscp af23
    class-map match-any AutoQos-4.0-Bulk-Data
      match dscp af11
      match dscp af12
      match dscp af13
    class-map match-all AutoQos-4.0-Scavenger
      match dscp cs1
```

The AutoQos-4.0-Signaling and AutoQos-4.0-VoIP classes must also match on CoS to the case where an IP phone is connected to an interface. (Cisco IP phones are only capable of remarking CoS bits, not DSCP.)

```
policy-map AutoQos-4.0-Input-Policy
      class AutoQos-4.0-VoIP
        set qos-group 32
      class AutoQos-4.0-Broadcast-Vid
        set qos-group 32
      class AutoQos-4.0-Realtime-Interact
        set qos-group 32
      class AutoQos-4.0-Network-Ctrl
        set qos-group 16
      class AutoQos-4.0-Internetwork-Ctrl
        set qos-group 16
      class AutoQos-4.0-Signaling
        set qos-group 16
      class AutoQos-4.0-Network-Mgmt
        set qos-group 16
      class AutoQos-4.0-Multimedia-Conf
        set qos-group 34
      class AutoQos-4.0-Multimedia-Stream
        set qos-group 26
      class AutoQos-4.0-Transaction-Data
        set qos-group 18
      class AutoQos-4.0-Bulk-Data
        set qos-group 10
      class AutoQos-4.0-Scavenger
        set qos-group 8
```

B. Template for egress queue classes and the srnd4 output policy that uses the egress classes to allocate eight queues. This template is required by all srnd commands:

```
    class-map match-all AutoQos-4.0-Priority-Queue
      match qos-group 32
    class-map match-all AutoQos-4.0-Control-Mgmt-Queue
```

```
      match qos-group 16
    class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
      match qos-group 34
    class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
      match qos-group 26
    class-map match-all AutoQos-4.0-Trans-Data-Queue
      match qos-group 18
    class-map match-all AutoQos-4.0-Bulk-Data-Queue
            match qos-group 10
    class-map match-any AutoQos-4.0-Scavenger-Queue
      match qos-group 8
      match dscp cs1
```

Because **police** commands executed in policy map configuration mode do not allow the remarking of qos-groups for traffic flows that exceed defined rate limits, AutoQos-4.0-Scavenger-Queue must be configured to match either qos-group 7 or dscp af11. When the **auto qos classify police** command has been executed, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos-group classification because qos-groups cannot be remarked as an exceed action. However, because AutoQos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, remarked packets will fall into it, despite retaining their original qos-group labels.

```
       policy-map AutoQos-4.0-Output-Policy
   class AutoQos-4.0-Scavenger-Queue
      bandwidth remaining percent 1
   class AutoQos-4.0-Priority-Queue
      priority
      police cir percent 30 bc 33 ms
               conform-action transmit exceed-action drop
   class AutoQos-4.0-Control-Mgmt-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Conf-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Stream-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Trans-Data-Queue
      bandwidth remaining percent 10
      dbl
   class AutoQos-4.0-Bulk-Data-Queue
      bandwidth remaining percent 4
      dbl
   class class-default
      bandwidth remaining percent 25
```

Interface Level Commands Generated

For Fa/Gig Ports:

```
Switch(config-if)# service-policy input AutoQos-4.0-Input-Policy
                   service-policy output AutoQos-4.0-Output-Policy
```

Examples

This example shows how to generate a QoS configuration on the cisco-telepresence interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos video cts
Switch(config-if)# do sh running interface gigabitethernet1/1
interface interface-id
 auto qos video cts
 qos trust device cts
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

```
end
```

This example shows how to generate QoS configuration for the cisco-camera interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos video ip-camera
Switch(config-if)# do sh running interface interface-id
interface interface-id
 auto qos video ip-camera
 qos trust device ip-camera
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

Related Commands

Command	Description
auto qos trust	Generates QoS configurations for trusted interfaces.
auto qos srnd4	Generates QoS configurations based on solution reference network design 4.0.

auto qos voip

To automatically configure quality of service (auto-QoS) for voice over IP (VoIP) within a QoS domain, use the **auto qos voip** interface configuration command. To change the auto-QoS configuration settings to the standard QoS defaults, use the **no** form of this command.

auto qos voip {**cisco-phone** | **trust**}

no auto qos voip {**cisco-phone** | **trust**}

Syntax Description

cisco-phone	Generates a QoS configuration for Cisco IP phone interfaces (conditional trust through CDP). The CoS labels of incoming packets are trusted only when a telephone is detected.
trust	Connects the interface to a trusted switch or router and automatically configures QoS for VoIP. The CoS and DSCP labels of incoming packets are trusted.

Defaults

Auto-QoS is disabled on all interfaces

Command Modes

Interface configuration mode

Usage Guidelines

Use this command to configure a QoS that is appropriate for VoIP traffic within the QoS domain, which includes the switch, the interior of the network, and the edge devices that can classify incoming traffic for QoS.

Apply the **cisco-phone** keyword on those ports (at the edge of the network) that are connected to Cisco IP phones. The switch detects the telephone through Cisco Discovery Protocol (CDP) and trusts those CoS labels in packets that are received from the telephone.

Apply the **trust** keyword on those ports that are connected to the interior of the network. Assume that the traffic has already been classified by the other edge devices. So, the CoS/DSCP labels in these packets are trusted.

When you enable the auto-QoS feature on the specified interface, these actions automatically occur:

- QoS is globally enabled (**qos** global configuration command).
- DBL is enabled globally (**qos dbl** global configuration command).
- When you enter the **auto qos voip cisco-phone** interface configuration command, the trusted boundary feature is enabled. It uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP phone. When a Cisco IP phone is detected, the ingress classification on the specific interface is set to trust the CoS label that is received in the packet because some older phones do not mark DSCP. When a Cisco IP phone is absent, the ingress classification is set to not trust the CoS label in the packet.
- When you enter the **auto qos voip trust** interface configuration command, the ingress classification on the specified interface is set to trust the CoS label that is received in the packet provided the specified interface is configured as Layer 2 (and is set to trust DSCP if the interface is configured as Layer 3).

You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging (before you enable auto-QoS) with the **debug auto qos** privileged EXEC command.

To disable auto-QoS on an interface, use the **no auto qos voip** interface configuration command. When you enter this command, the switch enables standard QoS and changes the auto-QoS settings to the standard QoS default settings for that interface. This action will not change any global configuration performed by auto-QoS; the global configuration remains the same.

Examples

This example shows how to enable auto-QoS and to trust the CoS and DSCP labels that are received in the incoming packets when the switch or router that is connected to Gigabit Ethernet interface 1/1 is a trusted device:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
```

This example shows how to enable auto-QoS and to trust the CoS labels that are received in incoming packets when the device connected to Fast Ethernet interface 2/1 is detected as a Cisco IP phone:

```
Switch(config)# interface fastethernet2/1
Switch(config-if)# auto qos voip cisco-phone
```

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled on an interface:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitethernet3/10
Switch(config-if)#auto qos voip trust
Switch(config-if)#
1d03h:  service-policy input AutoQos-VoIP-Input-Cos-Policy
1d03h:  service-policy output AutoQos-VoIP-Output-Policy
Switch(config-if)#intface gigabitethernet3/11
Switch(config-if)#auto qos voip
cisco-phone
Switch(config-if)#
1d03h:  qos trust device cisco-phone
1d03h:  service-policy input AutoQos-VoIP-Input-Cos-Policy
1d03h:  service-policy output AutoQos-VoIP-Output-Policy
Switch(config-if)#end
Switch#
```

You can verify your settings by entering the **show auto qos interface** command.

Related Commands

Command	Description
debug auto qos (refer to Cisco IOS documentation)	Debugs Auto QoS.
qos trust	Sets the trusted state of an interface.
show auto qos	Displays the automatic quality of service (auto-QoS) configuration that is applied.
show qos	Displays QoS information.
show qos interface	Displays queueing information.
show qos maps	Displays QoS map information.

auto qos voip cisco-softphone

To generate QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and mark police traffic coming from such interfaces, use the **auto qos voip** interface configuration command.

auto qos voip cisco-softphone

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Usage Guidelines

Ports configured with **auto qos voip** command are considered untrusted.

Global Level Commands Generated

After auto-QoS srnd4 commands are applied to an interface, they generate one or more of the following templates (A, B, and C) at the global configuration level. Typically, a command generates a series of class-maps that either match on ACLs or on DSCP (or CoS) values to differentiate traffic into application classes. An input policy is also generated, whch matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress-queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of these eight class-maps.

The commands generate templates only as needed. For example, on first use of a new commnand, global configurations that define the eight queue egress service-policy are generated. Subsequently, auto-QoS applied to other interfaces do not generate templates for egress queuing. This is because all auto-QoS commands rely on the same eight queue models after migration, already been generated from the first use of the new command.

The global template is defined by A, B, and C.

A. Template for ACLs and application classes used by the **auto qos voip cisco-softphone** command

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
      permit udp any any range 16384 32767
    ip access-list extended AutoQos-4.0-ACL-Signaling
      permit tcp any any range 2000 2002
      permit tcp any any range 5060 5061
            permit udp any any range 5060 5061
    ip access-list extended AutoQos-4.0-ACL-Transactional-Data
      permit tcp any any eq 443
      permit tcp any any eq 1521
      permit udp any any eq 1521
      permit tcp any any eq 1526
      permit udp any any eq 1526
      permit tcp any any eq 1575
      permit udp any any eq 1575
      permit tcp any any eq 1630
      permit udp any any eq 1630
```

```
 ip access-list extended AutoQos-4.0-ACL-Bulk-Data
   permit tcp any any eq ftp
   permit tcp any any eq ftp-data
   permit tcp any any eq 22
   permit tcp any any eq smtp
   permit tcp any any eq 465
   permit tcp any any eq 143
   permit tcp any any eq 993
   permit tcp any any eq pop3
   permit tcp any any eq 995
   permit tcp any any eq 1914
 ip access-list extended AutoQos-4.0-ACL-Scavenger
   permit tcp any any eq 1214
   permit udp any any eq 1214
   permit tcp any any range 2300 2400
   permit udp any any range 2300 2400
   permit tcp any any eq 3689
   permit udp any any eq 3689
   permit tcp any any range 6881 6999
   permit tcp any any eq 11999
   permit tcp any any range 28800 29100
 ip access-list extended AutoQos-4.0-ACL-Default
   permit ip any any

class-map match-any AutoQos-4.0-VoIP-Data
        match dscp ef
        match cos 5
      class-map match-all AutoQos-4.0-VoIP-Data-Cos
        match cos 5
      class-map match-any AutoQos-4.0-VoIP-Signal
        match dscp cs3
        match cos 3
      class-map match-all AutoQos-4.0-VoIP-Signal-Cos
        match cos 3
class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
        match access-group name AutoQos-4.0-ACL-Multimedia-Conf
class-map match-all AutoQos-4.0-Signaling-Classify
  match access-group name AutoQos-4.0-ACL-Signaling
class-map match-all AutoQos-4.0-Transaction-Classify
  match access-group name AutoQos-4.0-ACL-Transactional-Data
class-map match-all AutoQos-4.0-Bulk-Data-Classify
  match access-group name AutoQos-4.0-ACL-Bulk-Data
class-map match-all AutoQos-4.0-Scavenger-Classify
  match access-group name AutoQos-4.0-ACL-Scavenger
      class-map match-all AutoQos-4.0-Default-Classify
  match access-group name AutoQos-4.0-ACL-Default
```

AutoQos-4.0-VoIP-Data-Cos and AutoQos-4.0-VoIP-Signal-Cos handles those instances when a user connects an IP phone to an interface and enters the **auto qos voip cisco-phone** command on that interface. In this situation, the input service policy on the interface must match VoIP and signaling packets based solely on their CoS markings because switching ASICs on Cisco IP Phones are limited to only remarking the CoS bits of VoIP and signaling traffic. Matching DSCP markings would result in a security vulnerability because a user whose PC was connected to an IP phone connected to a switch would be able to remark DSCP markings of traffic arriving from their PC to DSCP ef using the NIC on their PC. This results in incorrectly placing non real-time traffic in the priority queue in the egress direction.

B. Template for the **auto qos voip cisco-softphone** command input service-policy

```
    policy-map AutoQos-4.0-Cisco-Softphone-Input-Policy
class AutoQos-4.0-VoIP-Data
  set dscp ef
  set cos 5
```

```
   set qos-group 32
   police cir 128000 bc 8000
   exceed-action set-dscp-transmit cs1
   exceed-action set-cos-transmit 1
       class AutoQos-4.0-VoIP-Signal
   set dscp cs3
   set cos 3
   set qos-group 16
   police cir 32000 bc 8000
   exceed-action set-dscp-transmit cs1
         exceed-action set-cos-transmit 1
class AutoQos-4.0-Multimedia-Conf-Classify
   set dscp af41
   set cos 4
   set qos-group 34
   police cir 5000000 bc 8000
   exceed-action drop
 class AutoQos-4.0-Signaling-Classify
   set dscp cs3
   set cos 3
   set qos-group 16
   police cir 32000 bc 8000
   exceed-action drop
 class AutoQos-4.0-Transaction-Classify
   set dscp af21
   set cos 2
   set qos-group 18
   police cir 10000000 bc 8000
   exceed-action set-dscp-transmit cs1
   exceed-action set-cos-transmit 1
 class AutoQos-4.0-Bulk-Data-Classify
   set dscp af11
   set cos 1
   set qos-group 10
   police cir 10000000 bc 8000
   exceed-action set-dscp-transmit cs1
         exceed-action set-cos-transmit 1
 class AutoQos-4.0-Scavenger-Classify
   set dscp cs1
   set cos 1
   set qos-group 8
   police cir 10000000 bc 8000
   exceed-action drop
 class AutoQos-4.0-Default-Classify
   set dscp default
   set cos 0
```

C. Template for egress queue classes and the srnd4 output policy that uses the egress classes to allocate eight queues. This template is required by all srnd4 commands:

```
class-map match-all AutoQos-4.0-Priority-Queue
      match qos-group 32
    class-map match-all AutoQos-4.0-Control-Mgmt-Queue
      match qos-group 16
    class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
      match qos-group 34
    class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
      match qos-group 26
    class-map match-all AutoQos-4.0-Trans-Data-Queue
      match qos-group 18
    class-map match-all AutoQos-4.0-Bulk-Data-Queue
            match qos-group 10
    class-map match-any AutoQos-4.0-Scavenger-Queue
      match qos-group 8
      match dscp cs1
```

Because the **police** commands executed in policy map configuration mode do not allow remarking of qos-groups for traffic flows that exceed defined rate limits, AutoQos-4.0-Scavenger-Queue must be configured to match either qos-group 7 or dscp af11. When the **auto qos classify police** command has been executed, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos-group classification because qos-groups cannot be remarked as an exceed action. However, because AutoQos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, remarked packets will fall into it, despite retaining their original qos-group labels.

```
        policy-map AutoQos-4.0-Output-Policy
   class AutoQos-4.0-Scavenger-Queue
      bandwidth remaining percent 1
   class AutoQos-4.0-Priority-Queue
      priority
      police cir percent 30 bc 33 ms
               conform-action transmit exceed-action drop
   class AutoQos-4.0-Control-Mgmt-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Conf-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Stream-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Trans-Data-Queue
      bandwidth remaining percent 10
      dbl
   class AutoQos-4.0-Bulk-Data-Queue
      bandwidth remaining percent 4
      dbl
   class class-default
      bandwidth remaining percent 25
            dbl
```

Interface Level Commands Generated

For Fa/Gig Ports:

```
Switch(config-if)#
                service-policy input AutoQos-4.0-Cisco-Softphone-Input-Policy
                service-policy input AutoQos-4.0-Output-Policy
```

Examples

This example shows how to generate QoS configuration for interfaces Gigabit Ethernet 1/1 connected to a PC that is running the Cisco IP SoftPhone application:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-softphone
Switch(config-if)# do sh running interface gigabitethernet1/1
interface gigabitethernet1/1
 auto qos voip cisco-phone
 qos trust device cisco-phone
 service-policy input AutoQos-4.0-Cisco-Phone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

Related Commands

Command	Description
auto qos voip cisco-softphone	Generate QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and marks police traffic coming from such interfaces.
auto qos classify	Generate a QoS configuration for an untrusted interface.
auto qos classify police	Police traffic form an untrusted interface.

auto-sync

To enable automatic synchronization of the configuration files in NVRAM, use the **auto-sync** command. To disable automatic synchronization, use the **no** form of this command.

auto-sync {**startup-config** | **config-register** | **bootvar** | **standard**}

no auto-sync {**startup-config** | **config-register** | **bootvar** | **standard**}

Syntax Description

startup-config	Specifies automatic synchronization of the startup configuration.
config-register	Specifies automatic synchronization of the configuration register configuration.
bootvar	Specifies automatic synchronization of the BOOTVAR configuration.
standard	Specifies automatic synchronization of the startup configuration, BOOTVAR, and configuration registers.

Defaults

Standard automatic synchronization of all configuration files

Command Modes

Redundancy main-cpu mode

Usage Guidelines

If you enter the **no auto-sync standard** command, no automatic synchronizations occur.

Examples

This example shows how (from the default configuration) to enable automatic synchronization of the configuration register in the main CPU:

```
Switch# config terminal
Switch (config)# redundancy
Switch (config-r)# main-cpu
Switch (config-r-mc)# no auto-sync standard
Switch (config-r-mc)# auto-sync configure-register
Switch (config-r-mc)#
```

Related Commands

Command	Description
redundancy	Enters the redundancy configuration mode.

bandwidth

To specify or modify the minimum bandwidth provided to a class belonging to a policy map attached to a physical port, use the **bandwidth** policy-map class command. To return to the default setting, use the **no** form of this command.

bandwidth {*bandwidth-kbps* | **percent** *percent* | **remaining percent** *percent*}

no bandwidth

Syntax Description

bandwidth-kbps	Amount of bandwidth in kbps assigned to the class. The range is 32 to 16000000.
percent *percent*	Percentage of available bandwidth assigned to the parent class. The range is 1 to 100.
remaining percent *percent*	Percentage of remaining bandwidth assigned to parent class. The range is 1 to 100. This command is supported only when priority queuing class is configured, and the prioity queuing class is not rate-limited.

Defaults

No bandwidth is specified.

Command Modes

Policy-map class configuration mode

Usage Guidelines

Use the **bandwidth** command only in a policy map attached to a physical port.

The **bandwidth** command specifies the minimum bandwidth for traffic in that class when there is traffic congestion in the switch. If the switch is not congested, the class receives more bandwidth than you specify with this command.

When queuing class is configured without any explicit bandwidth configuration, since the queue is not guaranteed any minimum bandwidth, this queue will get a share of any unallocated bandwidth on the port.

If there is no unallocated bandwidth for the new queue or if the unallocated bandwidth is not sufficient to meet the minimum configurable rate for all queues which do not have any explicit bandwidth configuration, then the policy association is rejected.

These restrictions apply to the **bandwidth** command:

- If the **percent** keyword is used, the sum of the class bandwidth percentages within a single policy map cannot exceed 100 percent. Percentage calculations are based on the bandwidth available on the port.
- The amount of bandwidth configured should be large enough to accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in either kbps or in percentages, but not a mix of both.

Examples

This example shows how to set the minimum bandwidth to 2000 kbps for a class called *silver-class*. The class already exists in the switch configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map polmap6
Switch(config-pmap)# class silver-class
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# end
```

This example shows how to guarantee 30 percent of the bandwidth for *class1* and 25 percent of the bandwidth for *class2* when CBWFQ is configured. A policy map with two classes is created and is then attached to a physical port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input policy1
Switch(config-if)# end
```

This example shows how bandwidth is guaranteed if low-latency queueing (LLQ) and bandwidth are configured. In this example, LLQ is enabled in a class called voice1.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# bandwidth remaining percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# class voice1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
dbl	Enables active queue management on a transmit queue used by a class of traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.

Command	Description
priority	Enables the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
shape (class-based queueing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
show policy-map	Displays information about the policy map.

call-home (global configuration)

To enter call home configuration submode, use the **call-home** command in global configuration mode.

call-home

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

Once you enter the **call-home** command, the prompt changes to Switch (cfg-call-home)#, and you have access to the call home configuration commands as follows:

- **alert-group**—Enables or disables an alert group. See the **alert-group** command.
- **contact-email-addr** *email-address*—Assigns the system contact's e-mail address. You can enter up to 128 alphanumeric characters in e-mail address format with no spaces.
- **contract-id** *alphanumeric*—Specifies the customer contract identification for Cisco AutoNotification. You can enter up to 64 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (" ").
- **copy profile** *source-profile target-profile*—Creates a new destination profile (*target-profile*) with the same configuration settings as the existing profile (*source-profile*).
- **customer-id** *name*—Provides customer identification for Cisco AutoNotify. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (" ").
- **default**—Sets a command to its defaults.
- **exit**—Exits call home configuration mode and returns to global configuration mode.
- **mail-server** {*ipv4-address* | *name*} **priority** *priority*—Assigns the customer's e-mail server address and relative priority. You can enter an IP address or a fully qualified domain name (FQDN), and assign a priority from 1 (highest) to 100 (lowest).

  You can define backup e-mail servers by repeating the **mail-server** command and entering different **priority** numbers.
- **no**—Negates a command or set its defaults.
- **phone-number** **+***phone-number*—Specifies the phone number of the contact person. The *phone-number* value must begin with a plus (+) prefix, and may contain only dashes (-) and numbers. You can enter up to 16 characters. If you include spaces, you must enclose your entry in quotes (" ").
- **profile** *name*—Enters call-home profile configuration mode. See the **profile** command.
- **rate-limit** *threshold*—Configures the call-home message rate-limit threshold; valid values are from 1 to 60 messages per minute.
- **sender** {**from** | **reply-to**} *email-address*—Specifies the call-home message sender's e-mail addresses. You can enter up to 128 alphanumeric characters in e-mail address format with no spaces.

- **site-id** *alphanumeric*—Specifies the site identification for Cisco AutoNotify. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (“ ”).
- **street-address** *street-address*—Specifies the street address for the RMA part shipments. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (“ ”).
- **vrf**—Specifies the VPN routing or forwarding instance name; limited to 32 characters.

Examples

This example show how to configure the contact information:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# call-home
Switch(cfg-call-home)# contact-email-addr username@example.com
Switch(cfg-call-home)# phone-number +1-800-555-4567
Switch(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345”
Switch(cfg-call-home)# customer-id Customer1234
Switch(cfg-call-home)# site-id Site1ManhattanNY
Switch(cfg-call-home)# contract-id Company1234
Switch(cfg-call-home)# exit
Switch(config)#
```

This example shows how to configure the call-home message rate-limit threshold:

```
Switch(config)# call-home
Switch(cfg-call-home)# rate-limit 50
```

This example shows how to set the call-home message rate-limit threshold to the default setting:

```
Switch(config)# call-home
Switch(cfg-call-home)# default rate-limit
```

This example shows how to create a new destination profile with the same configuration settings as an existing profile:

```
Switch(config)# call-home
Switch(cfg-call-home)# copy profile profile1 profile1a
```

This example shows how to configure the general e-mail parameters, including a primary and secondary e-mail server:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# call-home
Switch(cfg-call-home)# mail-server smtp.example.com priority 1
Switch(cfg-call-home)# mail-server 192.168.0.1 priority 2
Switch(cfg-call-home)# sender from username@example.com
Switch(cfg-call-home)# sender reply-to username@example.com
Switch(cfg-call-home)# exit
Switch(config)#
```

This example shows how to specify MgmtVrf as the vrf name where the call-home email message is forwarded:

```
Switch(cfg-call-home)# vrf MgmtVrf
```

Related Commands

Command	Description
alert-group (refer to Cisco IOS documentation)	Enables an alert group.
profile (refer to Cisco IOS documentation)	Enters call-home profile configuration mode.
show call-home	Displays call home configuration information.

call-home request

To submit information about your system to Cisco for report and analysis information from the Cisco Output Interpreter tool, use the **call-home request** command in privileged EXEC mode. An analysis report is sent by Cisco to a configured contact e-mail address.

call-home request {**output-analysis "***show-command***"** | **config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*]

Syntax Description

output-analysis "*show-command*"	Sends the output of the specified CLI show command for analysis. The show command must be contained in quotes (" ").
config-sanity **bugs-list** **command-reference** **product-advisory**	Specifies the type of report requested. Based on this keyword, the output of a predetermined set of commands such as the **show running-config all**, **show version**, and **show module** (standalone) or **show module switch all** (VS system) commands, is sent to Cisco for analysis.
profile *name*	(Optional) Specifies an existing profile to which the request is sent. If no profile is specified, the request is sent to the Cisco TAC profile.
ccoid *user-id*	(Optional) Specifies the identifier of a registered Smart Call Home user. If a *user-id* is specified, the resulting analysis report is sent to the e-mail address of the registered user. If no *user-id* is specified, the report is sent to the contact e-mail address of the device.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.

Based on the keyword specifying the type of report requested, the following information is returned in response to the request:

- **config-sanity**—Information on best practices as related to the current running configuration.
- **bugs-list**—Known bugs in the running version and in the currently applied features.
- **command-reference**—Reference links to all commands in the running configuration.
- **product-advisory**—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.

Examples

This example shows a request for analysis of a user-specified show command:

```
Switch# call-home request output-analysis "show diagnostic result module all" profile TG
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
call-home send	Sends a CLI command to be executed, with the command output to be sent by e-mail.
call-home send alert-group	Sends a specific alert group message.
service call-home (refer to Cisco IOS documentation)	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home send

To execute a CLI command and e-mail the command output, use the **call-home send** command in privileged EXEC mode.

call-home send "*cli-command***"** {**email** *email-addr* [**service-number** *SR*] | **service-number** *SR*}

Syntax Description

"*cli-command*"	Specifies a CLI command to be executed. The command output is sent by e-mail.
email *email-addr*	Specifies the e-mail address to which the CLI command output is sent. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com.
service-number *SR*	Specifies an active TAC case number to which the command output pertains. This number is required only if no e-mail address (or a TAC e-mail address) is specified, and will appear in the e-mail subject line.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command causes the specified CLI command to be executed on the system. The specified CLI command must be enclosed in quotes (""), and can be any run or show command, including commands for all modules.

The command output is then sent by e-mail to the specified e-mail address. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com. The e-mail is sent in long text format with the service number, if specified, in the subject line.

Examples

This example shows how to send a CLI command and have the command output e-mailed:

```
Switch# call-home send "show diagnostic result module all" email support@example.com
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home (refer to Cisco IOS documentation)	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home send alert-group

To send a specific alert group message, use the **call-home send alert-group** command in privileged EXEC mode.

call-home send alert-group {**configuration** | **diagnostic module** *number* | **inventory**} [**profile** *profile-name*]

Syntax Description

configuration	Sends the configuration alert-group message to the destination profile.
diagnostic module *number*	Sends the diagnostic alert-group message to the destination profile for a specific module number.
inventory	Sends the inventory call-home message.
profile *profile-name*	(Optional) Specifies the name of the destination profile.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

When you enter the module number, you can enter the number of the module.

If you do not specify the **profile** *profile-name*, the message is sent to all subscribed destination profiles.

Only the configuration, diagnostic, and inventory alert groups can be manually sent. The destination profile need not be subscribed to the alert group.

Examples

This example shows how to send the configuration alert-group message to the destination profile:

```
Switch# call-home send alert-group configuration
```

This example shows how to send the diagnostic alert-group message to the destination profile for a specific module number:

```
Switch# call-home send alert-group diagnostic module 3
```

This example shows how to send the diagnostic alert-group message to all destination profiles for a specific module number:

```
Switch# call-home send alert-group diagnostic module 3 profile Ciscotac1
```

This example shows how to send the inventory call-home message:

```
Switch# call-home send alert-group inventory
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
call-home test	Sends a call-home test message that you define.

service call-home (refer to Cisco IOS documentation)	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home test

To manually send a Call Home test message, use the **call-home test** command in privileged EXEC mode.

call-home test [**"***test-message***"**] **profile** *profile-name*

Syntax Description

"*test-message*"	(Optional) Test message text.
profile *profile-name*	Specifies the name of the destination profile.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command sends a test message to the specified destination profile. If you enter test message text, you must enclose the text in quotes ("") if it contains spaces. If you do not enter a message, a default message is sent.

Examples

This example shows how to manually send a Call Home test message:

```
Switch# call-home test "test of the day" profile Ciscotac1
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home (refer to Cisco IOS documentation)	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

channel-group

To assign and configure an EtherChannel interface to an EtherChannel group, use the **channel-group** command. To remove a channel group configuration from an interface, use the **no** form of this command.

channel-group *number* **mode** {**active** | **on** | **auto** [**non-silent**]} | {**passive** | **desirable** [**non-silent**]}

no channel-group

Syntax Description

number	Specifies the channel-group number; valid values are from 1 to 64.
mode	Specifies the EtherChannel mode of the interface.
active	Enables LACP unconditionally.
on	Forces the port to channel without PAgP.
auto	Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP packet negotiation.
non-silent	(Optional) Used with the auto or desirable mode when traffic is expected from the other device.
passive	Enables LACP only if an LACP device is detected.
desirable	Places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets.

Defaults

No channel groups are assigned.

Command Modes

Interface configuration mode

Usage Guidelines

You do not have to create a port-channel interface before assigning a physical interface to a channel group. If a port-channel interface has not been created, it is automatically created when the first physical interface for the channel group is created.

If a specific channel number is used for the PAgP-enabled interfaces of a channel group, that same channel number cannot be used for configuring a channel that has LACP-enabled interfaces or vice versa.

You can also create port channels by entering the **interface port-channel** command. This will create a Layer 3 port channel. To change the Layer 3 port channel into a Layer 2 port channel, use the **switchport** command before you assign physical interfaces to the channel group. A port channel cannot be changed from Layer 3 to Layer 2 or vice versa when it contains member ports.

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but we recommend that you do so.

Any configuration or attribute changes that you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel, but are part of the channel group).

You can create in **on** mode a usable EtherChannel by connecting two port groups together.

Caution Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Do not assign bridge groups on the physical EtherChannel interfaces because it creates loops.

Examples

This example shows how to add Gigabit Ethernet interface 1/1 to the EtherChannel group that is specified by port-channel 45:

```
Switch(config-if)# channel-group 45 mode on
Creating a port-channel interface Port-channel45
Switch(config-if)#
```

Related Commands

Command	Description
interface port-channel	Accesses or creates a port-channel interface.
show interfaces port-channel (refer to Cisco IOS documentation)	Displays the information about the Fast EtherChannel.

channel-protocol

To enable LACP or PAgP on an interface, use the **channel-protocol** command. To disable the protocols, use the **no** form of this command.

channel-protocol {**lacp** | **pagp**}

no channel-protocol {**lacp** | **pagp**}

Syntax Description

lacp	Enables LACP to manage channeling.
pagp	Enables PAgP to manage channeling.

Defaults

pagp

Command Modes

Interface configuration mode

Usage Guidelines

You can also select the protocol using the **channel-group** command.

If the interface belongs to a channel, the **no** form of this command is rejected.

All ports in an EtherChannel must use the same protocol; you cannot run two protocols on one module.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

You can manually configure a switch with PAgP on one side and LACP on the other side in the **on** mode.

You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol. You can use the **channel-protocol** command to restrict anyone from selecting a mode that is not applicable to the selected protocol.

Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).

For a complete list of guidelines, refer to the "Configuring EtherChannel" section of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

Examples

This example shows how to select LACP to manage channeling on the interface:

```
Switch(config-if)# channel-protocol lacp
Switch(config-if)#
```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
show etherchannel	Displays EtherChannel information for a channel.

cisp enable

Use the **cisp enable** global configuration command to enable Client Information Signalling Protocol (CISP) on a switch.

cisp enable

no cisp enable

Syntax Description

cisp enable	Enable CISP.

Defaults

None

Command Modes

Global configuration

Usage Guidelines

You must enable the CISP protocol (with the global **cisp enable** command) on both the authenticator and supplicant switch. The CISP protocol is crucial because it conveys the client information from the supplicant switch to the authenticator switch thereby providing access for the clients of the supplicant switch through the authenticator switch.

Examples

This example shows how to enable CISP:

```
switch(config)# cisp enable
```

Related Commands

Command	Description
dot1x credentials (global configuration)	Configures a profile on a supplicant switch.
show cisp (IOS command)	Displays CISP information for a specified interface.

class

To specify the name of the class whose traffic policy you want to create or change, use the **class** policy-map configuration command. To delete an existing class from a policy map, use the **no** form of this command.

class *class-name*

no class *class-name*

Syntax Description

class-name	Name of the predefined traffic class for which you want to configure or modify a traffic policy. The class was previously created through the **class-map** *class-map-name* global configuration command.

Defaults

No classes are defined; except for the class-default.

Command Modes

Policy-map configuration mode

Usage Guidelines

Before using the **class** command, you must create a class map for matching packets to the class by using the **class-map** global configuration command. You also must use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After specifying a policy map, you can configure a traffic policy for new classes or modify a traffic policy for any existing classes in that policy map. The class name that you specify with the **class** command in the policy map ties the characteristics for that class (its policy) to the class map and its match criteria, as configured through the **class-map** global configuration command. You attach the policy map to a port by using the **service-policy (interface configuration)** configuration command.

After you enter the **class** command, the switch enters policy-map class configuration mode, and these configuration commands are available:

- **bandwidth** Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map. For more information, see the **bandwidth** command.
- **dbl** Enables dynamic buffer limiting for traffic hitting this class. For details on **dbl** parameters refer to the **show qos dbl** command.
- **exit** Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no** Returns a command to its default setting.
- **police** Configures a single-rate policer, an aggregate policer, or a two-rate traffic policer that uses the committed information rate (CIR) and the peak information rate (PIR) for a class of traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** command. For more information about the two-rate policer, see the **police (two rates)** and the **police (percent)** command.
- **priority** Enables the strict priority queue for a class of traffic. For more information, see the **priority** command.

- **service-policy (policy-map class)** Creates a service policy as a quality of service (QoS) policy within a policy map (called a hierarchical service policy). For more information, see the **service-policy (policy-map class)** command. This command is effective only in a hierarchical policy map attached to an interface.
- **set** Classifies IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP) or IP-precedence in the packet. For more information, see the **set** command.
- **shape (class-based queueing)** Sets the token bucket committed information rate (CIR) in a policy map. For more information, see the **shape (class-based queueing)** command.
- **trust** Defines a trust state for a traffic class. For more information, see the **trust** command.

The switch supports up to 256 classes, including the default class, in a policy map. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class. You configure the default traffic class by specifying **class-default** as the class name in the **class** policy-map class configuration command. You can manipulate the default traffic class (for example, set policies to police or to shape it) just like any other traffic class, but you cannot delete it.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to create a policy map called policy1. When attached to an ingress port, the policy matches all the inbound traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mbps and bursts of 20 KB. Traffic exceeding the profile is marked down to a Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent.

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# service-policy input policy1
Switch#
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port.
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
dbl	Enables active queue management on a transmit queue used by a class of traffic.
police	Configures the Traffic Policing feature.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
police rate	Configures single- or dual-rate policer.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
priority	Enables the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port.
service-policy (interface configuration)	Attaches a policy map to an interface.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
set	Marks IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet.
shape (class-based queueing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
show policy-map	Displays information about the policy map.
trust	Defines a trust state for traffic classified through the **class** policy-map configuration command.

class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** global configuration command. To delete an existing class map and to return to global configuration mode, use the **no** form of this command.

class-map [**match-all** | **match-any**] *class-map-name*

no class-map [**match-all** | **match-any**] *class-map-name*

Syntax Description

match-all	(Optional) Perform a logical-AND of all matching under this class map. All criteria in the class map must be matched.
match-any	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria in the class map must be matched.
class-map-name	Name of the class map.

Defaults

No class maps are defined.

If neither the **match-all** nor the **match-any** keyword is specified, the default is **match-all**.

Command Modes

Global configuration mode

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode. Packets are checked against the match criteria configured for a class map to decide if the packet belongs to that class. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the quality of service (QoS) specifications set in the traffic policy.

After you enter the **class-map** command, the switch enters class-map configuration mode, and these configuration commands are available:

- **description** Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit** Exits from QoS class-map configuration mode.
- **match** Configures classification criteria. For more information, see the **match (class-map configuration)** command.
- **no** Removes a match statement from a class map.

Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Switch# configure terminal
Switch(config)# access-list 103 permit any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
Switch#
```

This example shows how to delete the class1 class map:

```
Switch# configure terminal
Switch(config)# no class-map class1
Switch#
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
match (class-map configuration)	Defines the match criteria for a class map.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
show class-map	Displays class map information.

clear counters

To clear the interface counters, use the **clear counters** command.

clear counters [{**FastEthernet** *interface_number*} | {**GigabitEthernet** *interface_number*} | {**null** *interface_number*} | {**port-channel** *number*} | {**vlan** *vlan_id*}]

Syntax Description

FastEthernet *interface_number*	(Optional) Specifies the Fast Ethernet interface; valid values are from 1 to 9.
GigabitEthernet *interface_number*	(Optional) Specifies the Gigabit Ethernet interface; valid values are from 1 to 9.
null *interface_number*	(Optional) Specifies the null interface; the valid value is 0.
port-channel *number*	(Optional) Specifies the channel interface; valid values are from 1 to 64.
vlan *vlan_id*	(Optional) Specifies the VLAN; valid values are from 1 to 4096.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command clears all the current interface counters from all the interfaces unless you specify an interface.

Note This command does not clear the counters that are retrieved using SNMP, but only those seen when you enter the **show interface counters** command.

Examples

This example shows how to clear all the interface counters:

```
Switch# clear counters
Clear "show interface" counters on all interfaces [confirm] y
Switch#
```

This example shows how to clear the counters on a specific interface:

```
Switch# clear counters vlan 200
Clear "show interface" counters on this interface [confirm]y
Switch#
```

Related Commands

Command	Description
show interface counters (refer to Cisco IOS documentation)	Displays interface counter information.

clear errdisable

To re-enable error-disabled VLANs on an interface, use the **clear errdisable** command.

clear errdisable interface {*name*} **vlan** [*range*]

Syntax Description

interface *name*	Specifies the interface of the VLAN(s) to recover.
vlan	Specifies all VLANs on the interface be recovered.
range	(Optional) Specifies the VLAN range to be recovered.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

If a VLAN range is not specified, all VLANs on the specified interface are re-enabled. The **clear errdisable** command recovers the disabled VLANs on an interface.

Clearing the error-disabled state from a virtual port does not change the link state of the physical port, and it does not affect other VLAN ports on the physical port. It does post an event to STP, and spanning tree goes through its normal process of bringing that VLAN port to the appropriate blocking or forwarding state.

Examples

This example shows how to re-enable a range of disabled VLANs on an interaface:

```
Switch# clear errdisable interface ethernet2 vlan 10-15
Switch#
```

Related Commands

Command	Description
errdisable detect	Enables error-disable detection.
show errdisable detect	Displays the error-disable detection status.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.
switchport port-security	Enables port security on an interface.

clear hw-module slot password

To clear the password on an intelligent line module, use the **clear hw-module slot password** command.

clear hw-module slot *slot_num* **password**

Syntax Description

slot_num	Slot on a line module.

Defaults

The password is not cleared.

Command Modes

Privileged EXEC mode

Usage Guidelines

You only need to change the password once unless the password is reset.

Examples

This example shows how to clear the password from slot 5 on a line module:

```
Switch# clear hw-module slot 5 password
Switch#
```

Related Commands

Command	Description
hw-module power	Turns the power off on a slot or line module.

clear interface gigabitethernet

To clear the hardware logic from a Gigabit Ethernet IEEE 802.3z interface, use the **clear interface gigabitethernet** command.

Note This command does not increment **interface resets** as displayed with the **show interface gigabitethernet mod/port** command.

clear interface gigabitethernet *mod/port*

Syntax Description

mod/port	Number of the module and port.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the hardware logic from a Gigabit Ethernet IEEE 802.3z interface:

```
Switch# clear interface gigabitethernet 1/1
Switch#
```

Related Commands

Command	Description
show interfaces status	Displays the interface status.

clear interface vlan

To clear the hardware logic from a VLAN, use the **clear interface vlan** command.

clear interface vlan *number*

Syntax Description

number	Number of the VLAN interface; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the hardware logic from a specific VLAN:

```
Switch# clear interface vlan 5
Switch#
```

Related Commands

Command	Description
show interfaces status	Displays the interface status.

clear ip access-template

To clear the statistical information in access lists, use the **clear ip access-template** command.

clear ip access-template *access-list*

Syntax Description

access-list	Number of the access list; valid values are from 100 to 199 for an IP extended access list, and from 2000 to 2699 for an expanded range IP extended access list.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the statistical information for an access list:

```
Switch# clear ip access-template 201
Switch#
```

clear ip arp inspection log

To clear the status of the log buffer, use the **clear ip arp inspection log** command.

clear ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the contents of the log buffer:

```
Switch# clear ip arp inspection log
Switch#
```

Related Commands

Command	Description
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
show ip arp inspection log	Displays the status of the log buffer.

clear ip arp inspection statistics

To clear the dynamic ARP inspection statistics, use the **clear ip arp inspection statistics** command.

clear ip arp inspection statistics [**vlan** *vlan-range*]

Syntax Description

vlan *vlan-range*	(Optional) Specifies the VLAN range.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the DAI statistics from VLAN 1 and how to verify the removal:

```
Switch# clear ip arp inspection statistics vlan 1
Switch# show ip arp inspection statistics vlan 1

 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                         0
Switch#
```

Related Commands

Command	Description
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection log	Displays the status of the log buffer.

clear ip dhcp snooping binding

To clear the DHCP snooping binding, use the **clear ip dhcp snooping binding** command.

clear ip dhcp snooping binding [*****] [*ip-address*] [**vlan** *vlan_num*] [**interface** *interface_num*]

Syntax Description

*	(Optional) Clears all DHCP snooping binding entries.
ip-address	(Optional) IP address for the DHCP snooping binding entries.
vlan *vlan_num*	(Optional) Specifies a VLAN.
interface *interface_num*	(Optional) Specifies an interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

These commands are mainly used to clear DHCP snooping binding entries.

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

Examples

This example shows how to clear all the DHCP snoop binding entries:

```
Switch# clear ip dhcp snooping binding *
Switch#
```

This example shows how to clear a specific DHCP snoop binding entry:

```
Switch# clear ip dhcp snooping binding 1.2.3.4
Switch#
```

This example shows how to clear all the DHCP snoop binding entries on the GigabitEthernet interface 1/1:

```
Switch# clear ip dhcp snooping binding interface gigabitEthernet 1/1
Switch#
```

This example shows how to clear all the DHCP snoop binding entries on VLAN 40:

```
Switch# clear ip dhcp snooping binding vlan 40
Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

clear ip dhcp snooping database

To clear the DHCP binding database, use the **clear ip dhcp snooping database** command.

clear ip dhcp snooping database

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the DHCP binding database:

```
Switch# clear ip dhcp snooping database
Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

clear ip dhcp snooping database statistics

To clear the DHCP binding database statistics, use the **clear ip dhcp snooping database statistics** command.

clear ip dhcp snooping database statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the DHCP binding database:

```
Switch# clear ip dhcp snooping database statistics
Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

clear ip igmp group

To delete the IGMP group cache entries, use the **clear ip igmp group** command.

clear ip igmp group [{**fastethernet** *mod/port*} | {**GigabitEthernet** *mod/port*} | {*host_name* | *group_address*} {**Loopback** *interface_number*} | {**null** *interface_number*} | {**port-channel** *number*} | {**vlan** *vlan_id*}]

Syntax Description

fastethernet	(Optional) Specifies the Fast Ethernet interface.
mod/port	(Optional) Number of the module and port.
GigabitEthernet	(Optional) Specifies the Gigabit Ethernet interface.
host_name	(Optional) Hostname, as defined in the DNS hosts table or with the **ip host** command.
group_address	(Optional) Address of the multicast group in four-part, dotted notation.
Loopback *interface_number*	(Optional) Specifies the loopback interface; valid values are from 0 to 2,147,483,647.
null *interface_number*	(Optional) Specifies the null interface; the valid value is 0.
port-channel *number*	(Optional) Specifies the channel interface; valid values are from 1 to 64.
vlan *vlan_id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The IGMP cache contains a list of the multicast groups of which hosts on the directly connected LAN are members.

To delete all the entries from the IGMP cache, enter the **clear ip igmp group** command with no arguments.

Examples

This example shows how to clear the entries for a specific group from the IGMP cache:

```
Switch# clear ip igmp group 224.0.255.1
Switch#
```

This example shows how to clear the IGMP group cache entries from a specific interface:

```
Switch# clear ip igmp group gigabitethernet 2/2
Switch#
```

Related Commands

Command	Description
ip host (refer to Cisco IOS documentation)	Defines a static host name-to-address mapping in the host cache.
show ip igmp groups (refer to Cisco IOS documentation)	Displays the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show ip igmp groups** command in EXEC mode.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

clear ip igmp snooping membership

To clear the explicit host-tracking database, use the **clear ip igmp snooping membership** command.

clear ip igmp snooping membership [vlan *vlan_id*]

Syntax Description

vlan *vlan_id*	(Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

By default, the explicit host tracking database maintains a maximum of 1-KB entries. After you reach this limit, no additional entries can be created in the database. To create more entries, you will need to delete the database with the **clear ip igmp snooping statistics vlan** command.

Examples

This example shows how to display the IGMP snooping statistics for VLAN 25:

```
Switch# clear ip igmp snooping membership vlan 25
Switch#
```

Related Commands

Command	Description
ip igmp snooping vlan explicit-tracking	Enables per-VLAN explicit host tracking.
show ip igmp snooping membership	Displays host membership information.

clear ip mfib counters

To clear the global MFIB counters and the counters for all active MFIB routes, use the **clear ip mfib counters** command.

clear ip mfib counters

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear all the active MFIB routes and global counters:

```
Switch# clear ip mfib counters
Switch#
```

Related Commands

Command	Description
show ip mfib	Displays all active Multicast Forwarding Information Base (MFIB) routes.

clear ip mfib fastdrop

To clear all the MFIB fast-drop entries, use the **clear ip mfib fastdrop** command.

clear ip mfib fastdrop

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If new fast-dropped packets arrive, the new fast-drop entries are created.

Examples

This example shows how to clear all the fast-drop entries:

```
Switch# clear ip mfib fastdrop
Switch#
```

Related Commands

Command	Description
ip mfib fastdrop	Enables MFIB fast drop.
show ip mfib fastdrop	Displays all currently active fast-drop entries and shows whether fast drop is enabled.

clear ip wccp

To remove Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the switch for a particular service, use the **clear ip wccp** command in privileged EXEC mode.

clear ip wccp [**vrf** *vrf-name* {**web-cache** | *service-number*}] [**web-cache** | *service-number*]

Syntax Description

web-cache	(Optional) Directs the router to remove statistics for the web cache service.
service-number	(Optional) Number of the cache service to be removed. The number can be from 0 to 99.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Usage Guidelines

Use the **show ip wccp** and **show ip wccp detail** commands to display WCCP statistics.

Use the **clear ip wccp** command to clear the WCCP counters for all WCCP services in all VRFs.

Examples

The following example shows how to clear all statistics associated with the web cache service:

```
Switch# clear ip wccp web-cache
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
show ip wccp	Displays global statistics related to the WCCP.

clear lacp counters

To clear the statistics for all the interfaces belonging to a specific channel group, use the **clear lacp counters** command.

clear lacp [*channel-group*] **counters**

Syntax Description

channel-group	(Optional) Channel-group number; valid values are from 1 to 64.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a channel group, all channel groups are cleared.

If you enter this command for a channel group that contains members in PAgP mode, the command is ignored.

Examples

This example shows how to clear the statistics for a specific group:

```
Switch# clear lacp 1 counters
Switch#
```

Related Commands

Command	Description
show lacp	Displays LACP information.

clear mac-address-table

To clear the global counter entries from the Layer 2 MAC address table, use the **clear mac-address-table** command.

clear mac-address-table {dynamic [{**address** *mac_addr*} | {**interface** *interface*}] [**vlan** *vlan_id*] | **notification**}

Syntax Description

dynamic	Specifies dynamic entry types.
address *mac_addr*	(Optional) Specifies the MAC address.
interface *interface*	(Optional) Specifies the interface and clears the entries associated with it; valid values are **FastEthernet** and **GigabitEthernet**.
vlan *vlan_id*	(Optional) Specifies the VLANs; valid values are from 1 to 4094.
notification	Specifies MAC change notification global counters.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

Enter the **clear mac-address-table dynamic** command with no arguments to remove all dynamic entries from the table.

The **clear mac-address-table notification** command only clears the global counters which are displayed with **show mac-address-table notification** command. It does not clear the global counters and the history table of the CISCO-MAC-NATIFICATION-MIB.

Examples

This example shows how to clear all the dynamic Layer 2 entries for a specific interface (gi1/1):

```
Switch# clear mac-address-table dynamic interface gi1/1
Switch#
```

This example shows how to clear the MAC address notification counters:

```
Switch# clear mac-address-table notification
Switch#
```

Related Commands

Command	Description
clear mac-address-table dynamic	Clears the dynamic address entries from the Layer 2 MAC address table.
mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mac-address-table notification	Enables MAC address notification on a switch.
main-cpu	Enters the main CPU submode and manually synchronizes the configurations on two supervisor engines.
show mac-address-table address	Displays the information about the MAC-address table.
snmp-server enable traps	Enables SNMP notifications.

clear mac-address-table dynamic

To clear the dynamic address entries from the Layer 2 MAC address table, use the **clear mac-address-table dynamic** command.

clear mac-address-table dynamic [{**address** *mac_addr*} | {**interface** *interface*}] [**vlan** *vlan_id*]

Syntax Description

address *mac_addr*	(Optional) Specifies the MAC address.
interface *interface*	(Optional) Specifies the interface and clears the entries associated with it; valid values are **FastEthernet** and **GigabitEthernet**.
vlan *vlan_id*	(Optional) Specifies the VLANs; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

Enter the **clear mac-address-table dynamic** command with no arguments to remove all dynamic entries from the table.

Examples

This example shows how to clear all the dynamic Layer 2 entries for a specific interface (gi1/1):

```
Switch# clear mac-address-table dynamic interface gi1/1
Switch#
```

Related Commands

Command	Description
mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
main-cpu	Enters the main CPU submode and manually synchronizes the configurations on two supervisor engines.
show mac-address-table address	Displays the information about the MAC-address table.

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command. This command is available only when your switch is running the cryptographic (encrypted) software image.

clear nmsp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear NMSP statistics:

```
Switch# clear nmsp statistics
Switch#
```

You can verify that information was deleted by entering the **show nmsp statistics** command.

Related Commands

Command	Description
show nmsp	Displays the NMSP information.

clear pagp

To clear the port-channel information, use the **clear pagp** command.

clear pagp {*group-number* | **counters**}

Syntax Description

group-number	Channel-group number; valid values are from 1 to 64.
counters	Clears traffic filters.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the port-channel information for a specific group:

```
Switch# clear pagp 32
Switch#
```

This example shows how to clear all the port-channel traffic filters:

```
Switch# clear pagp counters
Switch#
```

Related Commands

Command	Description
show pagp	Displays information about the port channel.

clear port-security

To delete all configured secure addresses or a specific dynamic or sticky secure address on an interface from the MAC address table, use the **clear port-security** command.

clear port-security dynamic [**address** *mac-addr* [**vlan** *vlan-id*]] | [**interface** *interface-id*] [**vlan access** | **voice**]

Syntax Description

dynamic	Deletes all the dynamic secure MAC addresses.
address *mac-addr*	(Optional) Deletes the specified secure MAC address.
vlan *vlan-id*	(Optional) Deletes the specified secure MAC address from the specified VLAN.
interface *interface-id*	(Optional) Deletes the secure MAC addresses on the specified physical port or port channel.
vlan access	(Optional) Deletes the secure MAC addresses from access VLANs.
vlan voice	(Optional) Deletes the secure MAC addresses from voice VLANs.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If you enter the **clear port-security all** command, the switch removes all the dynamic secure MAC addresses from the MAC address table.

Note You can clear sticky and static secure MAC addresses one at a time with the **no switchport port-security mac-address** command.

If you enter the **clear port-security dynamic interface** *interface-id* command, the switch removes all the dynamic secure MAC addresses on an interface from the MAC address table.

Examples

This example shows how to remove all the dynamic secure addresses from the MAC address table:

```
Switch# clear port-security dynamic
```

This example shows how to remove a dynamic secure address from the MAC address table:

```
Switch# clear port-security dynamic address 0008.0070.0007
```

This example shows how to remove all the dynamic secure addresses learned on a specific interface:

```
Switch# clear port-security dynamic interface gigabitethernet0/1
```

You can verify that the information was deleted by entering the **show port-security** command.

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.
switchport port-security	Enables port security on an interface.

clear pppoe intermediate-agent statistics

To clear PPPoE Intermediate Agent statistics (packet counters), use the **clear pppoe intermediate-agent statistics** command.

clear ppoe intermediate-agent statistics

Syntax Description

This command has no arguments**.**

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear PPPoE Intermediate Agent statistics:

```
Switch# clear pppoe intermediate-agent statistics
```

Related Commands

Command	Description
show pppoe intermediate-agent interface	Displays PPPoE Intermediate Agent statistics (packet counters).

clear qos

To clear the global and per-interface aggregate QoS counters, use the **clear qos** command.

clear qos [**aggregate-policer** [*name*] | **interface** {{**fastethernet** | **GigabitEthernet**} {*mod/interface*}} | **vlan** {*vlan_num*} | **port-channel** {*number*}]

Syntax Description

aggregate-policer *name*	(Optional) Specifies an aggregate policer.
interface	(Optional) Specifies an interface.
fastethernet	(Optional) Specifies the Fast Ethernet 802.3 interface.
GigabitEthernet	(Optional) Specifies the Gigabit Ethernet 802.3z interface.
mod/interface	(Optional) Number of the module and interface.
vlan *vlan_num*	(Optional) Specifies a VLAN.
port-channel *number*	(Optional) Specifies the channel interface; valid values are from 1 to 64.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

When you enter the **clear qos** command, the way that the counters work is affected and the traffic that is normally restricted could be forwarded for a short period of time.

The **clear qos** command resets the interface QoS policy counters. If no interface is specified, the **clear qos** command resets the QoS policy counters for all interfaces.

Examples

This example shows how to clear the global and per-interface aggregate QoS counters for all the protocols:

```
Switch# clear qos
Switch#
```

This example shows how to clear the specific protocol aggregate QoS counters for all the interfaces:

```
Switch# clear qos aggregate-policer
Switch#
```

Related Commands

Command	Description
show qos	Displays QoS information.

clear vlan counters

To clear the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs, use the **clear vlan counters** command.

clear vlan [*vlan-id*] **counters**

Syntax Description

vlan-id	(Optional) VLAN number; see the "Usage Guidelines" section for valid values.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a *vlan-id* value; the software-cached counter values for all the existing VLANs are cleared.

Examples

This example shows how to clear the software-cached counter values for a specific VLAN:

```
Switch# clear vlan 10 counters
Clear "show vlan" counters on this vlan [confirm] y
Switch#
```

Related Commands

Command	Description
show vlan counters	Displays VLAN counter information.

clear vmps statistics

To clear the VMPS statistics, use the **clear vmps statistics** command.

clear vmps statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the VMPS statistics:

```
Switch# clear vmps statistics
Switch#
```

Related Commands

Command	Description
show vmps	Displays VMPS information.
vmps reconfirm (privileged EXEC)	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

control-plane

To enter control-plane configuration mode, which allows users to associate or modify attributes or parameters (such as a service policy) that are associated with the control plane of the device, use the **control-plane** command.

control-plane

Syntax Description

This command has no arguments or keywords.

Defaults

Default service police *system-cpp-policy* is attached.

Command Modes

Global configuration mode

Usage Guidelines

After you enter the **control-plane** command, you can define control plane services for your route processor. For example, you can associate a service policy with the control plane to police all traffic that is destined to the control plane.

Examples

These examples show how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate:

```
Switch(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Switch(config)# access-list 140 permit tcp any any eq telnet
! Define class-map “telnet-class.”
Switch(config)# class-map telnet-class
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map control-plane
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c)# police 32000 1000 conform transmit exceed drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor.
Switch(config)# macro global apply system-cpp
Switch(config)# control-plane
Switch(config-cp)# service-police input system-cpp-policy
Switch(config-cp)# exit
```

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
match access-group (refer to the *Cisco IOS Release 12.2 Command Reference*)	Configures the match criteria for a class map on the basis of the specified access control list (ACL).
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (interface configuration)	Attaches a policy map to an interface.
show policy-map control-plane	Displays the configuration either of a class or of all classes for the policy map of a control plane.

counter

To assign counters to a Layer 3 interface, use the **counter** interface command. To remove a counter assignment, use the **no** form of this command.

counter {**ipv4** | **ipv6** | **ipv4 ipv6 separate**}

no counter

Syntax Description

ipv4	Enables collection of IPv4 statistics only.
ipv6	Enables collection of IPv6 statistics only.
ipv4 ipv6 separate	Enables collection of IPv4 and IPv6 statistics and displays them individually.

Defaults

Not enabled

Command Modes

Interface configuration

Usage Guidelines

Entering the **counter** command without keywords displays the statistics as a sum.

The total number of switch ports that can possess transmit and receive counters is 4092.

When you change a Layer 3 port assigned with a counter to a Layer 2 port, the hardware counters are cleared. This action is similar to entering the **no counter** command.

Examples

The following example shows how to enable counters on interface VLAN 1:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# counter ipv4
Switch(config-if)# end
Switch#
00:17:15: %SYS-5-CONFIG_I: Configured from console by console
Switch# show run interface vlan 1
Building configuration...

Current configuration : 63 bytes
!
interface Vlan1
 ip address 10.0.0.1 255.0.0.0
 counter ipv4
end
```

Note To remove the counter assignment, use the **no counter** command.

If you have already assigned the maximum number of counters, the **counter** command fails, displaying the following error message:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fa3/2
Switch(config-if)# no switchport
Switch(config-if)# counter ipv6
 Counter resource exhausted for interface fa3/2
Switch(config-if)# end
Switch#
00:24:18: %SYS-5-CONFIG_I: Configured from console by console
```

In this situation, you must release a counter from another interface so the new interface can use it.

dbl

To enable active queue management on a transmit queue used by a class of traffic, use the **dbl** command. Use the **no** form of this command to return to the default setting.

dbl

no dbl

Syntax Description

This command has no keywords or arguments.

Defaults

Active queue management is disabled.

Command Modes

Policy-map class configuration

Usage Guidelines

The semantics of the DBL configuration is similar to the WRED algorithm. The **dbl** command can operate alone on class-default; otherwise, it requires you to configure the **bandwidth** or **shape** commands on the class.

Examples

This example shows how to enable dbl action in a class:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

Related Commands

Command	Description
bandwidth	Creates a signaling class structure that can be referred to by its name.
class	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
show policy-map	Displays information about the policy map.

debug adjacency

To display information about the adjacency debugging, use the **debug adjacency** command. To disable debugging output, use the **no** form of this command.

debug adjacency [**ipc**]

no debug adjacency

Syntax Description

ipc	(Optional) Displays the IPC entries in the adjacency database.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display the information in the adjacency database:

```
Switch# debug adjacency
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
<... output truncated...>
Switch#
```

Related Commands

Command	Description
undebug adjacency (same as no debug adjacency)	Disables debugging output.

debug backup

To debug the backup events, use the **debug backup** command. To disable the debugging output, use the **no** form of this command.

debug backup

no debug backup

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to debug the backup events:

```
Switch# debug backup
Backup events debugging is on
Switch#
```

Related Commands

Command	Description
undebug backup (same as no debug backup)	Disables debugging output.

debug condition interface

To limit the debugging output of interface-related activities, use the **debug condition interface** command. To disable the debugging output, use the **no** form of this command.

debug condition interface {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **null** *interface_num* | **port-channel** *interface-num* | **vlan** *vlan_id*}

no debug condition interface {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **null** *interface_num* | **port-channel** *interface-num* | **vlan** *vlan_id*}

Syntax Description

fastethernet	Limits the debugging to Fast Ethernet interfaces.
mod/port	Number of the module and port.
GigabitEthernet	Limits the debugging to Gigabit Ethernet interfaces.
null *interface-num*	Limits the debugging to null interfaces; the valid value is 0.
port-channel *interface-num*	Limits the debugging to port-channel interfaces; valid values are from 1 to 64.
vlan *vlan_id*	Specifies the VLAN interface number; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to limit the debugging output to VLAN interface 1:

```
Switch# debug condition interface vlan 1
Condition 2 set
Switch#
```

Related Commands

Command	Description
debug interface	Abbreviates the entry of the **debug condition interface** command.
undebug condition interface (same as no debug condition interface)	Disables interface related activities.

debug condition standby

To limit the debugging output for the standby state changes, use the **debug condition standby** command. To disable the debugging output, use the **no** form of this command.

debug condition standby {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **port-channel** *interface-num* | **vlan** *vlan_id group-number*}

no debug condition standby {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **port-channel** *interface-num* | **vlan** *vlan_id group-number*}

Syntax Description

fastethernet	Limits the debugging to Fast Ethernet interfaces.
mod/port	Number of the module and port.
GigabitEthernet	Limits the debugging to Gigabit Ethernet interfaces.
port-channel *interface_num*	Limits the debugging output to port-channel interfaces; valid values are from 1 to 64.
vlan *vlan_id*	Limits the debugging of a condition on a VLAN interface; valid values are from 1 to 4094.
group-number	VLAN group number; valid values are from 0 to 255.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If you attempt to remove the only condition set, you will be prompted with a message asking if you want to abort the removal operation. You can enter **n** to abort the removal or **y** to proceed with the removal. If you remove the only condition set, an excessive number of debugging messages might occur.

Examples

This example shows how to limit the debugging output to group 0 in VLAN 1:

```
Switch# debug condition standby vlan 1 0
Condition 3 set
Switch#
```

This example shows the display if you try to turn off the last standby debug condition:

```
Switch# no debug condition standby vlan 1 0
This condition is the last standby condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no]: n
% Operation aborted
Switch#
```

Related Commands

Command	Description
undebug condition standby (same as no debug condition standby)	Disables debugging output.

debug condition vlan

To limit the VLAN debugging output for a specific VLAN, use the **debug condition vlan** command. To disable the debugging output, use the **no** form of this command.

debug condition vlan {*vlan_id*}

no debug condition vlan {*vlan_id*}

Syntax Description

vlan_id	Number of the VLAN; valid values are from 1 to 4096.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If you attempt to remove the only VLAN condition set, you will be prompted with a message asking if you want to abort the removal operation. You can enter **n** to abort the removal or **y** to proceed with the removal. If you remove the only condition set, it could result in the display of an excessive number of messages.

Examples

This example shows how to limit the debugging output to VLAN 1:

```
Switch# debug condition vlan 1
Condition 4 set
Switch#
```

This example shows the message that is displayed when you attempt to disable the last VLAN debug condition:

```
Switch# no debug condition vlan 1
This condition is the last vlan condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no]: n
% Operation aborted
Switch#
```

Related Commands

Command	Description
undebug condition vlan (same as no debug condition vlan)	Disables debugging output.

debug dot1x

To enable the debugging for the 802.1X feature, use the **debug dot1x** command. To disable the debugging output, use the **no** form of this command.

debug dot1x {**all** | **errors** | **events** | **packets** | **registry** | **state-machine**}

no debug dot1x {**all** | **errors** | **events** | **packets** | **registry** | **state-machine**}

Syntax Description

all	Enables the debugging of all conditions.
errors	Enables the debugging of print statements guarded by the dot1x error flag.
events	Enables the debugging of print statements guarded by the dot1x events flag.
packets	All incoming dot1x packets are printed with packet and interface information.
registry	Enables the debugging of print statements guarded by the dot1x registry flag.
state-machine	Enables the debugging of print statements guarded by the dot1x registry flag.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable the 802.1X debugging for all conditions:

```
Switch# debug dot1x all
Switch#
```

Related Commands

Command	Description
show dot1x	Displays dot1x information.
undebug dot1x (same as no debug dot1x)	Disables debugging output.

debug etherchnl

To debug EtherChannel, use the **debug etherchnl** command. To disable the debugging output, use the **no** form of this command.

debug etherchnl [**all** | **detail** | **error** | **event** | **idb** | **linecard**]

no debug etherchnl

Syntax Description

all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays the detailed EtherChannel debug messages.
error	(Optional) Displays the EtherChannel error messages.
event	(Optional) Debugs the major EtherChannel event messages.
idb	(Optional) Debugs the PAgP IDB messages.
linecard	(Optional) Debugs the SCP messages to the module.

Defaults

The default settings are as follows:

- Debug is disabled.
- All messages are displayed.

Command Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify a keyword, all debug messages are displayed.

Examples

This example shows how to display all the EtherChannel debug messages:

```
Switch# debug etherchnl
PAgP Shim/FEC debugging is on
22:46:30:FEC:returning agport Po15 for port (Fa2/1)
22:46:31:FEC:returning agport Po15 for port (Fa4/14)
22:46:33:FEC:comparing GC values of Fa2/25 Fa2/15 flag = 1 1
22:46:33:FEC:port_attrib:Fa2/25 Fa2/15 same
22:46:33:FEC:EC - attrib incompatable for Fa2/25; duplex of Fa2/25 is half, Fa2/15 is full
22:46:33:FEC:pagp_switch_choose_unique:Fa2/25, port Fa2/15 in agport Po3 is incompatable
Switch#
```

This example shows how to display the EtherChannel IDB debug messages:

```
Switch# debug etherchnl idb
Agport idb related debugging is on
Switch#
```

This example shows how to disable the debugging:

```
Switch# no debug etherchnl
Switch#
```

Related Commands

Command	Description
undebug etherchnl (same as no debug etherchnl)	Disables debugging output.

debug interface

To abbreviate the entry of the **debug condition interface** command, use the **debug interface** command. To disable debugging output, use the **no** form of this command.

debug interface {**FastEthernet** *mod/port* | **GigabitEthernet** *mod/port* | **null** | **port-channel** *interface-num* | **vlan** *vlan_id*}

no debug interface {**FastEthernet** *mod/port* | **GigabitEthernet** *mod/port* | **null** | **port-channel** *interface-num* | **vlan** *vlan_id*}

Syntax Description

FastEthernet	Limits the debugging to Fast Ethernet interfaces.
mod/port	Number of the module and port.
GigabitEthernet	Limits the debugging to Gigabit Ethernet interfaces.
null	Limits the debugging to null interfaces; the only valid value is 0.
port-channel *interface-num*	Limits the debugging to port-channel interfaces; valid values are from 1 to 64.
vlan *vlan_id*	Specifies the VLAN interface number; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to limit the debugging to interface VLAN 1:

```
Switch# debug interface vlan 1
Condition 1 set
Switch#
```

Related Commands

Command	Description
debug condition interface	Limits the debugging output of interface-related activities.
undebug etherchnl (same as no debug etherchnl)	Disables debugging output.

debug ipc

To debug the IPC activity, use the **debug ipc** command. To disable the debugging output, use the **no** form of this command.

debug ipc {**all** | **errors** | **events** | **headers** | **packets** | **ports** | **seats**}

no debug ipc {**all** | **errors** | **events** | **headers** | **packets** | **ports** | **seats**}

Syntax Description

all	Enables all IPC debugging.
errors	Enables the IPC error debugging.
events	Enables the IPC event debugging.
headers	Enables the IPC header debugging.
packets	Enables the IPC packet debugging.
ports	Enables the debugging of the creation and deletion of ports.
seats	Enables the debugging of the creation and deletion of nodes.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable the debugging of the IPC events:

```
Switch# debug ipc events
Special Events debugging is on
Switch#
```

Related Commands

Command	Description
undebug ipc (same as no debug ipc)	Disables debugging output.

debug ip dhcp snooping event

To debug the DHCP snooping events, use the **debug ip dhcp snooping event** command. To disable debugging output, use the **no** form of this command.

debug ip dhcp snooping event

no debug ip dhcp snooping event

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging of snooping event is disabled.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable the debugging for the DHCP snooping events:

```
Switch# debug ip dhcp snooping event
Switch#
```

This example shows how to disable the debugging for the DHCP snooping events:

```
Switch# no debug ip dhcp snooping event
Switch#
```

Related Commands

Command	Description
debug ip dhcp snooping packet	Debugs the DHCP snooping messages.

debug ip dhcp snooping packet

To debug the DHCP snooping messages, use the **debug ip dhcp snooping packet** command. To disable the debugging output, use the **no** form of this command.

debug ip dhcp snooping packet

no debug ip dhcp snooping packet

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging of snooping packet is disabled.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable the debugging for the DHCP snooping packets:

```
Switch# debug ip dhcp snooping packet
Switch#
```

This example shows how to disable the debugging for the DHCP snooping packets:

```
Switch# no debug ip dhcp snooping packet
Switch#
```

Related Commands

Command	Description
debug ip dhcp snooping event	Debugs the DHCP snooping events.

debug ip verify source packet

To debug the IP source guard messages, use the **debug ip verify source packet** command. To disable the debugging output, use the **no** form of this command.

debug ip verify source packet

no debug ip verify source packet

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging of snooping security packets is disabled.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable debugging for the IP source guard:

```
Switch# debug ip verify source packet
Switch#
```

This example shows how to disable debugging for the IP source guard:

```
Switch# no debug ip verify source packet
Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping limit rate	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

debug lacp

To debug the LACP activity, use the **debug lacp** command. To disable the debugging output, use the **no** form of this command.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp

Syntax Description

all	(Optional) Enables all LACP debugging.
event	(Optional) Enables the debugging of the LACP events.
fsm	(Optional) Enables the debugging of the LACP finite state machine.
misc	(Optional) Enables the miscellaneous LACP debugging.
packet	(Optional) Enables the LACP packet debugging.

Defaults

Debugging of LACP activity is disabled.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only by the supervisor engine and can be entered only from the Catalyst 4500 series switch console.

Examples

This example shows how to enable the LACP miscellaneous debugging:

```
Switch# debug lacp
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
```

Related Commands

Command	Description
undebug pagp (same as no debug pagp)	Disables debugging output.

debug monitor

To display the monitoring activity, use the **debug monitor** command. To disable the debugging output, use the **no** form of this command.

debug monitor {**all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests**}

no debug monitor {**all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests**}

Syntax Description

all	Displays all the SPAN debugging messages.
errors	Displays the SPAN error details.
idb-update	Displays the SPAN IDB update traces.
list	Displays the SPAN list tracing and the VLAN list tracing.
notifications	Displays the SPAN notifications.
platform	Displays the SPAN platform tracing.
requests	Displays the SPAN requests.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to debug the monitoring errors:

```
Switch# debug monitor errors
SPAN error detail debugging is on
Switch#
```

Related Commands

Command	Description
undebug monitor (same as no debug monitor)	Disables debugging output.

debug nmsp

To the enable debugging of the Network Mobility Services Protocol (NMSP) on the switch, use the **debug nmsp** command. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to disable debugging.

debug nmsp {**all** | **connection** | **error** | **event** | **packet** | **rx** | **tx**}

no debug nmsp

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC mode

Usage Guidelines

The **undebug nmsp** command is the same as the **no debug nmsp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show nmsp	Displays the NMSP information.

debug nvram

To debug the NVRAM activity, use the **debug nvram** command. To disable the debugging output, use the **no** form of this command.

debug nvram

no debug nvram

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to debug NVRAM:

```
Switch# debug nvram
NVRAM behavior debugging is on
Switch#
```

Related Commands

Command	Description
undebug nvram (same as no debug nvram)	Disables debugging output.

debug pagp

To debug the PAgP activity, use the **debug pagp** command. To disable the debugging output, use the **no** form of this command.

debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp

Syntax Description

all	(Optional) Enables all PAgP debugging.
dual-active	(Optional) Enables the PAgP dual-active debugging.
event	(Optional) Enables the debugging of the PAgP events.
fsm	(Optional) Enables the debugging of the PAgP finite state machine.
misc	(Optional) Enables the miscellaneous PAgP debugging.
packet	(Optional) Enables the PAgP packet debugging.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the supervisor engine and can be entered only from the Catalyst 4500 series switch console.

Examples

This example shows how to enable the PAgP miscellaneous debugging:

```
Switch# debug pagp misc
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
*Sep 30 10:13:03: SP: PAgP: pagp_h(Fa5/6) expired
*Sep 30 10:13:03: SP: PAgP: 135 bytes out Fa5/6
*Sep 30 10:13:03: SP: PAgP: Fa5/6 Transmitting information packet
*Sep 30 10:13:03: SP: PAgP: timer pagp_h(Fa5/6) started with interval 30000
<... output truncated...>
Switch#
```

Related Commands

Command	Description
undebug pagp (same as no debug pagp)	Disables debugging output.

debug platform packet protocol lacp

To debug the LACP protocol packets, use the **debug platform packet protocol lacp** command. To disable the debugging output, use the **no** form of this command.

debug platform packet protocol lacp [**receive** | **transmit** | **vlan**]

no debug platform packet protocol lacp [**receive** | **transmit** | **vlan**]

Syntax Description

receive	(Optional) Enables the platform packet reception debugging functions.
transmit	(Optional) Enables the platform packet transmission debugging functions.
vlan	(Optional) Enables the platform packet VLAN debugging functions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol lacp
Switch#
```

Related Commands

Command	Description
undebug platform packet protocol lacp (same as no debug platform packet protocol lacp)	Disables debugging output.

debug platform packet protocol pagp

To debug the PAgP protocol packets, use the **debug platform packet protocol pagp** command. To disable the debugging output, use the **no** form of this command.

debug platform packet protocol pagp [**receive** | **transmit** | **vlan**]

no debug platform packet protocol pagp [**receive** | **transmit** | **vlan**]

Syntax Description

receive	(Optional) Enables the platform packet reception debugging functions.
transmit	(Optional) Enables the platform packet transmission debugging functions.
vlan	(Optional) Enables the platform packet VLAN debugging functions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol pagp
Switch#
```

Related Commands

Command	Description
undebug platform packet protocol pagp (same as no debug platform packet protocol pagp)	Disables debugging output.

debug pm

To debug the port manager (PM) activity, use the **debug pm** command. To disable the debugging output, use the **no** form of this command.

debug pm {**all** | **card** | **cookies** | **etherchnl** | **messages** | **port** | **registry** | **scp** | **sm** | **span** | **split** | **vlan** | **vp**}

no debug pm {**all** | **card** | **cookies** | **etherchnl** | **messages** | **port** | **registry** | **scp** | **sm** | **span** | **split** | **vlan** | **vp**}

Syntax Description

all	Displays all PM debugging messages.
card	Debugs the module-related events.
cookies	Enables the internal PM cookie validation.
etherchnl	Debugs the EtherChannel-related events.
messages	Debugs the PM messages.
port	Debugs the port-related events.
registry	Debugs the PM registry invocations.
scp	Debugs the SCP module messaging.
sm	Debugs the state machine-related events.
span	Debugs the spanning-tree-related events.
split	Debugs the split-processor.
vlan	Debugs the VLAN-related events.
vp	Debugs the virtual port-related events.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable all PM debugging:

```
Switch# debug pm all
Switch#
```

Related Commands

Command	Description
undebug pm (same as no debug pm)	Disables debugging output.

debug port-security

To debug port security, use the **debug port-security** command. To disable the debugging output, use the **no** form of this command.

debug port-security

no debug port-security

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable all PM debugging:

```
Switch# debug port-security
Switch#
```

Related Commands

Command	Description
switchport port-security	Enables port security on an interface.

debug pppoe intermediate-agent

To turn on debugging of the PPPoE Intermediate Agent feature, use the **debug pppoe intermediate-agent** command. To turn off debugging, use the **no** form of this command.

debug pppoe intermediate-agent {**event** | **packet** | **all**}

no debug pppoe intermediate-agent {**event** | **packet** | **all**}

Syntax Description

event	Activates event debugging
packet	Activates packet debugging
all	Activates both event and packet debugging

Defaults

All debugging is turned off.

Command Modes

Privileged EXEC mode

Examples

This example shows how to turn on packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is on

*Sep  2 06:12:56.133: PPPOE_IA: Process new PPPoE packet, Message type: PADI, input
interface: Gi3/7, vlan : 2 MAC da: ffff.ffff.ffff, MAC sa: aabb.cc00.0000
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/4)
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/8)
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADO, input
interface: Gi3/4, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: 001d.e64c.6512
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADO, input
interface: Gi3/8, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: aabb.cc80.0000
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/7)
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADR, input
interface: Gi3/7, vlan : 2 MAC da: 001d.e64c.6512, MAC sa: aabb.cc00.0000
*Sep  2 06:12:56.145: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/4)
*Sep  2 06:12:56.145: PPPOE_IA: Process new PPPoE packet, Message type: PADS, input
interface: Gi3/4, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: 001d.e64c.6512
```

This example shows how to turn off packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is off
```

Related Commands

Command	Description
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
pppoe intermediate-agent limit rate	Limits the rate of the PPPoE Discovery packets arriving on an interface.
pppoe intermediate-agent trust	Sets the trust configuration of an interface.

debug redundancy

To debug supervisor engine redundancy, use the **debug redundancy** command. To disable the debugging output, use the **no** form of this command.

debug redundancy {**errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

no debug redundancy

Syntax Description

errors	Enables the redundancy facility for error debugging.
fsm	Enables the redundancy facility for FSM event debugging.
kpa	Enables the redundancy facility for keepalive debugging.
msg	Enables the redundancy facility for messaging event debugging.
progression	Enables the redundancy facility for progression event debugging.
status	Enables the redundancy facility for status event debugging.
timer	Enables the redundancy facility for timer event debugging.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to debug the redundancy facility timer event debugging:

```
Switch# debug redundancy timer
Redundancy timer debugging is on
Switch#
```

debug spanning-tree

To debug the spanning tree activities, use the **debug spanning-tree** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **etherchannel** | **config** | **events** | **exceptions** | **general** | **ha** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

no debug spanning-tree {**all** | **bpdu** | **bpdu-opt** | **etherchannel** | **config** | **events** | **exceptions** | **general** | **mst** | **pvst+** | **root** | **snmp**}

Syntax Description

all	Displays all the spanning tree debugging messages.
backbonefast	Debugs the BackboneFast events.
bpdu	Debugs the spanningtree BPDU.
bpdu-opt	Debugs the optimized BPDU handling.
etherchannel	Debugs the spanning tree EtherChannel support.
config	Debugs the spanning tree configuration changes.
events	Debugs the TCAM events.
exceptions	Debugs the spanning tree exceptions.
general	Debugs the general spanning tree activity.
ha	Debugs the HA events.
mstp	Debugs the multiple spanning tree events.
pvst+	Debugs the PVST+ events.
root	Debugs the spanning tree root events.
snmp	Debugs the spanning tree SNMP events.
switch	Debugs the switch debug events.
synchronization	Debugs the STP state synchronization events.
uplinkfast	Debugs the UplinkFast events.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to debug the spanning-tree PVST+:

```
Switch# debug spanning-tree pvst+
Spanning Tree PVST+ debugging is on
Switch#
```

Related Commands

Command	Description
undebug spanning-tree (same as no debug spanning-tree)	Disables debugging output.

debug spanning-tree backbonefast

To enable debugging of the spanning tree BackboneFast events, use the **debug spanning-tree backbonefast** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree backbonefast [**detail** | **exceptions**]

no debug spanning-tree backbonefast

Syntax Description

detail	(Optional) Displays the detailed BackboneFast debugging messages.
exceptions	(Optional) Enables the debugging of spanning tree BackboneFast exceptions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the supervisor engine and enterable only from the switch console.

Examples

This example shows how to enable the debugging and to display the detailed spanning tree BackboneFast debugging information:

```
Switch# debug spanning-tree backbonefast detail
Spanning Tree backbonefast detail debugging is on
Switch#
```

Related Commands

Command	Description
undebug spanning-tree backbonefast (same as no debug spanning-tree backbonefast)	Disables debugging output.

debug spanning-tree switch

To enable the switch shim debugging, use the **debug spanning-tree switch** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree switch {**all** | **errors** | **general** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

no debug spanning-tree switch {**all** | **errors** | **general** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

Syntax Description

all	Displays all the spanning-tree switch shim debugging messages.
errors	Enables the debugging of switch shim errors or exceptions.
general	Enables the debugging of general events.
pm	Enables the debugging of port manager events.
rx	Displays the received BPDU-handling debugging messages.
decode	Enables the debugging of the decode-received packets of the spanning-tree switch shim.
errors	Enables the debugging of the receive errors of the spanning-tree switch shim.
interrupt	Enables the shim ISR receive BPDU debugging on the spanning-tree switch.
process	Enables the process receive BPDU debugging on the spanning-tree switch.
state	Enables the debugging of the state changes on the spanning-tree port.
tx	Enables the transmit BPDU debugging on the spanning-tree switch shim.
decode	(Optional) Enables the decode-transmitted packets debugging on the spanning-tree switch shim.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the supervisor engine and enterable only from the switch console.

Examples

This example shows how to enable the transmit BPDU debugging on the spanning tree switch shim:

```
Switch# debug spanning-tree switch tx
Spanning Tree Switch Shim transmit bpdu debugging is on
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 303
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 304
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 305
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 349
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 350
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 351
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 801
<... output truncated...>
Switch#
```

Related Commands

Command	Description
undebug spanning-tree switch (same as no debug spanning-tree switch)	Disables debugging output.

debug spanning-tree uplinkfast

To enable the debugging of the spanning-tree UplinkFast events, use the **debug spanning-tree uplinkfast** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree uplinkfast [**exceptions**]

no debug spanning-tree uplinkfast

Syntax Description

exceptions	(Optional) Enables the debugging of the spanning tree UplinkFast exceptions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the supervisor engine and enterable only from the switch console.

Examples

This example shows how to debug the spanning tree UplinkFast exceptions:

```
Switch# debug spanning-tree uplinkfast exceptions
Spanning Tree uplinkfast exceptions debugging is on
Switch#
```

Related Commands

Command	Description
undebug spanning-tree uplinkfast (same as no debug spanning-tree uplinkfast)	Disables debugging output.

debug sw-vlan

To debug the VLAN manager activities, use the **debug sw-vlan** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan {**badpmcookies** | **events** | **management** | **packets** | **registries**}

no debug sw-vlan {**badpmcookies** | **events** | **management** | **packets** | **registries**}

Syntax Description

badpmcookies	Displays the VLAN manager incidents of bad port manager cookies.
events	Debugs the VLAN manager events.
management	Debugs the VLAN manager management of internal VLANs.
packets	Debugs the packet handling and encapsulation processes.
registries	Debugs the VLAN manager registries.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to debug the software VLAN events:

```
Switch# debug sw-vlan events
vlan manager events debugging is on
Switch#
```

Related Commands

Command	Description
undebug sw-vlan (same as no debug sw-vlan)	Disables debugging output.

debug sw-vlan ifs

To enable the VLAN manager Cisco IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

no debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

Syntax Description

open	Enables the VLAN manager IFS debugging of errors in an IFS file-open operation.
read	Debugs the errors that occurred when the IFS VLAN configuration file was open for reading.
write	Debugs the errors that occurred when the IFS VLAN configuration file was open for writing.
{**1** | **2** | **3** | **4**}	Determines the file-read operation. See the “Usage Guidelines” section for information about operation levels.
write	Debugs the errors that occurred during an IFS file-write operation.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The following are four types of file read operations:

- Operation **1**—Reads the file header, which contains the header verification word and the file version number.
- Operation **2**—Reads the main body of the file, which contains most of the domain and VLAN information.
- Operation **3**—Reads TLV descriptor structures.
- Operation **4**—Reads TLV data.

Examples

This example shows how to debug the TLV data errors during a file-read operation:

```
Switch# debug sw-vlan ifs read 4
vlan manager ifs read # 4 errors debugging is on
Switch#
```

Related Commands

Command	Description
undebug sw-vlan ifs (same as no debug sw-vlan ifs)	Disables debugging output.

debug sw-vlan notification

To enable the debugging of the messages that trace the activation and deactivation of the ISL VLAN IDs, use the **debug sw-vlan notification** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

no debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

Syntax Description

accfwdchange	Enables the VLAN manager notification of aggregated access interface STP forward changes.
allowedvlancfgchange	Enables the VLAN manager notification of changes to allowed VLAN configuration.
fwdchange	Enables the VLAN manager notification of STP forwarding changes.
linkchange	Enables the VLAN manager notification of interface link state changes.
modechange	Enables the VLAN manager notification of interface mode changes.
pruningcfgchange	Enables the VLAN manager notification of changes to pruning configuration.
statechange	Enables the VLAN manager notification of interface state changes.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to debug the software VLAN interface mode change notifications:

```
Switch# debug sw-vlan notification modechange
vlan manager port mode change notification debugging is on
Switch#
```

Related Commands

Command	Description
undebug sw-vlan notification (same as no debug sw-vlan notification)	Disables debugging output.

debug sw-vlan vtp

To enable the debugging of messages to be generated by the VTP protocol code, use the **debug sw-vlan vtp** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan vtp {**events** | **packets** | **pruning** [**packets** | **xmit**] | **xmit**}

no debug sw-vlan vtp {**events** | **packets** | **pruning** [**packets** | **xmit**] | **xmit**}

Syntax Description

events	Displays the general-purpose logic flow and detailed VTP debugging messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
packets	Displays the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
pruning	Enables the debugging message to be generated by the pruning segment of the VTP protocol code.
packets	(Optional) Displays the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer.
xmit	(Optional) Displays the contents of all outgoing VTP packets that the VTP code will request that the Cisco IOS VTP platform-dependent layer to send.
xmit	Displays the contents of all outgoing VTP packets that the VTP code will request that the Cisco IOS VTP platform-dependent layer to send; does not include pruning packets.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If you do not enter any more parameters after entering **pruning**, the VTP pruning debugging messages are displayed.

Examples

This example shows how to debug the software VLAN outgoing VTP packets:

```
Switch# debug sw-vlan vtp xmit
vtp xmit debugging is on
Switch#
```

Related Commands

Command	Description
undebug sw-vlan vtp (same as no debug sw-vlan vtp)	Disables debugging output.

debug udld

To enable the debugging of UDLD activity, use the **debug udld** command. To disable the debugging output, use the **no** form of this command.

debug udld {**events** | **packets** | **registries**}

no debug udld {**events** | **packets** | **registries**}

Syntax Description

events	Enables the debugging of UDLD process events as they occur.
packets	Enables the debugging of the UDLD process as it receives packets from the packet queue and attempts to transmit packets at the request of the UDLD protocol code.
registries	Enables the debugging of the UDLD process as it processes registry upcalls from the UDLD process-dependent module and other feature modules.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command is supportedonly on the supervisor engine and enterable only from the switch console.

Examples

This example shows how to debug the UDLD events:

```
Switch# debug udld events
UDLD events debugging is on
Switch#
```

This example shows how to debug the UDLD packets:

```
Switch# debug udld packets
UDLD packets debugging is on
Switch#
```

This example shows how to debug the UDLD registry events:

```
Switch# debug udld registries
UDLD registries debugging is on
Switch#
```

Related Commands

Command	Description
undebug udld (same as no debug udld)	Disables debugging output.

debug vqpc

To debug the VLAN Query Protocol (VQP), use the **debug vqpc** command. To disable the debugging output, use the **no** form of this command.

debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

Syntax Description

all	(Optional) Debugs all the VQP events.
cli	(Optional) Debugs the VQP command-line interface.
events	(Optional) Debugs the VQP events.
learn	(Optional) Debugs the VQP address learning.
packet	(Optional) Debugs the VQP packets.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable all VQP debugging:

```
Switch# debug vqpc all
Switch#
```

Related Commands

Command	Description
vmps reconfirm (privileged EXEC)	Immediately sends VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

define interface-range

To create a macro of interfaces, use the **define interface-range** command.

define interface-range *macro-name interface-range*

Syntax Description

macro-name	Name of the interface range macro; up to 32 characters.
interface-range	List of valid ranges when specifying interfaces; see the "Usage Guidelines" section.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

The macro name is a character string of up to 32 characters.

A macro can contain up to five ranges. An interface range cannot span modules.

When entering the *interface-range*, use these formats:

- *interface-type* {*mod*}/{*first-interface*} - {*last-interface*}
- *interface-type* {*mod*}/{*first-interface*} - {*last-interface*}

The valid values for *interface-type* are as follows:

- **FastEthernet**
- **GigabitEthernet**
- **Vlan** *vlan_id*

Examples

This example shows how to create a multiple-interface macro:

```
Switch(config)# define interface-range macro1 gigabitethernet 4/1-6, fastethernet 2/1-5
Switch(config)#
```

Related Commands

Command	Description
interface range	Runs a command on multiple ports at the same time.

deny

To deny an ARP packet based on matches against the DHCP bindings, use the **deny** command. To remove the specified ACEs from the access list, use the **no** form of this command.

deny {[**request**] **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **response** **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} [{**any** | **host** *target-ip* | *target-ip target-ip-mask*}] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [{**any** | **host** *target-mac* | *target-mac target-mac-mask*}]} [**log**]

no deny {[**request**] **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **response** **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} [{**any** | **host** *target-ip* | *target-ip target-ip-mask*}] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [{**any** | **host** *target-mac* | *target-mac target-mac-mask*}]} [**log**]

Syntax Description

request	(Optional) Requests a match for the ARP request. When **request** is not specified, matching is performed against all ARP packets.
ip	Specifies the sender IP address.
any	Specifies that any IP or MAC address will be accepted.
host *sender-ip*	Specifies that only a specific sender IP address will be accepted.
sender-ip sender-ip-mask	Specifies that a specific range of sender IP addresses will be accepted.
mac	Specifies the sender MAC address.
host *sender-mac*	Specifies that only a specific sender MAC address will be accepted.
sender-mac sender-mac-mask	Specifies that a specific range of sender MAC addresses will be accepted.
response	Specifies a match for the ARP responses.
ip	Specifies the IP address values for the ARP responses.
host *target-ip*	(Optional) Specifies that only a specific target IP address will be accepted.
target-ip target-ip-mask	(Optional) Specifies that a specific range of target IP addresses will be accepted.
mac	Specifies the MAC address values for the ARP responses.
host *target-mac*	(Optional) Specifies that only a specific target MAC address will be accepted.
target-mac target-mac-mask	(Optional) Specifies that a specific range of target MAC addresses will be accepted.
log	(Optional) Logs a packet when it matches the access control entry (ACE).

Defaults

At the end of the ARP access list, there is an implicit **deny ip any mac any** command.

Command Modes

arp-nacl configuration mode

Usage Guidelines

Deny clauses can be added to forward or drop ARP packets based on some matching criteria.

Examples

This example shows a host with a MAC address of 0000.0000.abcd and an IP address of 1.1.1.1. This example shows howto deny both requests and responses from this host:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
Switch# show arp access-list

ARP access list static-hosts
    deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

Related Commands

Command	Description
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
ip arp inspection filter vlan	Permits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and applies it to a VLAN.
permit	Permits an ARP packet based on matches against the DHCP bindings.

destination address

To configure the destination e-mail address or URL to which Call Home messages will be sent, use the **destination address** command.

destination address {**email** *email-address* | **http** *url*}

Syntax Description

email *email-address*	Specifies the destination e-mail address in 1 to 200 characters.
http *url*	Specifies the destination HTTP URL in 2 to 200 characters.

Defaults

This command has no default settings.

Command Modes

cfg-call-home-profile

Usage Guidelines

To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

When entering the https:// *destination* URL for the secure server, you must also configure a trustpoint CA.

Examples

This example shows how to set the destination to the e-mail address **callhome@cisco.com**:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination address email callhome@cisco.com
```

Related Commands

Command	Description
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

destination message-size-limit bytes

To configure a maximum destination message size for the destination profile, use the **destination message-size-limit bytes** command.

destination message-size-limit bytes

Syntax Description

This command has no arguments or keywords.

Defaults

3145728 bytes

Command Modes

cfg-call-home-profile

Usage Guidelines

To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples

This example shows how to configure the maximum message size for the destination profile as 3000000:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination message-size-limit 3000000
Switch(cfg-call-home-profile)#
```

Related Commands

Command	Description
destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

destination preferred-msg-format

To configure a preferred message format, use the **destination preferred-msg-format** command.

destination preferred-msg-format {**long-text** | **short-text** | **xml**}

Syntax Description

long-text	Sends the message in long-text format.
short-text	Sends the message in short-text format.
xml	Sends the message in XML format.

Defaults

xml

Command Modes

cfg-call-home-profile

Usage Guidelines

To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples

This example shows how to configure the preferred message format as long text:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination preferred-msg-format long-text
Switch(cfg-call-home-profile)#
```

Related Commands

Command	Description
destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

destination transport-method

To enable the message transport method, use the **destination transport-method** command.

destination transport-method {**email** | **http**}

Syntax Description

email	Enables e-mail as transport method.
http	Enables HTTP as transport method.

Defaults

e-mail

Command Modes

cfg-call-home-profile

Usage Guidelines

To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples

This example shows how to set the transport method to HTTP:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination transport-method http
```

Related Commands

Command	Description
destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination preferred-msg-format	Configures a preferred message format.
profile	Enters profile call-home configuration submode
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

diagnostic fpga soft-error recover

To configure the SEU behavior, use the **diagnostic fpga soft-error recover** command. To return to the default setting, use the **no** form of this command.

diagnostic fpga soft-error recover {conservative | aggressive}

no diagnostic fpga soft-error recover

Syntax Description

conservative	Dictates that the supervisor engine does not reload, Rather it issues a console error message once an hour. You should reload the supervisor engine at the next maintenance window.
aggressive	Dictates that the supervisor engine reloads immediately and automatically. A crashdump is generated, allowing you to identify the SEU event as the cause of the reload.

Defaults

A switch exhibits the default SEU behavior when this command is not configured. On redundant switches that have reached SSO, the default behavior is aggressive. In all other switches, the default behavior is conservative.

Command Modes

Global config mode

Usage Guidelines

SEU events on the system FPGAs result in a potentially unstable switch. The only recovery is to reload the affected supervisor engine. However, SEU events may be harmless, so you might want to delay the reload until a maintenance window, to avoid impacting users. Alternatively, you might want to force an immediate reload to avoid an instance where the switch crashes or drops traffic because of the SEU.

Examples

This example shows how to configure the SEU behavior as conservative:

```
Switch(config)# diagnostic fpga soft-error recover conservative
```

This example shows how to revert to the default behavior:

```
Switch(config)# no diagnositc fpga soft-error recover
```

diagnostic monitor action

To direct the action of the switch when it detects a packet memory failure, use the **diagnostic monitor action** command.

diagnostic monitor action [**conservative** | **normal** | **aggressive**]

Syntax Description

conservative	(Optional) Specifies that the bootup SRAM diagnostics log all failures and remove all affected buffers from the hardware operation. The ongoing SRAM diagnostics will log events, but will take no other action.
normal	(Optional) Specifies that the SRAM diagnostics operate as in conservative mode, except that an ongoing failure resets the supervisor engine; allows for the bootup tests to map out the affected memory.
aggressive	(Optional) Specifies that the SRAM diagnostics operate as in normal mode, except that a bootup failure only logs failures and does not allow the supervisor engine to come online; allows for either a redundant supervisor engine or network-level redundancy to take over.

Defaults

normal mode

Command Modes

Global configuration mode

Usage Guidelines

Use the **conservative** keyword when you do not want the switch to reboot so that the problem can be fixed.

Use the **aggressive** keyword when you have redundant supervisor engines, or when network-level redundancy has been provided.

Examples

This example shows how to configure the switch to initiate an RPR switchover when an ongoing failure occurs:

```
Switch# configure terminal
Switch (config)# diagnostic monitor action normal
```

Related Commands

Command	Description
show diagnostic result module test 2	Displays the module-based diagnostic test results.
show diagnostic result module test 3	Displays the module-based diagnostic test results.

diagnostic start

To run the specified diagnostic test, use the **diagnostic start** command.

diagnostic start {**module** *num*} {**test** *test-id*} [**port** *num*]

Syntax Description

module *num*	Module number.
test	Specifies a test to run.
test-id	Specifies an identification number for the test to be run; can be the cable diagnostic *test-id*, or the **cable-tdr** keyword.
port *num*	(Optional) Specifies the interface port number.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to run the specified diagnostic test at the specified module:

```
This exec command starts the TDR test on specified interface
Switch# diagnostic start module 1 test cable-tdr port 3
diagnostic start module 1 test cable-tdr port 3
module 1: Running test(s) 5 Run interface level cable diags
module 1: Running test(s) 5 may disrupt normal system operation
Do you want to continue? [no]: yes
yes
Switch#
2d16h: %DIAG-6-TEST_RUNNING: module 1: Running online-diag-tdr{ID=5} ...
2d16h: %DIAG-6-TEST_OK: module 1: online-diag-tdr{ID=5} has completed successfully

Switch#
```

Note The **show cable-diagnostic tdr** command displays the results of a TDR test. The test results will not be available until approximately 1 minute after the test starts. If you enter the **show cable-diagnostic tdr** command within 1 minute of the test starting, you may see a "TDR test is in progress on interface..." message.

Related Commands

Command	Description
show diagnostic content	Displays diagnostic content information.

dot1x auth-fail max-attempts

To configure the max number of attempts before a port is moved to the auth-fail VLAN, use the **dot1x auth-fail max-attempts** command. To return to the default setting, use the **no** form of this command.

dot1x auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts *max-attempts*

Syntax Description

max-attempts	Specifies a maximum number of attempts before a port is moved to the auth-fail VLAN in the range of 1 to 10.

Defaults

Default is 3.

Command Modes

Interface configuration mode

Examples

This example shows how to configure the maximum number of attempts before the port is moved to the auth-fail VLAN on Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail max-attempts 5
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
show dot1x	Displays 802.1x information.

dot1x auth-fail vlan

To enable the auth-fail VLAN on a port, use the **dot1x auth-fail vlan** command. To return to the default setting, use the **no** form of this command.

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan *vlan-id*

Syntax Description

vlan-id	Specifies a VLAN in the range of 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Examples

This example shows how to configure the auth-fail VLAN on Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
show dot1x	Displays dot1x information.

dot1x control-direction

To enable unidirectional port control on a per-port basis on a switch, use the **dot1x control-direction** command. Use the **no** form of this command to disable unidirectional port control.

dot1x control-direction [**in** | **both**]

no dot1x control-direction

Syntax Description

in	(Optional) Specifies controlling in-bound traffic on a port.
both	(Optional) Specifies controlling both in-bound and out-bound traffic on a port.

Defaults

Both in-bound and out-bound traffic will be controlled.

Command Modes

Interface configuration mode

Usage Guidelines

You can manage remote systems using unidirectional control. Unidirectional control enables you to turn on systems remotely using a specific Ethernet packet, known as a magic packet.

Using unidirectional control enables you to remotely manage systems using 802.1X ports. In the past, the port became unauthorized after the systems was turned off. In this state, the port only allowed the receipt and transmission of EAPoL packets. Therefore, there was no way for the unidirectional control magic packet to reach the host and without being turned on there was no way for the system to authenticate and open the port.

Examples

This example shows how to enable unidirectional control on incoming packets:

```
Switch(config-if)# dot1x control-direction in
Switch(config-if)#
```

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x credentials (global configuration)

Use the **dot1x credentials** global configuration command to configure a profile on a supplicant switch.

dot1x credentials *profile*

no dot1x credentials *profile*

Syntax Description

profile	Specify a profile for the supplicant switch.

Defaults

No profile is configured for the switch.

Command Modes

Global configuration

Usage Guidelines

You must have another switch set up as the authenticator for this switch to be the supplicant.

Examples

This example shows how to configure a switch as a supplicant:

```
Switch(config)# dot1x credentials profile
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
cisp enable	Enables Client Information Signalling Protocol (CISP).
show cisp (IOS command)	Displays CISP information for a specified interface.

dot1x critical

To enable the 802.1X critical authentication on a port, use the **dot1x critical** command. To return to the default setting, use the **no** form of this command.

dot1x critical

no dot1x critical

Syntax Description

This command has no keywords or variables.

Defaults

Critical authentication is disabled.

Command Modes

Interface configuration mode

Examples

This example shows how to enable 802.1x critical authentication:

```
Switch(config-if)# dot1x critical
Switch(config-if)#
```

Related Commands

Command	Description
dot1x critical eapol	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.
dot1x critical recovery delay	Sets the time interval between port reinitializations.
dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
show dot1x	Displays dot1x information.

dot1x critical eapol

To enable sending EAPOL success packets when a port is critically authorized partway through an EAP exchange, use the **dot1x critical eapol** command. To return to the default setting, use the **no** form of this command.

dot1x critical eapol

no dot1x critical eapol

Syntax Description

This command has no keywords or variables.

Defaults

The default is to not send EAPOL success packets.

Command Modes

Global configuration mode

Examples

This example shows how to enable sending EAPOL success packets:

```
Switch(config-if)# dot1x critical eapol
Switch(config-if)#
```

Related Commands

Command	Description
dot1x critical	Enables the 802.1X critical authentication on a port.
dot1x critical recovery delay	Sets the time interval between port reinitializations.
dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
show dot1x	Displays dot1x information.

dot1x critical recovery delay

To set the time interval between port reinitializations, use the **dot1x critical recovery delay** command. To return to the default setting, use the **no** form of this command.

dot1x critical recovery delay *delay-time*

no dot1x critical recovery delay

Syntax Description

delay-time	Specifies the interval between port reinitializations when AAA transistion occurs; valid values are from 1 to 10,000 milliseconds.

Defaults

Delay time is set to 100 milliseconds.

Command Modes

Global configuration mode

Examples

This example shows how to set the 802.1x critical recovery delay time to 500:

```
Switch(config-if)# dot1x critical recovery delay 500
Switch(config-if)#
```

Related Commands

Command	Description
dot1x critical	Enables the 802.1X critical authentication on a port.
dot1x critical eapol	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.
dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
show dot1x	Displays dot1x information.

dot1x critical vlan

To assign a critically authenticated port to a specific VLAN, use the **dot1x critical vlan** command. To return to the default setting, use the **no** form of this command.

dot1x critical vlan *vlan-id*

no dot1x critical *vlan-id*

Syntax Description

vlan-id	(Optional) Specifies the VLANs; valid values are from 1 to 4094.

Defaults

Critical authentication is disabled on a ports VLAN.

Command Modes

Interface configuration mode

Usage Guidelines

The type of VLAN specified must match the type of the port. If the port is an access port, the VLAN must be a regular VLAN. If the port is a private-VLAN host port, the VLAN must be the secondary VLAN of a valid private-VLAN domain. If the port is a routed port, no VLAN may be specified.

This command is not supported on platforms such as Layer 3 switches that do not include the Critical Auth VLAN subsystem.

Examples

This example shows how to enable 802.1x critical authentication on a ports VLAN:

```
Switch(config-if)# dot1x critical vlan 350
Switch(config-if)#
```

Related Commands

Command	Description
dot1x critical	Enables the 802.1X critical authentication on a port.
dot1x critical eapol	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.
dot1x critical recovery delay	Sets the time interval between port reinitializations.
show dot1x	Displays dot1x information.

dot1x guest-vlan

To enable a guest VLAN on a per-port basis, use the **dot1x guest-vlan** command. To return to the default setting, use the **no** form of this command.

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan *vlan-id*

Syntax Description

vlan-id	Specifies a VLAN in the range of 1 to 4094.

Defaults

This command has no default settings.; the guest VLAN feature is disabled.

Command Modes

Interface configuration mode

Usage Guidelines

Guest VLANs can be configured only on ports that are statically configured as access ports or private VLAN host ports. Statically configured access ports can be configured with regular VLANs as guest VLANs; statically configured private VLAN host ports can be configured with secondary private VLANs as guest VLANs.

Examples

This example shows how to enable a guest VLAN on Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 26
Switch(config-if)# end
Switch(config)# end
Switch#
```

Related Commands

Command	Description
dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
show dot1x	Displays dot1x information.

dot1x guest-vlan supplicant

To place an 802.1X-capable supplicant (host) into a guest VLAN, use the **dot1x guest-vlan supplicant** global configuration command. To return to the default setting, use the **no** form of this command.

dot1x quest-vlan supplicant

no dot1x quest-vlan supplicant

Syntax Description

This command has no arguments or keywords.

Defaults

802.1X-capable hosts are not put into a guest VLAN.

Command Modes

Global configuration mode

Usage Guidelines

With Cisco Release 12.2(25) EWA, you can use the **dot1x guest-vlan supplicant** command to place an 802.1X-capable host into a guest VLAN. Prior to Cisco Release 12.2(25)EWA, you could only place non-802.1X capable hosts into a guest VLAN.

When guest VLAN supplicant behavior is enabled, the Catalyst 4500 series switch does not maintain EAPOL packet history. The switch allows clients that fail 802.1X authentication to access a guest VLAN, whether or not EAPOL packets have been detected on the interface.

Examples

This example shows how to place an 802.1X-capable supplicant (host) into a guest VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# end
Switch#
```

Related Commands

Command	Description
dot1x system-auth-control	Enables 802.1X authentication on the switch.
show dot1x	Displays dot1x information.

dot1x host-mode

Use the **dot1x host-mode** interface configuration command on the switch stack or on a standalone switch to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port. Use the **multi-domain** keyword to enable multidomain authentication (MDA) on an IEEE 802.1x-authorized port. Use the **no** form of this command to return to the default setting.

dot1x host-mode {**multi-host** | **single-host** | **multi-domain**}

no dot1x host-mode [**multi-host** | **single-host** | **multi-domain**}

Syntax Description

multi-host	Enables multiple-hosts mode on the switch.
single-host	Enables single-host mode on the switch.
multi-domain	Enables MDA on a switch port.

Defaults

The default is single-host mode.

Command Modes

Interface configuration mode

Usage Guidelines

Use this command to limit an IEEE 802.1X-enabled port to a single client or to attach multiple clients to an IEEE 802.1X-enabled port. In multiple-hosts mode, only one of the attached hosts needs to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the **multi-domain** keyword to enable MDA on a port. MDA divides the port into both a data domain and a voice domain. MDA allows both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), on the same IEEE 802.1x-enabled port.

Before entering this command, make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified port.

You can assign both voice and data VLAN dynamically from the ACS server. No additional configuration is required to enable dynamic VLAN assignment on the switch.To enable VLAN assignment, you must configure the Cisco ACS server. For details on configuring the ACS server for voice VLAN assignment, refer to the "Cisco ACS Configuration for VLAN Assignment" section in the Catalyst 4500 Series Switch Software Configuration Guide-Release, 12.2(52)SG.

Examples

This example shows how to enable IEEE 802.1x authentication and to enable multiple-hosts mode:

```
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet6/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
Switch#
```

This example shows how to enable MDA and to allow both a host and a voice device on the port:

```
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet6/1
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x initialize

To unauthorize an interface before reinitializing 802.1X, use the **dot1x initialize** command.

dot1x initialize *interface*

Syntax Description

interface	Number of the interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

Use this command to initialize state machines and to set up the environment for fresh authentication.

Examples

This example shows how to initialize the 802.1X state machines on an interface:

```
Switch# dot1x initialize
Switch#
```

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x mac-auth-bypass

To enable the 802.1X MAC address bypassing on a switch, use the **dot1x mac-auth-bypass** command. Use the **no** form of this command to disable MAC address bypassing.

dot1x mac-auth-bypass [**eap**]

no dot1x mac-auth-bypass [**eap**]

Syntax Description

eap	(Optional) Specifies using EAP MAC address authentication.

Defaults

There is no default setting.

Command Modes

Interface configuration mode

Usage Guidelines

The removal of the **dot1x mac-auth-bypass** configuration from a port does not affect the authorization or authentication state of a port. If the port is in unauthenticated state, it remains unauthenticated, and if MAB is active, the authentication will revert back to the 802.1X Authenticator. If the port is authorized with a MAC address, and the MAB configuration is removed the port remains authorized until re-authentication takes place. When re-authentication occurs the MAC address is removed in favor of an 802.1X supplicant, which is detected on the wire.

Examples

This example shows how to enable EAP MAC address authentication:

```
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)#
```

dot1x max-reauth-req

To set the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process, use the **dot1x max-reauth-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-reauth-req *count*

no dot1x max-reauth-req

Syntax Description

count	Number of times that the switch retransmits EAP-Request/Identity frames before restarting the authentication process; valid values are from 1 to 10.

Defaults

The switch sends a maximum of two retransmissions.

Command Modes

Interface configuration mode

Usage Guidelines

You should 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. This setting impacts the wait before a non-dot1x-capable client is admitted to the guest VLAN, if one is configured.

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Examples

This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request/Identity frame before restarting the authentication process:

```
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)#
```

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x max-req

To set the maximum number of times that the switch retransmits an Extensible Authentication Protocol (EAP)-Request frame of types other than EAP-Request/Identity to the client before restarting the authentication process, use the **dot1x max-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-req *count*

no dot1x max-req

Syntax Description

count	Number of times that the switch retransmits EAP-Request frames of types other than EAP-Request/Identity before restarting the authentication process; valid values are from 1 to 10.

Defaults

The switch sends a maximum of two retransmissions.

Command Modes

Interface configuration mode

Usage Guidelines

You should 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.

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Examples

This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request frame before restarting the authentication process:

```
Switch(config-if)# dot1x max-req 5
Switch(config-if)#
```

This example shows how to return to the default setting:

```
Switch(config-if)# no dot1x max-req
Switch(config-if)#
```

Related Commands

Command	Description
dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
show dot1x	Displays dot1x information.

dot1x port-control

To enable manual control of the authorization state on a port, use the **dot1x port-control** command. To return to the default setting, use the **no** form of this command.

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

Syntax Description

auto	Enables 802.1X authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the switch and the client.
force-authorized	Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
force-unauthorized	Denies all access through the specified interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

Defaults

The port 802.1X authorization is disabled.

Command Modes

Interface configuration mode

Usage Guidelines

The 802.1X protocol is supported on both the Layer 2 static-access ports and the Layer 3-routed ports.

You can use the **auto** keyword only if the port is not configured as follows:

- Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.
- EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error message appears, and 802.1X is not enabled. If you enable 802.1X on an inactive port of an EtherChannel, the port does not join the EtherChannel.
- Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the switch, you must disable it on each port. There is no global configuration command for this task.

Examples

This example shows how to enable 802.1X on Gigabit Ethernet 1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# dot1x port-control auto
Switch#
```

You can verify your settings by using the **show dot1x all** or **show dot1x interface** *int* commands to show the port-control status. An enabled status indicates that the port-control value is set either to **auto** or to **force-unauthorized**.

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x re-authenticate

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port, use the **dot1x re-authenticate** command.

dot1x re-authenticate [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Module and port number of the interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

Examples

This example shows how to manually reauthenticate the device connected to Gigabit Ethernet interface 1/1:

```
Switch# dot1x re-authenticate interface gigabitethernet1/1
Starting reauthentication on gigabitethernet1/1
Switch#
```

dot1x re-authentication

To enable the periodic reauthentication of the client, use the **dot1x re-authentication** command. To return to the default setting, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

The periodic reauthentication is disabled.

Command Modes

Interface configuration mode

Usage Guidelines

You configure the amount of time between the periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples

This example shows how to disable the periodic reauthentication of the client:

```
Switch(config-if)# no dot1x re-authentication
Switch(config-if)#
```

This example shows how to enable the periodic reauthentication and set the number of seconds between the reauthentication attempts to 4000 seconds:

```
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout re-authperiod 4000
Switch#
```

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Related Commands

Command	Description
dot1x timeout	Sets the reauthentication timer.
show dot1x	Displays dot1x information.

dot1x system-auth-control

To enable 802.1X authentication on the switch, use the **dot1x system-auth-control** command. To disable 802.1X authentication on the system, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Defaults

The 802.1X authentication is disabled.

Command Modes

Global configuration mode

Usage Guidelines

You must enable **dot1x system-auth-control** if you want to use the 802.1X access controls on any port on the switch. You can then use the **dot1x port-control auto** command on each specific port on which you want the 802.1X access controls to be used.

Examples

This example shows how to enable 802.1X authentication:

```
Switch(config)# dot1x system-auth-control
Switch(config)#
```

Related Commands

Command	Description
dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
show dot1x	Displays dot1x information.

dot1x timeout

To set the reauthentication timer, use the **dot1x timeout** command. To return to the default setting, use the **no** form of this command.

dot1x timeout {**reauth-period** {*seconds* | **server**} | **quiet-period** *seconds* | **tx-period** *seconds* | **supp-timeout** *seconds* | **server-timeout** *seconds*}

no dot1x timeout {**reauth-period** | **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout**}

Syntax Description

reauth-period *seconds*	Number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the "Usage Guidelines" section for more information.
reauth-period server	Number of seconds between reauthentication attempts; valid values are from 1 to 65535 as derived from the Session-Timeout RADIUS attribute. See the "Usage Guidelines" section for more information.
quiet-period *seconds*	Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client; valid values are from 0 to 65535 seconds.
tx-period *seconds*	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request; valid values are from 1 to 65535 seconds.
supp-timeout *seconds*	Number of seconds that the switch waits for the retransmission of EAP-Request packets; valid values are from 30 to 65535 seconds.
server-timeout *seconds*	Number of seconds that the switch waits for the retransmission of packets by the back-end authenticator to the authentication server; valid values are from 30 to 65535 seconds.

Defaults

The default settings are as follows:

- Reauthentication period is 3600 seconds.
- Quiet period is 60 seconds.
- Transmission period is 30 seconds.
- Supplicant timeout is 30 seconds.
- Server timeout is 30 seconds.

Command Modes

Interface configuration mode

Usage Guidelines

The periodic reauthentication must be enabled before entering the **dot1x timeout re-authperiod** command. Enter the **dot1x re-authentication** command to enable periodic reauthentication.

Examples

This example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# end
Switch#
```

You can verify your settings by entering the **show dot1x** privileged EXEC command.

This example shows how to set up the switch to use a reauthentication timeout derived from a Session-Timeout attribute taken from the RADIUS Access-Accept message received when a host successfully authenticates via 802.1X:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x timeout reauth-period server
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
show dot1x	Displays dot1x information.

duplex

To configure the duplex operation on an interface, use the **duplex** command. To return to the default setting, use the **no** form of this command.

duplex {**auto** | **full** | **half**}

no duplex

Syntax Description

auto	Specifies the autonegotiation operation.
full	Specifies the full-duplex operation.
half	Specifies the half-duplex operation.

Defaults

Half-duplex operation

Command Modes

Interface configuration mode

Usage Guidelines

Table 2-1 lists the supported command options by interface.

Table 2-1 Supported duplex Command Options

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	**duplex** [**half** | **full**]	**half**	If the speed is set to **auto**, you will not be able to set the **duplex** mode. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex mode is set to **half** duplex.
100-Mbps fiber modules	**duplex** [**half** | **full**]	**half**	
Gigabit Ethernet Interface	Not supported.	Not supported.	Gigabit Ethernet interfaces are set to **full** duplex.
10/100/1000	**duplex** [**half** | **full**]		If the speed is set to **auto** or **1000**, you will not be able to set **duplex**. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex mode is set to **half** duplex.

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to **1000**, the duplex mode is set to **full**. If the transmission speed is changed to **10** or **100**, the duplex mode stays at **full**. You must configure the correct duplex mode on the switch when the transmission speed changes to **10** or **100** from 1000 Mbps.

⚠ **Caution** Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Table 2-2 describes the system performance for different combinations of the duplex and speed modes. The specified **duplex** command that is configured with the specified **speed** command produces the resulting action shown in the table.

Table 2-2 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half or **duplex full**	**speed auto**	Autonegotiates both speed and duplex modes
duplex half	**speed 10**	Forces 10 Mbps and half duplex
duplex full	**speed 10**	Forces 10 Mbps and full duplex
duplex half	**speed 100**	Forces 100 Mbps and half duplex
duplex full	**speed 100**	Forces 100 Mbps and full duplex
duplex full	**speed 1000**	Forces 1000 Mbps and full duplex

Examples

This example shows how to configure the interface for full-duplex operation:

```
Switch(config-if)# duplex full
Switch(config-if)#
```

Related Commands

Command	Description
speed	Configures the interface speed.
interface (refer to Cisco IOS documentation)	Configures an interface.
show controllers (refer to Cisco IOS documentation)	Displays controller information.
show interfaces	Displays interface information.

epm access control

To configure access control, use the **epm access control [open | default]** command.

epm access control [**open** | **default**]

Syntax Description

open	Specifies open access control.
default	Specifies default access control.

Defaults

If the **epm access control** command is not configured, the behavior defaults to the **epm access control default** command. Nothing is nvgened.

Command Modes

Configuration mode

Usage Guidelines

When you enter the **epm access** control command, it is nvgen'd.

If no ACLs are downloaded from the ACS server when a host is authenticated, the host is restricted by the port ACLs and do not receive additional permissions. In such a scenario, if you enter the **epm access control open** command, a **permit ip** *host* any entry is created for the host after authentication. This entry is created only if no ACLs are downloaded from the ACS.

The **epm access control open** command is particularly useful in authentication open mode. Traffic from a host is allowed to pass even before the host is authenticated. This traffic is restricted by the port ACL. In such a scenario, if no ACLs are downloaded from the ACS, the host will not receive any additional permissions. Even after authentication, the host is still restricted by the port ACL. If **epm access control open** is configured, complete access is granted upon authentication.

If **epm access control default** is configured and no ACL is downloaded, port ACL is the only ACL on the port. This is how access control functioned prior to Cisco IOS Release 12.2(54)SG.

Examples

The following example shows how to enable open access control:

```
Switch(config)# epm access control open
```

The following example shows how to enable default access control:

```
Switch(config)# epm access control default
```

Related Commands

Command	Description
show ipv6 snooping counters	Displays the number of packets dropped per port due to RA Guard.

erase

To erase a file system, use the **erase** command.

erase {**/all** [**non-default** | **nvram:**] | **cat4000_flash** | **nvram:** | **startup-config**}

Syntax Description

/all nvram:	Erases everything in nvram:.
/all non-default	Erases files and configuration in nonvolatile storage including nvram:, bootflash:, cat4000_flash:, and crashinfo: of the local supervisor engine. Resets the Catalyst 4500 series switch to the factory default settings. **Note** This command option is intended to work only on a standalone supervisor engine.
cat4000_flash:	Erases the VLAN database configuration file.
nvram:	Erases the startup-config and private-config file in NVRAM.
startup-config:	Erases the startup-config and private-config file in NVRAM.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

Caution When you use the **erase** command to erase a file system, you cannot recover the files in the file system.

In addition to the command options shown above, options with the prefix slave that are used to identify nvram: and flash (such as slavenvram: and slavecat4000_flash:) appear in the command help messages on the dual supervisor engine redundancy switch.

The **erase nvram:** command replaces the **write erase** and the **erase startup-confg** commands. This command erases both the startup-config and the private-config file.

The **erase /all nvram:** command erases all files in nvram: in addition to startup-config file and private-config file.

The **erase cat4000_flash:** command erases the VLAN database configuration file.

The **erase /all non-default** command facilitates the work of a manufacturing facility and repair center. It erases the configuration and states stored in the nonvolatile storage and resets the Catalyst 4500 series switch to the factory default settings. The default settings include those mentioned in the Cisco IOS library as well as those set by the **erase /all non-default** command (vtp mode=transparent, and the ROMMON variables: ConfigReg=0x2101, PS1= “rommon ! >” and EnableAutoConfig=1).

For the default settings, refer to these guides:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2, at this URL:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book.html

- *Cisco IOS Configuration Fundamentals Configuration Command Reference*, Release 12.2, at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html

Caution The **erase /all non-default** command can erase Cisco IOS images in bootflash:. Ensure that a Cisco IOS image can be copied back to the bootflash: (such as, from a accessible TFTP server or a flash card inserted in slot0:) (available on most chassis models), or that the switch can boot from a image stored in an accessible network server.

Examples

This example shows how to erase the files and configuration in a nonvolatile storage and reset the switch to factory default settings:

```
Switch# erase /all non-default
Switch#
Erase and format operation will destroy all data in non-volatile storage.  Continue?
[confirm]
Formatting bootflash: ...

Format of bootflash complete
Erasing nvram:
Erasing cat4000_flash:
Clearing crashinfo:data
Clearing the last power failure timestamp
Clearing all ROMMON variables
Setting default ROMMON variables:
     ConfigReg=0x2101
     PS1=rommon ! >
     EnableAutoConfig=1
Setting vtp mode to transparent
%WARNING! Please reboot the system for the changes to take effect
Switch#
00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

This example shows how to erase the contents in nvram.

```
Switch# erase /all nvram:
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
00:38:10: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram
Switch#
```

This example shows how to erase filesystem cat4000_flash.

```
Switch# erase cat4000_flash:
Erasing the cat4000_flash filesystem will remove all files! Continue? [confirm]
[OK]
Erase of cat4000_flash:complete
Switch#
```

Related Commands

Command	Description
boot config (refer to Cisco IOS documentation)	Specifies the device and filename of the configuration file.
delete (refer to Cisco IOS documentation)	Deletes a file from a flash memory device or NVRAM.
show bootvar	Displays BOOT environment variable information.
undelete (refer to Cisco IOS documentation)	Recovers a file marked “deleted” on a Class a flash file system.

errdisable detect

To enable error-disable detection, use the **errdisable detect** command. To disable the error-disable detection feature, use the **no** form of this command.

errdisable detect cause {**all** | **arp-inspection** [**action shutdown vlan**] | **bpduguard shutdown vlan** | **dhcp-rate-limit** [**action shutdown vlan**] | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap**}

no errdisable detect cause {**all** | **arp-inspection** [**action shutdown vlan**] | **bpduguard shutdown vlan** | **dhcp-rate-limit** [**action shutdown vlan**] | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap**}

Syntax Description

cause	Specifies error-disable detection to detect a specific cause.
all	Specifies error-disable detection for all error-disable causes.
arp-inspection	Specifies the detection for the ARP inspection error-disable cause.
action shutdown vlan	(Optional) Specifies per-VLAN error-disable for ARP inspection and DHCP rate limiting.
bpduguard shutdown vlan	Specifies per-VLAN error-disable for BPDU guard.
dhcp-rate-limit	Specifies the detection for the DHCP rate-limit error-disable cause.
dtp-flap	Specifies the detection for the DTP flap error-disable cause.
gbic-invalid	Specifies the detection for the GBIC invalid error-disable cause.
l2ptguard	Specifies the detection for the Layer 2 protocol-tunnel error-disable cause.
link-flap	Specifies the detection for the link flap error-disable cause.
pagp-flap	Specifies the detection for the PAgP flap error-disable cause.

Defaults

All error-disable causes are detected.

Command Modes

Global configuration mode

Usage Guidelines

A cause (dtp-flap, link-flap, pagp-flap) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state (an operational state that is similar to link-down state).

You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from the error-disable state.

To prevent the port from shutting down, you can use the **shutdown vlan** option to shut down just the offending VLAN on the port where the violation occured. This option is available for the following three causes: bpduguard, arp-inspection, and dhcp-rate-limit. You can use the **clear errdisable** command to recover disabled VLANs on a port.

Examples

This example shows how to enable error-disable detection for the link-flap error-disable cause:

```
Switch(config)# errdisable detect cause link-flap
Switch(config)#
```

This example shows how to enable per-VLAN error-disable detection for BPDU guard:

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
Switch(config)#
```

This example shows how to disable error-disable detection for DAI:

```
Switch(config)# no errdisable detect cause arp-inspection
Switch(config)# end
Switch# show errdisable detect
ErrDisable Reason    Detection   Mode
-----------------    ----------  ------
arp-inspection       Enabled     port
bpduguard            Enabled     vlan
channel-misconfig    Enabled     port
dhcp-rate-limit      Enabled     port
dtp-flap             Enabled     port
gbic-invalid         Enabled     port
psecure-violation    Enabled     port/vlan
Switch#
```

Related Commands

Command	Description
show errdisable detect	Displays the error disable detection status.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

errdisable recovery

To configure the recovery mechanism variables, use the **errdisable recovery** command. To return to the default setting, use the **no** form of this command.

errdisable recovery [**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **storm-control** | **udld** | **unicastflood** | **vmps**} [**arp-inspection**] [**interval** {*interval*}]]

no errdisable recovery [**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **storm-control** | **udld** | **unicastflood** | **vmps**} [**arp-inspection**] [**interval** {*interval*}]]

Syntax Description

cause	(Optional) Enables the error-disable recovery to recover from a specific cause.
all	(Optional) Enables the recovery timers for all error-disable causes.
arp-inspection	(Optional) Enables the recovery timer for the ARP inspection cause.
bpduguard	(Optional) Enables the recovery timer for the BPDU guard error-disable cause.
channel-misconfig	(Optional) Enables the recovery timer for the channel-misconfig error-disable cause.
dhcp-rate-limit	(Optional) Enables the recovery timer for the DHCP rate limit error-disable cause.
dtp-flap	(Optional) Enables the recovery timer for the DTP flap error-disable cause.
gbic-invalid	(Optional) Enables the recovery timer for the GBIC invalid error-disable cause.
l2ptguard	(Optional) Enables the recovery timer for the Layer 2 protocol-tunnel error-disable cause.
link-flap	(Optional) Enables the recovery timer for the link flap error-disable cause.
pagp-flap	(Optional) Enables the recovery timer for the PAgP flap error-disable cause.
pesecure-violation	(Optional) Enables the recovery timer for the pesecure violation error-disable cause.
security-violation	(Optional) Enables the automatic recovery of ports disabled due to 802.1X security violations.
storm-control	(Optional) Enables the timer to recover from storm-control error-disable state.
udld	(Optional) Enables the recovery timer for the UDLD error-disable cause.
unicastflood	(Optional) Enables the recovery timer for the unicast flood error-disable cause.
vmps	(Optional) Enables the recovery timer for the VMPS error-disable cause.
arp-inspection	(Optional) Enables the ARP inspection cause and recovery timeout.
interval *interval*	(Optional) Specifies the time to recover from a specified error-disable cause; valid values are from 30 to 86400 seconds.

Defaults

Error disable recovery is disabled.

The recovery interval is set to 300 seconds.

Command Modes

Global configuration mode

Usage Guidelines

A cause (bpduguard, dtp-flap, link-flap, pagp-flap, udld) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state (an operational state that is similar to the link-down state). If you do not enable error-disable recovery for the cause, the interface stays in the error-disabled state until a shutdown and no shutdown occurs. If you enable recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry operation again once all the causes have timed out.

You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from error disable.

Examples

This example shows how to enable the recovery timer for the BPDU guard error disable cause:

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)#
```

This example shows how to set the timer to 300 seconds:

```
Switch(config)# errdisable recovery interval 300
Switch(config)#
```

This example shows how to enable the errdisable recovery for arp-inspection:

```
Switch(config)# errdisable recovery cause arp-inspection
Switch(config)# end
Switch# show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Enabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Switch#
```

Related Commands

Command	Description
show errdisable detect	Displays the error disable detection status.
show errdisable recovery	Displays error disable recovery timer information.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

flowcontrol

To configure a Gigabit Ethernet interface to send or receive pause frames, use the **flowcontrol** command. To disable the flow control setting, use the **no** form of this command.

flowcontrol {**receive** | **send**} {**off** | **on** | **desired**}

no flowcontrol {**receive** | **send**} {**off** | **on** | **desired**}

Syntax Description

receive	Specifies that the interface processes pause frames.
send	Specifies that the interface sends pause frames.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Obtains predictable results whether a remote port is set to on, off, or desired.

Defaults

The default settings for Gigabit Ethernet interfaces are as follows:

- Sending pause frames is off—Non-oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—Non-oversubscribed Gigabit Ethernet interfaces.
- Sending pause frames is on—Oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—Oversubscribed Gigabit Ethernet interfaces.

Table 2-3 shows the default settings for the modules.

Table 2-3 Default Module Settings

Module	Ports	Send
All modules except WS-X4418-GB and WS-X4416-2GB-TX	All ports except for the oversubscribed ports	Off
WS-X4418-GB	Uplink ports (1–2)	Off
WS-X4418-GB	Oversubscribed ports (3–18)	On
WS-X4412-2GB-TX	Uplink ports (13–14)	Off
WS-X4412-2GB-TX	Oversubscribed ports (1–12)	On
WS-X4416-2GB-TX	Uplink ports (17–18)	Off

Command Modes

Interface configuration mode

Usage Guidelines

The pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

Table 2-4 describes the guidelines for using the different configurations of the **send** and **receive** keywords with the **flowcontrol** command.

Table 2-4 Keyword Configurations for send and receive

Configuration	Description
send on	Enables a local port to send pause frames to remote ports. To obtain predictable results, use **send on** only when remote ports are set to **receive on** or **receive desired**.
send off	Prevents a local port from sending pause frames to remote ports. To obtain predictable results, use **send off** only when remote ports are set to **receive off** or **receive desired**.
send desired	Obtains predictable results whether a remote port is set to **receive on**, **receive off**, or **receive desired**.
receive on	Enables a local port to process pause frames that a remote port sends. To obtain predictable results, use **receive on** only when remote ports are set to **send on** or **send desired**.
receive off	Prevents remote ports from sending pause frames to a local port. To obtain predictable results, use **send off** only when remote ports are set to **receive off** or **receive desired**.
receive desired	Obtains predictable results whether a remote port is set to **send on**, **send off**, or **send desired**.

Table 2-5 identifies how the flow control will be forced or negotiated on the Gigabit Ethernet interfaces based on their speed settings.

Table 2-5 Send Capability by Switch Type, Module, and Port

Interface Type	Configured Speed	Advertised Flow Control
10/100/1000BASE-TX	Speed 1000	Configured flow control always
1000BASE-T	Negotiation always enabled	Configured flow control always negotiated
1000BASE-X	No speed nonegotiation	Configured flow control negotiated
1000BASE-X	Speed nonegotiation	Configured flow control forced

Examples

This example shows how to enable send flow control:

```
Switch(config-if)# flowcontrol receive on
Switch(config-if)#
```

This example shows how to disable send flow control:

```
Switch(config-if)# flowcontrol send off
Switch(config-if)#
```

This example shows how to set receive flow control to desired:

```
Switch(config-if)# flowcontrol receive desired
Switch(config-if)#
```

Related Commands

Command	Description
interface port-channel	Accesses or creates a port-channel interface.
interface range	Runs a command on multiple ports at the same time.
show flowcontrol	Displays the per-interface status and statistics related to flow control.
show running-config	Displays the running-configuration for a switch.
speed	Configures the interface speed.

hardware statistics

To enable TCAM hardware statistics in your ACLs use the **hardware statistics** command. To disable TCAM hardware statistics, use the **no** form of this command.

hardware statistics

no hardware statistics

Syntax Description

This command has no arguments or keywords.

Defaults

Hardware statistics is disabled.

Command Modes

Global configuration mode

Examples

This example shows how to enable TCAM hardware statistics in your ACLs ace:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip access-list extended myv4
Switch(config-ext-nacl)#permit ip any any
Switch(config-ext-nacl)#hardware statistics
Switch(config-ext-nacl)#end
```

Related Commands

Command	Description
ip access list (refer to Cisco IOS documentation**)**	Creates an IP ACL (Access Control List).
ipv6 access list (refer to Cisco IOS documentation)	Creates an IPv6 ACL.
mac access-list extended	Defines the extended MAC access lists.

hw-module beacon

To control the beacon LED in conjunction with the beacon button, enter the **hw-module beacon** command:

hw-module beacon [on | off]

Syntax Description

on	Turns on the LED.
off	Turns off the LED.

Defaults

none

Command Modes

global configuration

Usage Guidelines

Either press the beacon button on the front side of the switch or enter the **hw-mod beacon** command, so the switch is identifiable when the operator walks around the isle to the back side of the switch. (The LED and the CLI function as switch identifiers when multiple units are present.)

Pressing the blue beacon LED switch toggles the beacon LED state.

Examples

If numerous WS-C4500X-32 chassis are in close proximity and you want to remove a transceiver from one chassis' port 11, you can identify it with the **hw-module beacon on** command:

```
Switch# hw-module beacon on
Switch#
*Feb 16 13:12:24.418: %C4K_IOSMODPORTMAN-6-BEACONTURNEDON: Beacon has been turned on
```

The WS-C4500X-32 whose beacon was turned on is the switch you are looking for.

After you complete the necessary service on a switch with the beacon LED turned on, you should either press the beacon button to turn it off, or enter the **hw-module beacon off** command to turn the LED off.

```
Switch# hw-module beacon off
Switch#
*Feb 16 13:12:18.083: %C4K_IOSMODPORTMAN-6-BEACONTURNEDOFF: Beacon has been turned off
```

hw-module power

To turn the power off on a slot or line module, use the **no hw-module power** command. To turn the power back on, use the **hw-module power** command.

hw-module [**slot** | **module**] *number* **power**

no hw-module [**slot** | **module**] *number* **power**

Syntax Description

slot	(Optional) Specifies a slot on a chassis.
module	(Optional) Specifies a line module.
number	Slot or module number.

Defaults

After a boot up, the power is on.

Command Modes

Global configuration mode

Usage Guidelines

After you enter **no hw-mod mod x power** command and OIR the linecard, the configuratio persists and is valid for any slot in the chassis it is applied to.

Examples

This example shows how to shut off power to a module in slot 5:

```
Switch# no hw-module slot 5 power
Switch#
```

Related Commands

Command	Description
clear hw-module slot password	Clears the password on an intelligent line module.

hw-module system max-queue-limit

To enable a user to change the queue limit for all interfaces globally use the **hw-module system max-queue-limit** command. To cancel the global setting, use the **no** form of the command.

hw-module system max-queue-limit *max-queue-limit*

no hw-module system max-queue-limit *max-queue-limit*

Syntax Description

max-queue-limit	Specifies the queue limit for all interfaces. Valid values are from 1024 to 8184. This parameter must be a multiple of 8.

Defaults

Not enabled by default

Command Modes

Global configuration mode

Usage Guidelines

This command allows you to change the queue limit for all interfaces globally rather than apply a policy with a queue limit to all the interfcaes.

This is a global configuration command. It can be overriden by the per port, per class, **queue-limit** command.

For a standalone supervisor engine, you must reboot the engine after applying this command. For a redundant supervisor engine, you must enter the **redundancy reload shelf** command to enforce a reboot on both the supervisor engines.

Examples

This example shows how to set the queue limit globally to 1024:

```
Switch> enable
Switch# configure terminal
Switch(config)# hw-module system max-queue-limit 1024
Need to reboot to take effect max queue limit
Switch(config)# exit
Switch# reload  (for standalone supervisors)
Switch# redundancy reload shelf (for reduandancy supervisors in SSO mode)
or
Switch# redundancy force-switchover (followed by another redundancy force-switchover, for
reduandancy supervisors in RPR mode
```

instance

To map a VLAN or a set of VLANs to an MST instance, use the **instance** command. To return the VLANs to the common instance default, use the **no** form of this command.

instance *instance-id* {**vlans** *vlan-range*}

no instance *instance-id*

Syntax Description

instance-id	MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.
vlans *vlan-range*	Specifies the number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.

Defaults

Mapping is disabled.

Command Modes

MST configuration mode

Usage Guidelines

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing ones.

Any unmapped VLAN is mapped to the CIST instance.

Examples

This example shows how to map a range of VLANs to instance 2:

```
Switch(config-mst)# instance 2 vlans 1-100
Switch(config-mst)#
```

This example shows how to map a VLAN to instance 5:

```
Switch(config-mst)# instance 5 vlans 1100
Switch(config-mst)#
```

This example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Switch(config-mst)# no instance 2 vlans 40-60
Switch(config-mst)#
```

This example shows how to move all the VLANs mapped to instance 2 back to the CIST instance:

```
Switch(config-mst)# no instance 2
Switch(config-mst)#
```

Related Commands

Command	Description
name	Sets the MST region name.
revision	Sets the MST configuration revision number.

Command	Description
show spanning-tree mst	Displays MST protocol information.
spanning-tree mst configuration	Enters the MST configuration submode.