



# 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](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]**

<b>Syntax Description</b>	<b>keyword 1</b>	(Optional) Specifies a keyword that is needed while applying a macro to an interface.
	<b>keyword 2</b>	(Optional) Specifies a keyword that is needed while applying a macro to an interface.
	<b>keyword 3</b>	(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

---

## Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

## 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
switchport
@

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
	<b>macro apply cisco-desktop</b>	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
	<b>macro apply cisco-phone</b>	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
	<b>macro apply cisco-router</b>	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
	<b>macro apply cisco-switch</b>	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**

## 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

---

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---



---

**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**

---

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

---



---

**Related Commands**

---

Command	Description
<a href="#">aaa accounting system default</a>	Receives the session termination messages after the switch reboots.
<a href="#">start-stop group radius</a>	

---

# 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

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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**

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

**Related Commands**

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

**access-group mode**

# access-group mode

To specify the override modes (for example, VACL overrides PAACL) 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}**

<b>Syntax Description</b>	<b>prefer port</b>	Specifies that the PAACL mode take precedence if PAACLs are configured. If no PAACL features are configured on the port, other features applicable to the interface are merged and applied on the interface.
	<b>prefer vlan</b>	Specifies that the VLAN-based ACL mode take precedence. If no VLAN-based ACL features are configured on the port's VLAN, the PAACL features on the port are applied.
	<b>merge</b>	Merges applicable ACL features before they are programmed into the hardware.

<b>Defaults</b>	PACL override mode
-----------------	--------------------

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	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).
-------------------------	--

<b>Examples</b>	This example shows how to make the PAACL 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
	<b>show access-group mode interface</b>	Displays the ACL configuration on a Layer 2 interface.
	<b>show ip interface</b> (refer to Cisco IOS documentation)	Displays the IP interface configuration.
	<b>show mac access-group interface</b>	Displays the ACL configuration on a Layer 2 interface.

---

 access-list hardware capture mode

# 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}**

<b>Syntax Description</b>	<b>global</b>	Specifies the capture of control packets globally on all VLANs.
	<b>vlan</b>	Specifies the capture of control packets on a specific VLAN.

---

**Defaults** The control packets are globally captured.

---

**Command Modes** Global configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(40)SG	Support for this command was introduced on the Catalyst 4500 series switch.

---

**Usage Guidelines** This command is not supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis. 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**

# 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}**

<b>Syntax Description</b>	<b>packed</b> 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. <b>scattered</b> 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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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**

# 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	<b>feature</b> Specifies adjustment of region balance for ACLs. <b>qos</b> Specifies adjustment of region balance for QoS. <b>input</b> Specifies adjustment of region balance for input ACL and QoS. <b>output</b> Specifies adjustment of region balance for output ACL and QoS. <b>balance bal-num</b> 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

Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

**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

<b>drop</b>	Sets the action to drop packets.
<b>forward</b>	Sets the action to forward packets to their destination.

---



---

## Defaults

This command has no default settings.

---

## Command Modes

VLAN access-map mode

---

## Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---



---

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

---

**active**

# 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

Command History	Release	Modification
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

**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
	<a href="#">destination address</a>	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	<a href="#">destination message-size-limit bytes</a>	Configures a maximum destination message size for the destination profile.
	<a href="#">destination preferred-msg-format</a>	Configures a preferred message format.
	<a href="#">destination transport-method</a>	Enables the message transport method.

# 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<b>exit</b> (refer to Cisco IOS documentation)	Closes an active terminal session by logging off the switch.
	<b>reset</b>	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.
	<b>show vlan</b>	Displays VLAN information.

**■ apply**

Command	Description
<b>shutdown vlan</b> (refer to Cisco IOS documentation)	Shuts down VLAN switching.
<b>vtp (global configuration mode)</b>	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***

<b>Syntax Description</b>	<i>name</i> Specifies the access control list name.	
<b>Defaults</b>	This command has no default settings.	
<b>Command Modes</b>	Global configuration mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
<b>Examples</b>	This example shows how to define an ARP access list named static-hosts:  Switch(config)# <b>arp access-list static-hosts</b> Switch(config)#	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>deny</b></a>	Denies an ARP packet based on matches against the DHCP bindings.
	<a href="#"><b>ip arp inspection filter vlan</b></a>	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.
	<a href="#"><b>permit</b></a>	Permits an ARP packet based on matches against the DHCP bindings.

**attach module**

# attach module

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

**attach module mod**

<b>Syntax Description</b>	<i>mod</i> Target module for the command.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	<p>This command applies only to the Access Gateway Module on Catalyst 4500 series switches.</p> <p>The valid values for <i>mod</i> 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.</p> <p>When you execute the <b>attach module mod</b> command, the prompt changes to <b>Gateway#</b>.</p> <p>This command is identical in the resulting action to the <b>session module mod</b> and the <b>remote login module mod</b> commands.</p>
-------------------------	---

<b>Examples</b>	<p>This example shows how to remotely log in to an Access Gateway Module:</p> <pre>Switch# attach module 5 Attaching console to module 5 Type 'exit' at the remote prompt to end the session  Gateway&gt;</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">remote login module</a>	Remotely connects to a specific module.
	<a href="#">session module</a>	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**

<b>Syntax Description</b>	<b>both</b> Enables bidirectional control on the port. <b>in</b> Enables unidirectional control on the port.
---------------------------	---

<b>Command Default</b>	both
------------------------	------

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SG	Support for this command was introduced.

<b>Usage Guidelines</b>	The <b>authentication control-direction</b> 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.

**■ authentication control-direction**

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**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show authentication</b></a>	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**

<b>Syntax Description</b>	<i>milliseconds</i>	Specifies the recovery delay period in milliseconds to wait to reinitialize a critical port when an unavailable RADIUS server becomes available. The range is 1 to 10000 milliseconds.
---------------------------	---------------------	--

<b>Command Default</b>	10000 milliseconds
------------------------	--------------------

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SG	Support for this command was introduced.

<b>Usage Guidelines</b>	The <b>authentication critical recovery delay</b> 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.

<b>Examples</b>	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)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show authentication</b>	Displays Authentication Manager information.

---

 authentication event

## 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]}
authentication event no-response action authorize vlan vlan}}
no authentication event {fail} | {server {alive | dead}} | {no-response}
```

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

Command Default	The default settings are as follows: <ul style="list-style-type: none"> <li>The <i>count</i> is 2 by default.</li> <li>The current authentication method is retried indefinitely (and fails each time) until the AAA server becomes reachable.</li> </ul>
-----------------	---

Command Modes	Interface configuration mode
---------------	------------------------------

Command History	Release	Modification
	12.2(50)SG	Support for this command was introduced.

Usage Guidelines	The <b>authentication event fail</b> command replaces the following dot1x commands, which are deprecated in Cisco IOS Release 12.2(50)SG and later releases: <ul style="list-style-type: none"> <li>[no] <b>dot1x auth-fail max-attempts count</b></li> <li>[no] <b>dot1x auth-fail vlan vlan</b></li> </ul>
------------------	--

The **authentication event fail** command is supported only for dot1x to signal authentication failures. By default, this type of failure causes the authentication method to be retried. You can configure to either authorize the port in the configured VLAN or 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 dot1x 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 dot1x 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
<a href="#">show authentication</a>	Displays Authentication Manager information.

---

 authentication fallback

# 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***

---

<b>Syntax Description</b>	<i>profile</i>	The fallback profile name to use when failing over to WebAuth (maximum of 200 characters).
---------------------------	----------------	--

---

<b>Command Default</b>	Disabled
------------------------	----------

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SG	Support for this command was introduced.

---

<b>Usage Guidelines</b>	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.

---

<b>Examples</b>	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)#

```

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show authentication</b>	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	<b>single-host</b>	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.
	<b>multi-auth</b>	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.
	<b>multi-domain</b>	Specifies the session based on a combination of MAC address and domain, with the restriction that only one MAC is allowed per domain.
	<b>multi-host</b>	Specifies the session as an interface session, but allows more than one client on the port.
	<b>open</b>	(Optional) Configures the host-mode with open policy on the port.

**Command Default** This command has no default settings.

**Command Modes** Interface configuration mode

Command History	Release	Modification
	12.2(50)SG	Support for this command was introduced.

**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.

**■ authentication host-mode**

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**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show authentication</b></a>	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

Command History	Release	Modification
	12.2(50)SG	Support for this command was introduced.

**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.

**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
<a href="#">show authentication</a>	Displays Authentication Manager information.

**■ authentication order**

# 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**

<b>Syntax Description</b>	<i>method1</i>	Authentication method to be attempted. The valid values are as follows: <ul style="list-style-type: none"> <li>• <b>dot1x</b>—Adds the dot1x authentication method.</li> <li>• <b>mab</b>—Adds the MAB authentication method.</li> <li>• <b>webauth</b>—Adds the WebAuth authentication method.</li> </ul>
	<i>method2</i>	(Optional) Authentication method to be attempted. The valid values are as follows: <ul style="list-style-type: none"> <li>• <b>dot1x</b>—Adds the dot1x authentication method.</li> <li>• <b>mab</b>—Adds the MAB authentication method.</li> <li>• <b>webauth</b>—Adds the WebAuth authentication method.</li> </ul>
	<i>method3</i>	

**Command Default** The default order is dot1x, MAB, then WebAuth.

**Command Modes** Interface configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SG	Support for this command was introduced.

**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)#{/pre>
```

---

**Related Commands**

Command	Description
<a href="#">show authentication</a>	Displays Authentication Manager information.

---

**■ authentication periodic**

# 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

---

Command History	Release	Modification
	12.2(50)SG	Support for this command was introduced.

---

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

**[no] dot1x reauthentication**

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
<a href="#">authentication timer</a>	Configures the authentication timer.
<a href="#">show authentication</a>	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**

<b>Syntax Description</b>	<b>auto</b> (Optional) Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state. <b>force-authorized</b> (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 <b>force-authorized</b> keyword is the default. <b>force-unauthorized</b> (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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SG	Support for this command was introduced.

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

**[no] dot1x port-control [auto | force-authorized | force-unauthorized]**

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.

**■ authentication port-control**

- 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**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show authentication</b></a>	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**

<b>Syntax Description</b>	<i>method1</i>	Authentication method to be attempted. The valid values are as follows: <ul style="list-style-type: none"> <li>• <b>dot1x</b>—Adds the dot1x authentication method.</li> <li>• <b>mab</b>—Adds the MAB authentication method.</li> <li>• <b>webauth</b>—Adds the Webauth authentication method.</li> </ul>
	<i>method2</i> <i>method3</i>	(Optional) Authentication method to be attempted. The valid values are as follows: <ul style="list-style-type: none"> <li>• <b>dot1x</b>—Adds the dot1x authentication method.</li> <li>• <b>mab</b>—Adds the MAB authentication method.</li> <li>• <b>webauth</b>—Adds the Webauth authentication method.</li> </ul>

**Command Default** The default order is dot1x, MAB, then webauth.

**Command Modes** Interface configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SG	Support for this command was introduced.

**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.

**■ authentication priority****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 weauth
Switch(config-if)#{/pre}
```

**Related Commands**

Command	Description
<a href="#"><b>authentication order</b></a>	Specifies the order in which authentication methods should be attempted for a client on an interface.
<a href="#"><b>show authentication</b></a>	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} }
```

<b>Syntax Description</b>	<b>inactivity</b> <i>value</i> <b>reauthenticate</b> <b>server</b> <b>reauthenticate</b> <i>value</i> <b>restart</b> <i>value</i>	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. <b>Note</b> 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. 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). Specifies the amount of time in seconds after which an automatic reauthentication is initiated. Range is 1 to 65535. Default is 3600. 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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SG	Support for this command was introduced.

**Usage Guidelines** Reauthentication only occurs if it is enabled on the interface.

The **authentication timer reauthenticate** *value* command replaces the following dot1x command that is deprecated in Cisco IOS Release 12.2(50)SG and later releases:

```
[no] dot1x timeout {reauth-period seconds | quiet-period seconds | tx-period seconds |
supp-timeout seconds | server-timeout seconds}
```

**authentication timer****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**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show authentication</b></a>	Displays Authentication Manager information.

## 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	<b>cisco-phone</b> Connects the interface to a Cisco IP phone and automatically configures QoS for VoIP. The CoS labels of incoming packets are trusted only when the telephone is detected. <b>trust</b> 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

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

Use the **trust** keyword on the ports that are connected to the interior of the network. Because it is assumed that the traffic has already been classified by the other edge devices, 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 old 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.

**auto qos voip**

- 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 if 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. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

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 on Supervisor Engines other than a Supervisor Engine 6-E:

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
Switch(config-if)#
00:00:56:qos
00:00:57:qos map cos 3 to dscp 26
00:00:57:qos map cos 5 to dscp 46
00:00:58:qos map dscp 32 to tx-queue 1
00:00:58:qos dbl
00:01:00:policy-map autoqos-voip-policy
00:01:00: class class-default
00:01:00: dbl
00:01:00:interface GigabitEthernet1/1
00:01:00: qos trust cos
00:01:00: tx-queue 3
00:01:00: priority high
00:01:00: shape percent 33
00:01:00: service-policy output autogos-voip-policy
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-phone
Switch(config-if)#
00:00:55:qos
00:00:56:qos map cos 3 to dscp 26
00:00:57:qos map cos 5 to dscp 46
00:00:58:qos map dscp 32 to tx-queue 1
00:00:58:qos dbl
00:00:59:policy-map autoqos-voip-policy
```

```

00:00:59: class class-default
00:00:59: dbl
00:00:59:interface GigabitEthernet1/1
00:00:59: qos trust device cisco-phone
00:00:59: qos trust cos
00:00:59: tx-queue 3
00:00:59: priority high
00:00:59: shape percent 33
00:00:59: bandwidth percent 33
00:00:59: service-policy output autoqos-voip-policy

```

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled on an interface on a Supervisor Engine 6-E:

```

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

**auto-sync**

## 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	<b>startup-config</b> Specifies automatic synchronization of the startup configuration.
<b>config-register</b>	Specifies automatic synchronization of the configuration register configuration.
<b>bootvar</b>	Specifies automatic synchronization of the BOOTVAR configuration.
<b>standard</b>	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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).

**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 config-register
Switch (config-r-mc)#[/pre]
```

Related Commands	Command	Description
	<b>redundancy</b>	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**

<b>Syntax Description</b>	<b>bandwidth-kbps</b> Amount of bandwidth in kbps assigned to the class. The range is 32 to 16000000. <b>percent percent</b> Percentage of available bandwidth assigned to the parent class. The range is 1 to 100. <b>remaining percent percent</b> 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 priority queuing class is not rate-limited.
---------------------------	---

**Defaults** No bandwidth is specified.

**Command Modes** Policy-map class configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.

**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.

**bandwidth**

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
	<b>class</b>	Specifies the name of the class whose traffic policy you want to create or change.
	<b>dbl</b>	Enables active queue management on a transmit queue used by a class of traffic.
	<b>policy-map</b>	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.
	<b>priority</b>	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.
	<b>service-policy (policy-map class)</b>	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	<b>shape (class-based queueing)</b>	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
	<b>show policy-map</b>	Displays information about the policy map.

**call-home (global configuration)**

# 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

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis.

**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 shows 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) #
```

**call-home (global configuration)**

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
	<b>alert-group</b> (refer to Cisco IOS documentation)	Enables an alert group.
	<b>profile</b> (refer to Cisco IOS documentation)	Enters call-home profile configuration mode.
	<b>show call-home</b>	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	
<b>output-analysis</b> “ <i>show-command</i> ”	Sends the output of the specified CLI show command for analysis. The <i>show</i> command must be contained in quotes (“ ”).
<b>config-sanity</b>	Specifies the type of report requested. Based on this keyword, the output of a predetermined set of commands such as the <b>show running-config all</b> , <b>show version</b> , and <b>show module</b> (standalone) or <b>show module switch all</b> (VS system) commands, is sent to Cisco for analysis.
<b>bugs-list</b>	
<b>command-reference</b>	
<b>product-advisory</b>	
<b>profile</b> <i>name</i>	(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.
<b>ccoid</b> <i>user-id</i>	(Optional) Specifies the identifier of a registered Smart Call Home user. If a <i>user-id</i> is specified, the resulting analysis report is sent to the e-mail address of the registered user. If no <i>user-id</i> 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

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis.

**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.

**call-home request****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**

<a href="#">call-home (global configuration)</a>	Enters call home configuration mode.
<a href="#">call-home send</a>	Sends a CLI command to be executed, with the command output to be sent by e-mail.
<a href="#">call-home send alert-group</a>	Sends a specific alert group message.
<a href="#">service call-home</a> (refer to Cisco IOS documentation)	Enables or disables Call Home.
<a href="#">show call-home</a>	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}
```

<b>Syntax Description</b>	<p><b>"cli-command"</b>      Specifies a CLI command to be executed. The command output is sent by e-mail.</p> <p><b>email email-addr</b>      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.</p> <p><b>service-number SR</b>      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.</p>
---------------------------	---

**Command Default**      This command has no default settings.

**Command Modes**      Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis

**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
```

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

**call-home send alert-group**

# 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	
<b>configuration</b>	Sends the configuration alert-group message to the destination profile.
<b>diagnostic module</b> <i>number</i>	Sends the diagnostic alert-group message to the destination profile for a specific module number.
<b>inventory</b>	Sends the inventory call-home message.
<b>profile</b> <i>profile-name</i>	(Optional) Specifies the name of the destination profile.

**Command Default** This command has no default settings.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis.

**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**

<a href="#">call-home (global configuration)</a>	Enters call home configuration mode.
<a href="#">call-home test</a>	Sends a call-home test message that you define.
<a href="#">service call-home</a> (refer to Cisco IOS documentation)	Enables or disables Call Home.
<a href="#">show call-home</a>	Displays call-home configuration information.

**call-home test**

# 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*

<b>Syntax Description</b>	<i>"test-message"</i> (Optional) Test message text. <b>profile</b> <i>profile-name</i> Specifies the name of the destination profile.
---------------------------	--

**Command Default** This command has no default settings.

**Command Modes** Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis

**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
```

<b>Related Commands</b>	<b>call-home (global configuration)</b> Enters call home configuration mode.
	<b>call-home send alert-group</b> Sends a specific alert group message.
	<b>service call-home</b> (refer to Cisco IOS documentation) Enables or disables Call Home.
	<b>show call-home</b> 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

<b>number</b>	Specifies the channel-group number; valid values are from 1 to 64.
<b>mode</b>	Specifies the EtherChannel mode of the interface.
<b>active</b>	Enables LACP unconditionally.
<b>on</b>	Forces the port to channel without PAgP.
<b>auto</b>	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.
<b>non-silent</b>	(Optional) Used with the auto or desirable mode when traffic is expected from the other device.
<b>passive</b>	Enables LACP only if an LACP device is detected.
<b>desirable</b>	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

## Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(13)EW	Support for LACP was added.

## 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.

**channel-group**

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
<b>interface port-channel</b>	Accesses or creates a port-channel interface.
<b>show interfaces port-channel</b> (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}**

<b>Syntax Description</b>	<b>lacp</b> Enables LACP to manage channeling. <b>pagp</b> Enables PAgP to manage channeling.				
<b>Defaults</b>	PAgP				
<b>Command Modes</b>	Interface configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th><b>Release</b></th><th><b>Modification</b></th></tr> </thead> <tbody> <tr> <td>12.1(13)EW</td><td>Support for this command was introduced on the Catalyst 4500 series switches.</td></tr> </tbody> </table>	<b>Release</b>	<b>Modification</b>	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.
<b>Release</b>	<b>Modification</b>				
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.				
<b>Usage Guidelines</b>	<p>This command is not supported on systems that are configured with a Supervisor Engine I. You can also select the protocol using the <a href="#">channel-group</a> command.</p> <p>If the interface belongs to a channel, the <b>no</b> form of this command is rejected.</p> <p>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.</p> <p>You can manually configure a switch with PAgP on one side and LACP on the other side in the <b>on</b> mode.</p> <p>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 <b>channel-protocol</b> command to restrict anyone from selecting a mode that is not applicable to the selected protocol.</p> <p>Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).</p> <p>For a complete list of guidelines, refer to the “Configuring EtherChannel” section of the <i>Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide</i>.</p>				
<b>Examples</b>	<p>This example shows how to select LACP to manage channeling on the interface:</p> <pre>Switch(config-if)# channel-protocol lacp Switch(config-if)#</pre>				

**channel-protocol**

Related Commands	Command	Description
	<a href="#">channel-group</a>	Assigns and configures an EtherChannel interface to an EtherChannel group.
	<a href="#">show etherchannel</a>	Displays EtherChannel information for a channel.

# 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*

<b>Syntax Description</b>	<i>class-name</i> Name of the predefined traffic class for which you want to configure or modify a traffic policy. The class was previously created through the <b>class-map</b> <i>class-map-name</i> global configuration command.
---------------------------	--

<b>Defaults</b>	No classes are defined; except for the class-default.
-----------------	---

<b>Command Modes</b>	Policy-map configuration mode
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switches.

<b>Usage Guidelines</b>	Before using the <b>class</b> command, you must create a class map for matching packets to the class by using the <b>class-map</b> global configuration command. You also must use the <b>policy-map</b> 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 <b>class</b> 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 <b>class-map</b> global configuration command. You attach the policy map to a port by using the <b>service-policy (interface configuration)</b> 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. This command is available on the Supervisor Engine 6-E and the Catalyst 4900M chassis.
- **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. The two-rate traffic policer is supported on a Supervisor Engine 6-E and the Catalyst 4900M chassis.

- **priority** Enables the strict priority queue for a class of traffic. For more information, see the **priority** command. This command is supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.
- **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. This command is supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.
- **trust** Defines a trust state for a traffic class. For more information, see the **trust** command. This command is not supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.

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 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
	<b>bandwidth</b>	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port.
	<b>class-map</b>	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
	<b>dbl</b>	Enables active queue management on a transmit queue used by a class of traffic.
	<b>police</b>	Configures the Traffic Policing feature.
	<b>police (percent)</b>	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
	<b>police rate</b>	Configures single- or dual-rate policer.
	<b>policy-map</b>	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	<b>priority</b>	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.
	<b>service-policy (interface configuration)</b>	Attaches a policy map to an interface.
	<b>service-policy (policy-map class)</b>	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	<b>set</b>	Marks IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet.
	<b>shape (class-based queueing)</b>	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
	<b>show policy-map</b>	Displays information about the policy map.
	<b>trust</b>	Defines a trust state for traffic classified through the <b>class</b> 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	<b>match-all</b> (Optional) Perform a logical-AND of all matching under this class map. All criteria in the class map must be matched.
	<b>match-any</b> (Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria in the class map must be matched.
	<i>class-map-name</i> Name of the class map.

Defaults	No class maps are defined. If neither the <b>match-all</b> nor the <b>match-any</b> keyword is specified, the default is <b>match-all</b> .
----------	--

Command Modes	Global configuration mode
---------------	---------------------------

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switches.

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**

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

**■ clear counters**

# 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}]
```

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

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

<b>Release</b>	<b>Modification</b>
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended VLAN addresses was added.

## 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
<b>show interface counters</b> (refer to Cisco IOS documentation)	Displays interface counter information.

---

■ **clear energywise neighbors**

# clear energywise neighbors

Use the **clear energywise neighbors** privileged EXEC command to delete the EnergyWise neighbor tables.

## **clear energywise neighbors**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(52)SG	This command was introduced.

**Examples** This example shows how to delete the neighbor tables:

```
Switch# clear energywise neighbors
Cleared all non static energywise neighbors
```

You can verify that the tables were deleted by entering the **show energywise neighbors** privileged EXEC command.



**Note** The **clear energywise neighbors** command clears all discovered neighbors.

Related Commands	Command	Description
	<a href="#">show energywise</a>	Displays the EnergyWise settings and status of the entity and PoE ports.

# clear errdisable

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

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

## Syntax Description

<b>interface</b> <i>name</i>	Specifies the interface of the VLAN(s) to recover.
<b>vlan</b>	Specifies all VLANs on the interface be recovered.
<b>range</b>	(Optional) Specifies the VLAN range to be recovered.

## Defaults

This command has no default settings.

## Command Modes

Global configuration mode

## Command History

<b>Release</b>	<b>Modification</b>
12.2(52)SG	Added support for per-VLAN error-disable detection.

## 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 interface:

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

## Related Commands

<b>Command</b>	<b>Description</b>
<a href="#">errdisable detect</a>	Enables error-disable detection.
<a href="#">show errdisable detect</a>	Displays the error-disable detection status.
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in error-disabled state.
<a href="#">switchport port-security</a>	Enables port security on an interface.

---

■ **clear hw-module slot password**

## 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**

<b>Syntax Description</b>	<i>slot_num</i> Slot on a line module.
---------------------------	--

<b>Defaults</b>	The password is not cleared.
-----------------	------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	You only need to change the password once unless the password is reset.
-------------------------	---

<b>Examples</b>	This example shows how to clear the password from slot 5 on a line module:
	Switch# <b>clear hw-module slot 5 password</b> Switch#

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>hw-module power</b></a>	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** On a Catalyst 4500 series switch, 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

---

## Command History

Release	Modification
---------	--------------

12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
------------	---

---



---

## 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
---------	-------------

<a href="#">show interfaces status</a>	Displays the interface status.
--	--------------------------------

---

---

■ **clear interface vlan**

## clear interface vlan

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

**clear interface vlan *number***

---

<b>Syntax Description</b>	<i>number</i> Number of the VLAN interface; valid values are from 1 to 4094.
---------------------------	--

---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

---

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

---

<b>Examples</b>	This example shows how to clear the hardware logic from a specific VLAN:
	<pre>Switch# <b>clear interface vlan 5</b> Switch#</pre>

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>show interfaces status</b></a>	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***

<b>Syntax Description</b>	<i>access-list</i> 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.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Examples</b>	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**

## 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

---

<b>Release</b>	<b>Modification</b>
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---



---

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

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

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">arp access-list</a>	Defines an ARP access list or adds clauses at the end of a predefined list.
	<a href="#">show ip arp inspection log</a>	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*]**

<b>Syntax Description</b>	<b>vlan <i>vlan-range</i></b> (Optional) Specifies the VLAN range.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">arp access-list</a>	Defines an ARP access list or adds clauses at the end of a predefined list.
	<a href="#">clear ip arp inspection log</a>	Clears the status of the log buffer.
	<a href="#">show ip arp inspection log</a>	Displays the status of the log buffer.

---

■ **clear ip dhcp snooping binding**

## 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**

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

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC mode

---

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(44)SG	Support for this command was introduced on the Catalyst 4500 series switch.

---

**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
	<a href="#">ip dhcp snooping</a>	Globally enables DHCP snooping.
	<a href="#">ip dhcp snooping binding</a>	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
	<a href="#">ip dhcp snooping information option</a>	Enables DHCP option 82 data insertion.
	<a href="#">ip dhcp snooping trust</a>	Enables DHCP snooping on a trusted VLAN.
	<a href="#">ip dhcp snooping vlan</a>	Enables DHCP snooping on a VLAN or a group of VLANs.
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.

---

■ **clear ip dhcp snooping database**

## 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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**Examples** This example shows how to clear the DHCP binding database:

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip dhcp snooping</a>	Globally enables DHCP snooping.
	<a href="#">ip dhcp snooping binding</a>	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
	<a href="#">ip dhcp snooping information option</a>	Enables DHCP option 82 data insertion.
	<a href="#">ip dhcp snooping trust</a>	Enables DHCP snooping on a trusted VLAN.
	<a href="#">ip dhcp snooping vlan</a>	Enables DHCP snooping on a VLAN or a group of VLANs.
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**Examples** This example shows how to clear the DHCP binding database:

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

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

---

■ **clear ip igmp group**

## 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}]
```

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

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC mode

---

**Command History**

<b>Release</b>	<b>Modification</b>
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

**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
	<b>ip host</b> (refer to Cisco IOS documentation)	Defines a static host name-to-address mapping in the host cache.
	<b>show ip igmp groups</b> (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 <b>show ip igmp groups</b> command in EXEC mode.
	<b>show ip igmp interface</b>	Displays the information about the IGMP-interface status and configuration.

---

■ **clear ip igmp snooping membership**

## 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*]**

<b>Syntax Description</b>	<b>vlan <i>vlan_id</i></b> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	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 <b>clear ip igmp snooping statistics vlan</b> command.
-------------------------	---

<b>Examples</b>	This example shows how to display the IGMP snooping statistics for VLAN 25:
	<pre>Switch# clear ip igmp snooping membership vlan 25 Switch#</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp snooping vlan explicit-tracking</a>	Enables per-VLAN explicit host tracking.
	<a href="#">show ip igmp snooping membership</a>	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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<a href="#">show ip mfib</a>	Displays all active Multicast Forwarding Information Base (MFIB) routes.

---

■ **clear ip mfib fastdrop**

## 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

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<a href="#">ip mfib fastdrop</a>	Enables MFIB fast drop.
	<a href="#">show ip mfib fastdrop</a>	Displays all currently active fast-drop entries and shows whether fast drop is enabled.

# 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**

<b>Syntax Description</b>	<i>channel-group</i> (Optional) Channel-group number; valid values are from 1 to 64.	
<b>Defaults</b>	This command has no default settings.	
<b>Command Modes</b>	Privileged EXEC mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.
<b>Usage Guidelines</b>	<p>This command is not supported on systems that are configured with a Supervisor Engine I.</p> <p>If you do not specify a channel group, all channel groups are cleared.</p> <p>If you enter this command for a channel group that contains members in PAgP mode, the command is ignored.</p>	
<b>Examples</b>	<p>This example shows how to clear the statistics for a specific group:</p> <pre>Switch# clear lacp 1 counters Switch#</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show lacp</a>	Displays LACP information.

---

■ **clear mac-address-table**

## 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}
```

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

---

**Defaults** This command has no default settings.

---

**Command Modes** Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.
	12.2(31)SG	Support for MAC address notification global counters added.

---

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

---

■ **clear mac-address-table dynamic**

## 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]**

<b>Syntax Description</b>	<b>address mac_addr</b> (Optional) Specifies the MAC address. <b>interface interface</b> (Optional) Specifies the interface and clears the entries associated with it; valid values are <b>FastEthernet</b> and <b>GigabitEthernet</b> . <b>vlan vlan_id</b> (Optional) Specifies the VLANs; valid values are from 1 to 4094.
---------------------------	---

---

**Defaults** This command has no default settings.

---

**Command Modes** Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

---

**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#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>mac-address-table aging-time</b></a>	Configures the aging time for entries in the Layer 2 table.
	<a href="#"><b>main-cpu</b></a>	Enters the main CPU submode and manually synchronize the configurations on the two supervisor engines.
	<a href="#"><b>show mac-address-table address</b></a>	Displays the information about the MAC-address table.

# clear pagp

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

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

<b>Syntax Description</b>	<b>group-number</b> Channel-group number; valid values are from 1 to 64. <b>counters</b> Clears traffic filters.
---------------------------	---

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>show pagp</b></a>	Displays information about the port channel.

**■ clear port-security**

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

---

**Command History**

Release	Modification
12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.
12.2(31)SG	Add support for sticky port security.

---

**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
	<a href="#">show port-security</a>	Displays information about the port-security setting.
	<a href="#">switchport port-security</a>	Enables port security on an interface.

**■ clear qos**

# 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

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

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.



### Note

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
	<a href="#">show qos</a>	Displays QoS information.

**■ clear vlan counters**

# 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**

<b>Syntax Description</b>	<i>vlan-id</i> (Optional) VLAN number; see the “Usage Guidelines” section for valid values.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.

<b>Usage Guidelines</b>	If you do not specify a <i>vlan-id</i> value; the software-cached counter values for all the existing VLANs are cleared.
-------------------------	--

<b>Examples</b>	This example shows how to clear the software-cached counter values for a specific VLAN:
	<pre>Switch# clear vlan 10 counters Clear "show vlan" counters on this vlan [confirm] y Switch#</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show vlan counters</a>	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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.

**Examples** This example shows how to clear the VMPS statistics:

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

Related Commands	Command	Description
	<a href="#">show vmps</a>	Displays VMPS information.
	<a href="#">vmps reconfirm (privileged EXEC)</a>	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

**control-plane**

## 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 named “system-cpp-policy” is attached.

**Command Modes** Global configuration mode

Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced.

**Usage Guidelines** This command is not supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.

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

**counter**

# counter

To assign a counter set to a switch port, use the **counter** command. To remove a counter assignment, use the **no** form of this command.

**counter**

**no counter**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** This command has no default setting.

---

**Command Modes** Interface configuration mode

---

Command History	Release	Modification
	12.2(40)SG	Support for this command was introduced.

---

**Usage Guidelines** This command is supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.

The total number of switch ports that can have transmit and receive counters is 4096.

When a Layer 3 port with counter assigned is changed to a Layer 2 port or removed, the hardware counters are freed. This action is similar to entering the **no counter** command.

---

**Examples** This example shows how to assign a counter set to a switch port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 20
Switch(config-if)# counter
Switch(config-if)# end
Switch#
```

**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

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(40)SG	Added support for the Supervisor Engine 6E.

**Usage Guidelines** The semantics of the DBL configuration is similar to the (W)RED 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
	<b>bandwidth</b>	Creates a signaling class structure that can be referred to by its name.
	<b>class</b>	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.

Command	Description
<a href="#">policy-map</a>	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
<a href="#">service-policy (policy-map class)</a>	Creates a service policy that is a quality of service (QoS) policy within a policy map.
<a href="#">show policy-map</a>	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**

<b>Syntax Description</b>	<b>ipc</b> (Optional) Displays the IPC entries in the adjacency database.
---------------------------	---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Examples</b>	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
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#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>undebug adjacency</b> (same as no debug adjacency)	Disables debugging output.

**debug backup**

## 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

---

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---



---

**Examples** This example shows how to debug the backup events:

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

---

Related Commands	Command	Description
	<b>undebug backup</b> (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}
```

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

**Defaults**              This command has no default settings.

**Command Modes**        Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

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

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>debug interface</b>	Abbreviates the entry of the <b>debug condition interface</b> command.
	<b>undebug condition interface</b>	Disables interface related activities. (same as no debug condition interface)

■ **debug condition standby**

## 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}
```

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

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

**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
<b>undebbug condition standby</b> (same as no debug condition standby)	Disables debugging output.

---

 ■ **debug condition vlan**

## 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}**

---

<b>Syntax Description</b>	<i>vlan_id</i> Number of the VLAN; valid values are from 1 to 4096.
---------------------------	---

---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

---

<b>Usage Guidelines</b>	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 <b>n</b> to abort the removal or <b>y</b> to proceed with the removal. If you remove the only condition set, it could result in the display of an excessive number of messages.
-------------------------	--

---

<b>Examples</b>	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
	<b>undebug condition vlan</b> (same as no debug condition vlan)	Disables debugging output.

**debug dot1x**

## 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}**

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

<b>Defaults</b>	
Debugging is disabled.	
<b>Command Modes</b>	
Privileged EXEC mode	
<b>Command History</b>	
<b>Release</b>	<b>Modification</b>
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Examples</b>	
This example shows how to enable the 802.1X debugging for all conditions:	

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

<b>Related Commands</b>	
<b>Command</b>	<b>Description</b>
<a href="#">show dot1x</a>	Displays dot1x information.
<b>undebug dot1x</b> (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	<b>all</b> (Optional) Displays all EtherChannel debug messages. <b>detail</b> (Optional) Displays the detailed EtherChannel debug messages. <b>error</b> (Optional) Displays the EtherChannel error messages. <b>event</b> (Optional) Debugs the major EtherChannel event messages. <b>idb</b> (Optional) Debugs the PAgP IDB messages. <b>linecard</b> (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

## Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

## 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#
```

**■ debug etherchnl**

This example shows how to disable the debugging:

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

Related Commands	Command	Description
	<b>undebug etherchnl</b> (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	<b>FastEthernet</b>	Limits the debugging to Fast Ethernet interfaces.
<i>mod/port</i>		Number of the module and port.
<b>GigabitEthernet</b>		Limits the debugging to Gigabit Ethernet interfaces.
<b>null</b>		Limits the debugging to null interfaces; the only valid value is 0.
<b>port-channel</b> <i>interface-num</i>		Limits the debugging to port-channel interfaces; valid values are from 1 to 64.
<b>vlan</b> <i>vlan_id</i>		Specifies the VLAN interface number; valid values are from 1 to 4094.

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

**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
	<b>debug condition interface</b>	Limits the debugging output of interface-related activities.
	<b>undebug etherchnl</b> (same as no <b>debug etherchnl</b> )	Disables debugging output.

**debug ipc**

## 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	<b>all</b> Enables all IPC debugging. <b>errors</b> Enables the IPC error debugging. <b>events</b> Enables the IPC event debugging. <b>headers</b> Enables the IPC header debugging. <b>packets</b> Enables the IPC packet debugging. <b>ports</b> Enables the debugging of the creation and deletion of ports. <b>seats</b> Enables the debugging of the creation and deletion of nodes.
--------------------	---

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<b>undebug ipc</b> (same as <b>no debug ipc</b> )	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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

**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
	<a href="#"><b>debug ip dhcp snooping packet</b></a>	Debugs the DHCP snooping messages.

---

```
■ debug ip dhcp snooping packet
```

## 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

---

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

**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
	<a href="#">debug ip dhcp snooping event</a>	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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
<a href="#">ip dhcp snooping</a>	Globally enables DHCP snooping.
<a href="#">ip dhcp snooping limit rate</a>	Enables DHCP option 82 data insertion.
<a href="#">ip dhcp snooping trust</a>	Enables DHCP snooping on a trusted VLAN.
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding entries.

**debug lacp**

## 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	<b>all</b> (Optional) Enables all LACP debugging. <b>event</b> (Optional) Enables the debugging of the LACP events. <b>fsm</b> (Optional) Enables the debugging of the LACP finite state machine. <b>misc</b> (Optional) Enables the miscellaneous LACP debugging. <b>packet</b> (Optional) Enables the LACP packet debugging.
--------------------	--

**Defaults** Debugging of LACP activity is disabled.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<b>undebug pagp</b> (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	<b>all</b> Displays all the SPAN debugging messages.
<b>errors</b>	Displays the SPAN error details.
<b>idb-update</b>	Displays the SPAN IDB update traces.
<b>list</b>	Displays the SPAN list tracing and the VLAN list tracing.
<b>notifications</b>	Displays the SPAN notifications.
<b>platform</b>	Displays the SPAN platform tracing.
<b>requests</b>	Displays the SPAN requests.

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<b>undebug monitor</b> (same as no debug monitor)	Disables debugging output.

---

 debug nvram

## 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

---

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---



---

**Examples** This example shows how to debug NVRAM:

```
Switch# debug nvram
NVRAM behavior debugging is on
Switch#
```

---

Related Commands	Command	Description
	<b>undebug nvram</b> (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

<b>all</b>	(Optional) Enables all PAgP debugging.
<b>dual-active</b>	(Optional) Enables the PAgP dual-active debugging.
<b>event</b>	(Optional) Enables the debugging of the PAgP events.
<b>fsm</b>	(Optional) Enables the debugging of the PAgP finite state machine.
<b>misc</b>	(Optional) Enables the miscellaneous PAgP debugging.
<b>packet</b>	(Optional) Enables the PAgP packet debugging.

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

## 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 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
<b>undebug pagp</b> (same as <b>no debug pagp</b> )	Disables debugging output.

---

 debug platform packet protocol lacp

# 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]**

<b>Syntax Description</b>	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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

**Examples** This example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol lacp
Switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>undebbug platform packet protocol lacp</b>	Disables debugging output. (same as no debug platform packet protocol lacp)

# 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]**

<b>Syntax Description</b>	<b>receive</b> (Optional) Enables the platform packet reception debugging functions. <b>transmit</b> (Optional) Enables the platform packet transmission debugging functions. <b>vlan</b> (Optional) Enables the platform packet VLAN debugging functions.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Examples</b>	This example shows how to enable all PM debugging:
	<pre>Switch# debug platform packet protocol pagp Switch#</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>undebug platform packet protocol pagp</b> (same as no debug platform packet protocol pagp)	Disables debugging output.

**debug pm**

## 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

<b>all</b>	Displays all PM debugging messages.
<b>card</b>	Debugs the module-related events.
<b>cookies</b>	Enables the internal PM cookie validation.
<b>etherchnl</b>	Debugs the EtherChannel-related events.
<b>messages</b>	Debugs the PM messages.
<b>port</b>	Debugs the port-related events.
<b>registry</b>	Debugs the PM registry invocations.
<b>scp</b>	Debugs the SCP module messaging.
<b>sm</b>	Debugs the state machine-related events.
<b>span</b>	Debugs the spanning-tree-related events.
<b>split</b>	Debugs the split-processor.
<b>vlan</b>	Debugs the VLAN-related events.
<b>vp</b>	Debugs the virtual port-related events.

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC mode

### Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

### Examples

This example shows how to enable all PM debugging:

```
Switch# debug pm all
Switch#
```

### Related Commands

Command	Description
<b>undebug pm</b> (same as <b>no debug pm</b> )	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

---

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

---

**Examples** This example shows how to enable all PM debugging:

```
Switch# debug port-security  
Switch#
```

---

Related Commands	Command	Description
	<a href="#">switchport port-security</a>	Enables port security on an interface.

---

**debug redundancy**

## debug redundancy

To debug the 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
```

<b>Syntax Description</b>	
<b>errors</b>	Enables the redundancy facility for error debugging.
<b>fsm</b>	Enables the redundancy facility for FSM event debugging.
<b>kpa</b>	Enables the redundancy facility for keepalive debugging.
<b>msg</b>	Enables the redundancy facility for messaging event debugging.
<b>progression</b>	Enables the redundancy facility for progression event debugging.
<b>status</b>	Enables the redundancy facility for status event debugging.
<b>timer</b>	Enables the redundancy facility for timer event debugging.

---

**Defaults** This command has no default settings.

---

**Command Modes** Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).

---

**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	<b>all</b> Displays all the spanning tree debugging messages.
<b>backbonefast</b>	Debugs the BackboneFast events.
<b>bpdu</b>	Debugs the spanningtree BPDU.
<b>bpdu-opt</b>	Debugs the optimized BPDU handling.
<b>etherchannel</b>	Debugs the spanning tree EtherChannel support.
<b>config</b>	Debugs the spanning tree configuration changes.
<b>events</b>	Debugs the TCAM events.
<b>exceptions</b>	Debugs the spanning tree exceptions.
<b>general</b>	Debugs the general spanning tree activity.
<b>ha</b>	Debugs the HA events.
<b>mstp</b>	Debugs the multiple spanning tree events.
<b>pvst+</b>	Debugs the PVST+ events.
<b>root</b>	Debugs the spanning tree root events.
<b>snmp</b>	Debugs the spanning tree SNMP events.
<b>switch</b>	Debugs the switch debug events.
<b>synchronization</b>	Debugs the STP state synchronization events.
<b>uplinkfast</b>	Debugs the UplinkFast events.

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**Examples** This example shows how to debug the spanning-tree PVST+:

```
Switch# debug spanning-tree pvst+
Spanning Tree PVST+ debugging is on
Switch#
```

■ **debug spanning-tree**

Related Commands	Command	Description
	<b>undebug spanning-tree</b> (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**

<b>Syntax Description</b>	<b>detail</b> (Optional) Displays the detailed BackboneFast debugging messages. <b>exceptions</b> (Optional) Enables the debugging of spanning tree BackboneFast exceptions.				
<b>Defaults</b>	This command has no default settings.				
<b>Command Modes</b>	Privileged EXEC mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th><b>Release</b></th><th><b>Modification</b></th></tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td><td>Support for this command was introduced on the Catalyst 4500 series switch.</td></tr> </tbody> </table>	<b>Release</b>	<b>Modification</b>	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
<b>Release</b>	<b>Modification</b>				
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.				
<b>Usage Guidelines</b>	This command is supported only by the supervisor engine and can be entered only from the Catalyst 4500 series switch console.				
<b>Examples</b>	<p>This example shows how to enable the debugging and to display the detailed spanning tree BackboneFast debugging information:</p> <pre>Switch# debug spanning-tree backbonefast detail Spanning Tree backbonefast detail debugging is on Switch#</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><b>undebug spanning-tree backbonefast</b> (same as no debug spanning-tree backbonefast)</td><td>Disables debugging output.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<b>undebug spanning-tree backbonefast</b> (same as no debug spanning-tree backbonefast)	Disables debugging output.
<b>Command</b>	<b>Description</b>				
<b>undebug spanning-tree backbonefast</b> (same as no debug spanning-tree backbonefast)	Disables debugging output.				

---

 ■ debug spanning-tree switch

## 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	
<b>all</b>	Displays all the spanning-tree switch shim debugging messages.
<b>errors</b>	Enables the debugging of switch shim errors or exceptions.
<b>general</b>	Enables the debugging of general events.
<b>pm</b>	Enables the debugging of port manager events.
<b>rx</b>	Displays the received BPDU-handling debugging messages.
<b>decode</b>	Enables the debugging of the decode-received packets of the spanning-tree switch shim.
<b>errors</b>	Enables the debugging of the receive errors of the spanning-tree switch shim.
<b>interrupt</b>	Enables the shim ISR receive BPDU debugging on the spanning-tree switch.
<b>process</b>	Enables the process receive BPDU debugging on the spanning-tree switch.
<b>state</b>	Enables the debugging of the state changes on the spanning-tree port.
<b>tx</b>	Enables the transmit BPDU debugging on the spanning-tree switch shim.
<b>decode</b>	(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
---------------	----------------------

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	This command is supported only by the supervisor engine and can be entered 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
<b>undebug spanning-tree switch</b> (same as <b>no debug spanning-tree switch</b> )	Disables debugging output.

---

■ **debug spanning-tree uplinkfast**

## 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**

---

<b>Syntax Description</b>	<b>exceptions</b> (Optional) Enables the debugging of the spanning tree UplinkFast exceptions.
---------------------------	--

---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

<b>Usage Guidelines</b>	This command is supported only by the supervisor engine and can be entered only from the switch console.
-------------------------	--

---

<b>Examples</b>	This example shows how to debug the spanning tree UplinkFast exceptions:
	<pre>Switch# debug spanning-tree uplinkfast exceptions Spanning Tree uplinkfast exceptions debugging is on Switch#</pre>

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>undebbug spanning-tree uplinkfast</b> (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	<b>badpmcookies</b>	Displays the VLAN manager incidents of bad port manager cookies.
	<b>events</b>	Debugs the VLAN manager events.
	<b>management</b>	Debugs the VLAN manager management of internal VLANs.
	<b>packets</b>	Debugs the packet handling and encapsulation processes.
	<b>registries</b>	Debugs the VLAN manager registries.

**Defaults** This command has no default settings.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<b>undebug sw-vlan</b> (same as no debug sw-vlan)	Disables debugging output.

---

```
■ debug sw-vlan ifs
```

## 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	<b>open</b>	Enables the VLAN manager IFS debugging of errors in an IFS file-open operation.
	<b>read</b>	Debugs the errors that occurred when the IFS VLAN configuration file was open for reading.
	<b>write</b>	Debugs the errors that occurred when the IFS VLAN configuration file was open for writing.
	<b>{1   2   3   4}</b>	Determines the file-read operation. See the “Usage Guidelines” section for information about operation levels.
	<b>write</b>	Debugs the errors that occurred during an IFS file-write operation.

---

**Defaults** This command has no default settings.

---

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

**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
	<b>undebbug sw-vlan ifs</b> (same as no debug sw-vlan ifs)	Disables debugging output.

---

 debug sw-vlan notification

## 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	
<b>accfwdchange</b>	Enables the VLAN manager notification of aggregated access interface STP forward changes.
<b>allowedvlancfgchange</b>	Enables the VLAN manager notification of changes to allowed VLAN configuration.
<b>fwdchange</b>	Enables the VLAN manager notification of STP forwarding changes.
<b>linkchange</b>	Enables the VLAN manager notification of interface link state changes.
<b>modechange</b>	Enables the VLAN manager notification of interface mode changes.
<b>pruningcfgchange</b>	Enables the VLAN manager notification of changes to pruning configuration.
<b>statechange</b>	Enables the VLAN manager notification of interface state changes.

---

**Defaults**

This command has no default settings.

---

**Command Modes**

Privileged EXEC mode

---

**Command History**

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

**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
<b>undebug sw-vlan notification</b> (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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<b>undebbug sw-vlan vtp</b> (same as no debug sw-vlan vtp)	Disables debugging output.

**debug udld**

## 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	<b>events</b> Enables the debugging of UDLD process events as they occur.
	<b>packets</b> 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.
	<b>registries</b> 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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 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
	<b>undebug udld</b> (same as no debug udld)	Disables debugging output.

---

 debug vqpc

## 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]**

<b>Syntax Description</b>	<b>all</b> (Optional) Debugs all the VQP events. <b>cli</b> (Optional) Debugs the VQP command-line interface. <b>events</b> (Optional) Debugs the VQP events. <b>learn</b> (Optional) Debugs the VQP address learning. <b>packet</b> (Optional) Debugs the VQP packets.
---------------------------	---

---

**Defaults** This command has no default settings.

---

**Command Modes** Privileged EXEC mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---

**Examples** This example shows how to enable all VQP debugging:

```
Switch# debug vqpc all
Switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">vmpls reconfirm (privileged EXEC)</a>	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*

<b>Syntax Description</b>	<i>macro-name</i> Name of the interface range macro; up to 32 characters. <i>interface-range</i> List of valid ranges when specifying interfaces; see the “Usage Guidelines” section.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	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*

<b>Examples</b>	This example shows how to create a multiple-interface macro:
-----------------	--

```
Switch(config)# define interface-range macro1 gigabitether 4/1-6, fastether 2/1-5
Switch(config)#

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">interface range</a>	Runs a command on multiple ports at the same time.

**■ deny**

## 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**

<b>request</b>	(Optional) Requests a match for the ARP request. When <b>request</b> is not specified, matching is performed against all ARP packets.
<b>ip</b>	Specifies the sender IP address.
<b>any</b>	Specifies that any IP or MAC address will be accepted.
<b>host sender-ip</b>	Specifies that only a specific sender IP address will be accepted.
<b>sender-ip sender-ip-mask</b>	Specifies that a specific range of sender IP addresses will be accepted.
<b>mac</b>	Specifies the sender MAC address.
<b>host sender-mac</b>	Specifies that only a specific sender MAC address will be accepted.
<b>sender-mac sender-mac-mask</b>	Specifies that a specific range of sender MAC addresses will be accepted.
<b>response</b>	Specifies a match for the ARP responses.
<b>ip</b>	Specifies the IP address values for the ARP responses.
<b>host target-ip</b>	(Optional) Specifies that only a specific target IP address will be accepted.
<b>target-ip target-ip-mask</b>	(Optional) Specifies that a specific range of target IP addresses will be accepted.
<b>mac</b>	Specifies the MAC address values for the ARP responses.
<b>host target-mac</b>	(Optional) Specifies that only a specific target MAC address will be accepted.
<b>target-mac target-mac-mask</b>	(Optional) Specifies that a specific range of target MAC addresses will be accepted.
<b>log</b>	(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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	Deny clauses can be added to forward or drop ARP packets based on some matching criteria.
-------------------------	---

<b>Examples</b>	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
	<a href="#">arp access-list</a>	Defines an ARP access list or adds clauses at the end of a predefined list.
	<a href="#">ip arp inspection filter vlan</a>	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.
	<a href="#">permit</a>	Permits an ARP packet based on matches against the DHCP bindings.

destination address

# 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*}**

<b>Syntax Description</b>	<b>email <i>email-address</i></b>	Specifies the destination e-mail address in 1 to 200 characters.
	<b>http <i>url</i></b>	Specifies the destination HTTP URL in 2 to 200 characters.

**Defaults** This command has no default settings.

**Command Modes** cfg-call-home-profile

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

**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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>destination message-size-limit bytes</b>	Configures a maximum destination message size for the destination profile.
	<b>destination preferred-msg-format</b>	Configures a preferred message format.
	<b>destination transport-method</b>	Enables the message transport method.

# 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

Command History	Release	Modification
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

**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
	<a href="#">destination address</a>	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	<a href="#">destination preferred-msg-format</a>	Configures a preferred message format.
	<a href="#">destination transport-method</a>	Enables the message transport method.

---

 destination preferred-msg-format

# 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	
<b>long-text</b>	Sends the message in long-text format.
<b>short-text</b>	Sends the message in short-text format.
<b>xml</b>	Sends the message in XML format.

Defaults	xml
----------	-----

Command Modes	cfg-call-home-profile
---------------	-----------------------

Command History	Release	Modification
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

Usage Guidelines	To enter profile call-home configuration submode, use the <b>profile</b> command in call-home configuration mode.
------------------	---

Examples	This example shows how to configure the preferred message format as long text:
	<pre>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)#+</pre>

Related Commands	Command	Description
	<a href="#">destination address</a>	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	<a href="#">destination message-size-limit bytes</a>	Configures a maximum destination message size for the destination profile.
	<a href="#">destination transport-method</a>	Enables the message transport method.

# destination transport-method

To enable the message transport method, use the **destination transport-method** command.

```
destination transport-method {email | http}
```

<b>Syntax Description</b>	<b>email</b>	Enables e-mail as transport method.
	<b>http</b>	Enables HTTP as transport method.

<b>Defaults</b>	e-mail
-----------------	--------

<b>Command Modes</b>	cfg-call-home-profile
----------------------	-----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

<b>Usage Guidelines</b>	To enter profile call-home configuration submode, use the <b>profile</b> command in call-home configuration mode.
-------------------------	---

<b>Examples</b>	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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">destination address</a>	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	<a href="#">destination message-size-limit bytes</a>	Configures a maximum destination message size for the destination profile.
	<a href="#">destination preferred-msg-format</a>	Configures a preferred message format.

---

```
■ diagnostic fpga soft-error recover aggressive
```

# diagnostic fpga soft-error recover aggressive

To configure the SEU behavior, use the **diagnostic fpga soft-error recover aggressive** command. To return to the default setting, use the **no** form of this command.

**diagnostic fpga soft-error recover aggressive**

**no diagnostic fpga soft-error recover aggressive**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** The default behavior of a non-redundant switch or a switch that is not in SSO mode is to log a console message every hour until the supervisor engine resets. This command changes this behavior so that the supervisor engine reloads immediately. The default behavior of a supervisor engine when the switch is in SSO mode is to reload immediately because the reload has minimal impact on traffic.

---

**Command Modes** Global config mode

---

Command History	Release	Modification
	12.2(53)SG3, 12.2(54)SG, 15.0(2)SG XE 3.1.1SG	Support for this command was provided on the Catalyst 4500 series switch.

---



---

**Usage Guidelines** The **no** form of the command accepts neither conservative nor aggressive keywords.

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 aggressive:

```
Switch(config)# diagnostic fpga soft-error recover aggressive
```

This example shows how to revert to the default behavior:

```
Switch(config)# no diagnostic fpga soft-error recover aggressive
```

# 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]**

<b>Syntax Description</b>	<b>conservative</b> (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. <b>normal</b> (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. <b>aggressive</b> (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.						
<b>Defaults</b>	normal mode						
<b>Command Modes</b>	Global configuration mode						
<b>Command History</b>	<table border="1"> <thead> <tr> <th><b>Release</b></th><th><b>Modification</b></th></tr> </thead> <tbody> <tr> <td>12.2(18)EW</td><td>This command was introduced on the Catalyst 4500 series switch.</td></tr> </tbody> </table>	<b>Release</b>	<b>Modification</b>	12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.		
<b>Release</b>	<b>Modification</b>						
12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.						
<b>Usage Guidelines</b>	<p>Use the <b>conservative</b> keyword when you do not want the switch to reboot so that the problem can be fixed.</p> <p>Use the <b>aggressive</b> keyword when you have redundant supervisor engines, or when network-level redundancy has been provided.</p>						
<b>Examples</b>	<p>This example shows how to configure the switch to initiate an RPR switchover when an ongoing failure occurs:</p> <pre>Switch# configure terminal Switch (config)# diagnostic monitor action normal</pre>						
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><a href="#">show diagnostic result module test 2</a></td><td>Displays the module-based diagnostic test results.</td></tr> <tr> <td><a href="#">show diagnostic result module test 3</a></td><td>Displays the module-based diagnostic test results.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<a href="#">show diagnostic result module test 2</a>	Displays the module-based diagnostic test results.	<a href="#">show diagnostic result module test 3</a>	Displays the module-based diagnostic test results.
<b>Command</b>	<b>Description</b>						
<a href="#">show diagnostic result module test 2</a>	Displays the module-based diagnostic test results.						
<a href="#">show diagnostic result module test 3</a>	Displays the module-based diagnostic test results.						

**diagnostic start**

# diagnostic start

To run the specified diagnostic test, use the **diagnostic start** command.

```
diagnostic start {module num} {test test-id} [port num]
```

---

## Syntax Description

<b>module num</b>	Module number.
<b>test</b>	Specifies a test to run.
<i>test-id</i>	Specifies an identification number for the test to be run; can be the cable diagnostic <i>test-id</i> , or the <b>cable-tdr</b> keyword.
<b>port num</b>	(Optional) Specifies the interface port number.

---

## Defaults

This command has no default settings.

---

## Command Modes

Privileged EXEC mode

---

## Command History

Release	Modification
12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.

---

## Examples

This example shows how to run the specified diagnostic test at the specified module:

```
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
<a href="#">show diagnostic content</a>	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***

<b>Syntax Description</b>	<i>max-attempts</i>	Specifies a maximum number of attempts before a port is moved to the auth-fail VLAN in the range of 1 to 10.
---------------------------	---------------------	--

<b>Defaults</b>	Default is 3.
-----------------	---------------

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Examples</b>	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#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">dot1x max-reauth-req</a>	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	<a href="#">show dot1x</a>	Displays dot1x information.

---

dot1x auth-fail vlan

## 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***

---

<b>Syntax Description</b>	<i>vlan-id</i> Specifies a VLAN in the range of 1 to 4094.
---------------------------	--

---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.

---

<b>Examples</b>	This example shows how to configure the auth-fail VLAN on Fast Ethernet interface 4/3:
	<pre>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#</pre>

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">dot1x max-reauth-req</a>	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	<a href="#">show dot1x</a>	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**

<b>Syntax Description</b>	<b>in</b> (Optional) Specifies controlling in-bound traffic on a port. <b>both</b> (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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

**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 system 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)#

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show dot1x</b>	Displays dot1x information.

**dot1x critical**

## 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

Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

**Examples** This example shows how to enable 802.1x critical authentication:

```
Switch(config-if)# dot1x critical
Switch(config-if)#
```

**Related Commands**

Command	Description
<a href="#"><b>dot1x critical eapol</b></a>	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.
<a href="#"><b>dot1x critical recovery delay</b></a>	Sets the time interval between port reinitializations.
<a href="#"><b>dot1x critical vlan</b></a>	Assigns a critically authenticated port to a specific VLAN.
<a href="#"><b>show dot1x</b></a>	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

Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

**Examples** This example shows how to enable sending EAPOL success packets:

```
Switch(config-if)# dot1x critical eapol
Switch(config-if)#

```

Related Commands	Command	Description
	<a href="#">dot1x critical</a>	Enables the 802.1X critical authentication on a port.
	<a href="#">dot1x critical recovery delay</a>	Sets the time interval between port reinitializations.
	<a href="#">dot1x critical vlan</a>	Assigns a critically authenticated port to a specific VLAN.
	<a href="#">show dot1x</a>	Displays dot1x information.

---

 dot1x critical recovery delay

# 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**

---

<b>Syntax Description</b>	<i>delay-time</i>	Specifies the interval between port reinitializations when AAA transition occurs; valid values are from 1 to 10,000 milliseconds.
---------------------------	-------------------	---

---

<b>Defaults</b>	Delay time is set to 100 milliseconds.
-----------------	--

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

---

<b>Examples</b>	This example shows how to set the 802.1x critical recovery delay time to 500:
	<pre>Switch(config-if)# dot1x critical recovery delay 500 Switch(config-if)# </pre>

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">dot1x critical</a>	Enables the 802.1X critical authentication on a port.
	<a href="#">dot1x critical eapol</a>	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.
	<a href="#">dot1x critical vlan</a>	Assigns a critically authenticated port to a specific VLAN.
	<a href="#">show dot1x</a>	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***

<b>Syntax Description</b>	<i>vlan-id</i> (Optional) Specifies the VLANs; valid values are from 1 to 4094.										
<b>Defaults</b>	Critical authentication is disabled on a ports VLAN.										
<b>Command Modes</b>	Interface configuration mode										
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.2(31)SG</td><td>Support for this command was introduced on the Catalyst 4500 series switch.</td></tr> </tbody> </table>	Release	Modification	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.						
Release	Modification										
12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.										
<b>Usage Guidelines</b>	<p>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.</p> <p>This command is not supported on platforms such as Layer 3 switches that do not include the Critical Auth VLAN subsystem.</p>										
<b>Examples</b>	<p>This example shows how to enable 802.1x critical authentication on a ports VLAN:</p> <pre>Switch(config-if)# dot1x critical vlan 350 Switch(config-if)#</pre>										
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td><a href="#">dot1x critical</a></td><td>Enables the 802.1X critical authentication on a port.</td></tr> <tr> <td><a href="#">dot1x critical eapol</a></td><td>Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.</td></tr> <tr> <td><a href="#">dot1x critical recovery delay</a></td><td>Sets the time interval between port reinitializations.</td></tr> <tr> <td><a href="#">show dot1x</a></td><td>Displays dot1x information.</td></tr> </tbody> </table>	Command	Description	<a href="#">dot1x critical</a>	Enables the 802.1X critical authentication on a port.	<a href="#">dot1x critical eapol</a>	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.	<a href="#">dot1x critical recovery delay</a>	Sets the time interval between port reinitializations.	<a href="#">show dot1x</a>	Displays dot1x information.
Command	Description										
<a href="#">dot1x critical</a>	Enables the 802.1X critical authentication on a port.										
<a href="#">dot1x critical eapol</a>	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.										
<a href="#">dot1x critical recovery delay</a>	Sets the time interval between port reinitializations.										
<a href="#">show dot1x</a>	Displays dot1x information.										

**dot1x guest-vlan**

## 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***

<b>Syntax Description</b>	<i>vlan-id</i> Specifies a VLAN in the range of 1 to 4094.
---------------------------	--

<b>Defaults</b>	This command has no default settings.; the guest VLAN feature is disabled.
-----------------	--

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EWA	Support for secondary VLAN as the configured guest VLAN ID was added.

<b>Usage Guidelines</b>	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.
-------------------------	---

<b>Examples</b>	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#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">dot1x max-reauth-req</a>	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	<a href="#">show dot1x</a>	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 guest-vlan supplicant**

**no dot1x guest-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

Command History	Release	Modification
	12.2(25)EWA	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<a href="#">dot1x system-auth-control</a>	Enables 802.1X authentication on the switch.
	<a href="#">show dot1x</a>	Displays dot1x information.

**dot1x host-mode**

## 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]**

<b>Syntax Description</b>	<b>multi-host</b> Enables multiple-hosts mode on the switch. <b>single-host</b> Enables single-host mode on the switch. <b>multi-domain</b> Enables MDA on a switch port.
---------------------------	---

**Defaults**      The default is single-host mode.

**Command Modes**      Interface configuration mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(20)EWA	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(37)SG	Added support for multiple domains.

**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**

<b>Command</b>	<b>Description</b>
<a href="#">show dot1x</a>	Displays dot1x information.

**dot1x initialize**

# dot1x initialize

To unauthorize an interface before reinitializing 802.1X, use the **dot1x initialize** command.

**dot1x initialize *interface***

<b>Syntax Description</b>	<i>interface</i>	Number of the interface.
---------------------------	------------------	--------------------------

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	Use this command to initialize state machines and to set up the environment for fresh authentication.
-------------------------	---

<b>Examples</b>	This example shows how to initialize the 802.1X state machines on an interface:
	Switch# <b>dot1x initialize</b> Switch#

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show dot1x</a>	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]**

<b>Syntax Description</b>	<b>eap</b> (Optional) Specifies using EAP MAC address authentication.				
<b>Defaults</b>	There is no default setting.				
<b>Command Modes</b>	Interface configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th><b>Release</b></th><th><b>Modification</b></th></tr> </thead> <tbody> <tr> <td>12.2(31)SG</td><td>Support for this command was introduced on the Catalyst 4500 series switch.</td></tr> </tbody> </table>	<b>Release</b>	<b>Modification</b>	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.
<b>Release</b>	<b>Modification</b>				
12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.				
<b>Usage Guidelines</b>	The removal of the <b>dot1x mac-auth-bypass</b> 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.				
<b>Examples</b>	This example shows how to enable EAP MAC address authentication: <pre>Switch(config-if)# <b>dot1x mac-auth-bypass</b> Switch(config-if)#</pre>				

---

dot1x max-reauth-req

## 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**

<b>Syntax Description</b>	<i>count</i> Number of times that the switch retransmits EAP-Request/Identity frames before restarting the authentication process; valid values are from 1 to 10.
---------------------------	---

<b>Defaults</b>	The switch sends a maximum of two retransmissions.
-----------------	--

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	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.

<b>Examples</b>	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)#

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show dot1x</a>	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	<i>count</i> 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	This command was modified to control on EAP-Request/Identity retransmission limits.

**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)#

```

**dot1x max-req**

Related Commands	Command	Description
	<a href="#">dot1x initialize</a>	Unauthorizes an interface before reinitializing 802.1X.
	<a href="#">dot1x max-reauth-req</a>	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	<a href="#">show dot1x</a>	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.
Command Modes	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.
Command History	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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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.

**dot1x port-control**

- 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**

<b>Command</b>	<b>Description</b>
<a href="#">show dot1x</a>	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*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b> (Optional) Module and port number of the interface.
---------------------------	--

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

<b>Command Modes</b>	Privileged EXEC mode
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	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.
-------------------------	--

<b>Examples</b>	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**

# 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**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

<b>Defaults</b>	The periodic reauthentication is disabled.
-----------------	--

---

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

---



---

<b>Usage Guidelines</b>	You configure the amount of time between the periodic reauthentication attempts by using the <b>dot1x timeout re-authperiod</b> global configuration command.
-------------------------	---

---

<b>Examples</b>	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.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dot1x timeout</b>	Sets the reauthentication timer.
	<b>show dot1x</b>	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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
	<a href="#">dot1x initialize</a>	Unauthorizes an interface before reinitializing 802.1X.
	<a href="#">show dot1x</a>	Displays dot1x information.

**dot1x timeout**

## 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}
```

<b>Syntax Description</b>	<b>reauth-period seconds</b> Number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the “Usage Guidelines” section for more information. <b>reauth-period server</b> 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. <b>quiet-period seconds</b> 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. <b>tx-period seconds</b> 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. <b>supp-timeout seconds</b> Number of seconds that the switch waits for the retransmission of EAP-Request packets; valid values are from 30 to 65535 seconds. <b>server-timeout seconds</b> 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.
- Suplicant timeout is 30 seconds.
- Server timeout is 30 seconds.

### Command Modes

Interface configuration mode

### Command History

Release	Modification
12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switches.
12.2(25)EWA	Support for selecting the reauthentication timer from the “server” was added.

**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**

<b>Command</b>	<b>Description</b>
<a href="#">dot1x initialize</a>	Unauthorizes an interface before reinitializing 802.1X.
<a href="#">show dot1x</a>	Displays dot1x information.

**■ duplex**

## 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**

<b>Syntax Description</b>	<b>auto</b> Specifies the autonegotiation operation. <b>full</b> Specifies the full-duplex operation. <b>half</b> Specifies the half-duplex operation.
---------------------------	--

<b>Defaults</b>	Half-duplex operation
-----------------	-----------------------

<b>Command Modes</b>	Interface configuration mode
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	Table 2-1 lists the supported command options by interface.
-------------------------	---

**Table 2-1 Supported duplex Command Options**

<b>Interface Type</b>	<b>Supported Syntax</b>	<b>Default Setting</b>	<b>Guidelines</b>
10/100-Mbps module	<b>duplex [half   full]</b>	<b>half</b>	If the speed is set to <b>auto</b> , you will not be able to set the <b>duplex</b> mode. If the speed is set to <b>10</b> or <b>100</b> , and you do not configure the duplex setting, the duplex mode is set to <b>half</b> duplex.
100-Mbps fiber modules	<b>duplex [half   full]</b>	<b>half</b>	
Gigabit Ethernet Interface	Not supported.	Not supported.	Gigabit Ethernet interfaces are set to <b>full</b> duplex.
10/100/1000	<b>duplex [half   full]</b>		If the speed is set to <b>auto</b> or <b>1000</b> , you will not be able to set <b>duplex</b> . If the speed is set to <b>10</b> or <b>100</b> , and you do not configure the duplex setting, the duplex mode is set to <b>half</b> 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
<b>duplex half</b> or <b>duplex full</b>	<b>speed auto</b>	Autonegotiates both speed and duplex modes
<b>duplex half</b>	<b>speed 10</b>	Forces 10 Mbps and half duplex
<b>duplex full</b>	<b>speed 10</b>	Forces 10 Mbps and full duplex
<b>duplex half</b>	<b>speed 100</b>	Forces 100 Mbps and half duplex
<b>duplex full</b>	<b>speed 100</b>	Forces 100 Mbps and full duplex
<b>duplex full</b>	<b>speed 1000</b>	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
<a href="#">speed</a>	Configures the interface speed.
<a href="#">interface</a> (refer to Cisco IOS documentation)	Configures an interface.
<a href="#">show controllers</a> (refer to Cisco IOS documentation)	Displays controller information.
<a href="#">show interfaces</a>	Displays interface information.

**■ energywise (global configuration)**

# energywise (global configuration)

Use the **energywise** global configuration command to enable and configure EnergyWise on an entity. Use the **no** form of this command to disable EnergyWise on the entity and remove the EnergyWise configuration.

```
energywise {importance importance | keywords word,word,... | level level | management
tcp-port-number | name name | neighbor hostname | ip-address udp-port-number | role role}
no energywise {importance | keywords | level | management | name | neighbor | role}
```

<b>Syntax Description</b>	<b>importance <i>importance</i></b> Sets the importance of the entity. The range is from 1 to 100.
<b>keywords <i>word,word,...</i></b>	Assigns at least one keyword for the entity. When assigning multiple keywords, separate the keywords with commas, and do not use spaces between keywords. For the <i>word</i> value: <ul style="list-style-type: none"> <li>• You can enter alphanumeric characters and symbols such as #, (, %, ! or &amp;.</li> <li>• Do not use an asterisk (*) or a blank space between the characters and symbols.</li> </ul>
<b>level <i>level</i></b>	Sets the power level of the entity. The only valid value is 10.
<b>management <i>tcp-port-number</i></b>	Specifies the TCP port that connects to the management station. The range is from 1 to 65000.
<b>name <i>name</i></b>	Specifies the EnergyWise-specific entity name. For the <i>name</i> value: <ul style="list-style-type: none"> <li>• You can enter alphanumeric characters and symbols such as #, (, %, ! or &amp;.</li> <li>• Do not use an asterisk (*) or a blank space between the characters and symbols.</li> </ul>
<b>neighbor <i>hostname</i>   <i>ip-address</i> <i>udp-port-number</i></b>	Assigns a static neighbor. <ul style="list-style-type: none"> <li>• Hostname (<i>hostname</i>) or IP address (<i>ip-address</i>).</li> <li>• UDP port (<i>udp-port-number</i>) that sends and receives queries. The range is from 1 to 65000.</li> </ul>
<b>role <i>role</i></b>	Specifies the role of the entity in the EnergyWise domain. For example, lobby.b20. For the <i>role</i> value: <ul style="list-style-type: none"> <li>• You can enter alphanumeric characters and symbols such as #, (, %, ! or &amp;.</li> <li>• Do not use an asterisk (*) or a blank space between the characters and symbols.</li> </ul>

---

<b>Defaults</b>	The importance is 1. No keywords are defined. The power level is 10. The <i>tcp-port-number</i> is 43440. The name is the hostname. No neighbors are assigned. The role is the model number.
-----------------	--

---

<b>Command Modes</b>	Configuration
----------------------	---------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SG	This command was introduced.

---

<b>Usage Guidelines</b>	When you add an entity to a domain, EnergyWise is enabled on the entity and its PoE ports.
-------------------------	--

<b>Examples</b>	This example shows how to enable EnergyWise, assign the entity to a domain, and set the password:
<pre>Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30 Switch(config)# energywise importance 50 Switch(config)# energywise keywords lab1,devlab Switch(config)# energywise management 60500 Switch(config)# energywise name Entity01 Switch(config)# energywise neighbor 4500-21 43440 Switch(config)# energywise role role.lobbyaccess Switch(config)# end</pre>	

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show energywise</a>	Displays the EnergyWise settings and status.

---

---

 ■ **energywise (interface configuration)**

# energywise (interface configuration)

Use the **energywise** interface configuration command to configure EnergyWise on the power over Ethernet (PoE) port. Use the **no** form of this command to disable EnergyWise on the port and remove the EnergyWise configuration.

**energywise [importance *importance* | keywords *word,word,...* | level *level* [recurrence at *minute hour day\_of\_month month day\_of\_week*] | name *name* | role *role*]**

**no energywise**

---

<b>Syntax Description</b>	<b>importance <i>importance</i></b> (Optional) Sets the importance of the port. The range is from 1 to 100.
<b>keywords <i>word,word,...</i></b>	(Optional) Assigns at least one keyword for the port. When assigning multiple keywords, separate the keywords with commas, and do not use spaces between keywords. For the <i>word</i> value: <ul style="list-style-type: none"> <li>You can enter alphanumeric characters and symbols such as #, (, %, ! or &amp;.</li> <li>Do not use an asterisk (*) or a blank space between the characters and symbols.</li> </ul>
<b>level <i>level</i></b>	(Optional) Sets the power level of the port. The only valid values are 0 and 10.
<b>recurrence</b>	(Optional) Schedules the power-on or power-off recurrence.
<b>importance <i>importance</i></b> <b>at <i>minute hour day_of_month month day_of_week</i></b>	<ul style="list-style-type: none"> <li><b>importance <i>importance</i></b>—Sets the importance of the port in the domain. The range is from 1 to 100.</li> <li><i>minute</i>—The range is from 0 to 59. Use * for the wildcard.</li> <li><i>hour</i>—The range is from 0 to 23. Use * for the wildcard.</li> <li><i>day_of_month</i>—The range is from 1 to 31. Use * for the wildcard.</li> <li><i>month</i>—The range is from 1 to 12. You can also enter <b>jan, feb, mar, apr</b>, and so on. Use * for the wildcard.</li> <li><i>day_of_week</i>—The range is from 0 to 7 (0 and 7 both represent Sunday). Use * for the wildcard.</li> </ul>
<b>Note</b>	The specified times are local times based on the PoE-entity time zone.
<b>Note</b>	If the day of the month and day of the week are both specified, (that is, are not wildcards), the recurrence is executed when either field matches the current time.
<b>Note</b>	Recurrence takes effect within the minute specified, rather than exactly on the minute; it could occur as much as 60 seconds late.

---

---

<b>name</b> <i>name</i>	(Optional) Specifies the EnergyWise-specific port name.
For the <i>name</i> value:	
<b>role</b> <i>role</i>	(Optional) Specifies the role of the port in the domain. For example, lobbyport.
For the <i>role</i> value:	

---

**Defaults**

The importance is 1.

No keywords are defined.

The power level is 10.

The name is the short version of the interface name; for example, Gi1.2 for Gigabit Ethernet 1/2.

**Command Modes**

Interface Configuration

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(52)SG	This command was introduced.

---

**Usage Guidelines**

To return the **importance** and **level** values to the default settings, use the **default energywise importance** and the **default energywise level** commands.

**Examples**

This example shows how to enable and configure EnergyWise on the PoE port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
Switch(config)# interface Gi1.2
Switch(config-if)# energywise level 10 recurrence importance 90 at 0 8 * * *
Switch(config-if)# energywise level 0 recurrence importance 90 at 0 20 * * *
Switch(config-if)# energywise importance 50
Switch(config-if)# energywise name lobbyInterface.3
Switch(config-if)# energywise role role.lobbyaccess
Switch(config-if)# end
```



**Note** Recurrence takes effect within the minute specified, rather than exactly on the minute; it could occur as much as 60-seconds late.

■ **energywise (interface configuration)**

Related Commands	Command	Description
	<a href="#">show energywise</a>	Displays the EnergyWise settings and status.

# energywise domain

Use the **energywise domain** global configuration command to enable EnergyWise on the entity, assign the entity to a domain, and set the password for secure communication among the entities in the domain. Use the **no** form of this command to disable EnergyWise on the entity and to remove the EnergyWise configuration.

**energywise domain** *domain-name secret [0 | 7] password [protocol udp port *udp-port-number* [interface *interface-id* | ip *ip-address*]]*

**no energywise domain**

## Syntax Description

<b>domain</b> <i>domain-name</i>	Assigns the entity to a domain with the specified <i>domain-name</i> . <ul style="list-style-type: none"> <li>You can enter alphanumeric characters and symbols such as #, (, %, ! or &amp;.</li> <li>Do not use an asterisk (*) or a blank space between the characters and symbols.</li> </ul>
<b>secret</b> <i>[0   7]</i> <i>password</i>	Sets the <i>password</i> for secure communication among the entities in the domain. <ul style="list-style-type: none"> <li>(Optional) <b>0</b>—Use an unencrypted password.</li> <li>(Optional) <b>7</b>—Use an hidden password. This requires service password-encryption to be enabled.</li> </ul> If you do not enter <b>0</b> or <b>7</b> , the entity uses the default value of 0. For the <i>password</i> value: <ul style="list-style-type: none"> <li>You can enter alphanumeric characters and symbols such as #, (, %, ! or &amp;.</li> <li>Do not use an asterisk (*) or a blank space between the characters and symbols.</li> </ul>
<b>port</b> <i>udp-port-number</i>	(Optional) Specifies the UDP port that sends and receives queries. The range is from 1 to 65000.
<b>interface</b> <i>interface-id</i>	(Optional) In a bridged network, specifies the interface that you would prefer for communicating with other EnergyWise switches rather than letting the switch select an interface by default.
<b>ip</b> <i>ip-address</i>	(Optional) In a routed network, specifies the IP address to be used while communicating with EnergyWise peers instead of letting the system choose a default.  The <b>interface</b> and <b>ip</b> options are mutually exclusive.

## Defaults

The entity is not assigned to a domain.

The password is not set.

The *udp-port-number* is 43440.

**■ energywise domain**

**Command Modes** Configuration

Command History	Release	Modification
	12.2(52)SG	This command was introduced.

**Usage Guidelines** If you enter the **energywise domain *domain-name* secret [0 | 7] *password*** command, the entity selects the first available interface to communicate with the network and with management applications.

**Examples** This example shows how to enable EnergyWise and how to set the *domain-name* and *password* values::

```
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
```

This example shows how to enable EnergyWise and to specify the route to the management applications:

```
Switch(config)# energywise domain cisco secret 0 cisco protocol udp port 43440 ip 192.168.1.2
```

**Related Commands**

Command	Description
<a href="#"><b>show energywise</b></a>	Displays the EnergyWise settings and status.

# energywise query

Use the **energywise query** privileged EXEC command to run a query to display power information or to power the entities or PoE ports.

**energywise query importance *importance* {keywords *word,word,...* | name *name*} collect {delta | usage}**

**energywise query importance *importance* {keywords *word,word,...* | name *name*} set level *level***

**energywise query importance *importance* {keywords *word,word,...* | name *name*} sum {delta | usage}**

<b>Syntax Description</b>	<b>importance <i>importance</i></b> Sets the importance of the entity or ports. The range is from 1 to 100.
<b>keywords <i>word,word,...</i></b>	Specifies one of more keywords to use in the query. When specifying multiple keywords, separate the keywords with commas, and do not use spaces between keywords. For the <i>word</i> value: <ul style="list-style-type: none"> <li>You can enter alphanumeric characters and symbols such as #, (, %, ! or &amp;.</li> <li>Do not use an asterisk (*) or a blank space between the characters and symbols.</li> </ul>
<b>name <i>name</i></b>	Name to use in the query. For the wildcard, use * or <i>name*</i> with the asterisk at the end of the name. For the <i>name</i> value: <ul style="list-style-type: none"> <li>You can enter alphanumeric characters and symbols such as #, (, %, ! or &amp;.</li> <li>Do not use an asterisk (*) or a blank space between the characters and symbols.</li> </ul>
<b>collect {delta   usage}</b>	Displays the delta or usage values for the entity or PoE ports. <ul style="list-style-type: none"> <li><b>delta</b>—Displays only the differences between the current and available power levels.</li> <li><b>usage</b>—Displays only the current power usage.</li> </ul>
<b>set level <i>level</i></b>	Sets the power level of the entity or the PoE ports. For the entity, the only valid value is 10. For the ports, the valid values are 0 and 10.
<b>sum {delta   usage}</b>	Displays the sum of the delta or usage values for the entity or PoE ports. <ul style="list-style-type: none"> <li><b>delta</b>—Displays only the sum of the differences between the current and available power levels .</li> <li><b>usage</b>—Displays only the sum of the current power usage.</li> </ul>

**■ energywise query****Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(52)SG	This command was introduced.

**Usage Guidelines** To power on or power off ports, enter the **energywise query {keywords word,word,... | name name} set level level** command.

**Caution** Use this query with care because it affects the entity on which you enter the command and other devices in the domain that match the query criteria.

**Examples**

These examples show how to filter with the entity name:

```
Switch# energywise query importance 100 name phone* collect usage
EnergyWise query, timeout is 3 seconds:
```

Host	Name	Usage
2.2.2.21	phone	0.0 (W)
2.2.2.21	phone	15.4 (W)
2.2.2.21	phone	0.0 (W)
2.2.2.22	phone	0.0 (W)
2.2.2.21	phone	0.0 (W)
2.2.2.22	phone	15.4 (W)
2.2.2.21	phone	0.0 (W)
2.2.2.23	phone	15.4 (W)
2.2.2.21	phone	0.0 (W)

Queried: 9    Responded: 9    Time: 0.26 seconds

```
Switch# energywise query importance 100 name * sum usage
EnergyWise query, timeout is 3 seconds:
```

Total Usage
346.3 (W)

Queried: 147    Responded: 147    Time: 0.121 seconds

```
Switch# energywise query importance 100 name lobby* collect usage
```

EnergyWise query, timeout is 3 seconds:

Host	Name	Usage
2.2.4.30	lobbyInterface.17	10.0 (W)

Queried: 1    Responded: 1    Time: 0.7 seconds

```
Switch# energywise query importance 100 name Fa1.0.4* sum usage
```

EnergyWise query, timeout is 3 seconds:

Total Usage

```
-----
12.9 (W)

Queried: 10      Responded: 10      Time: 0.6 seconds
```

This example shows the sum of the delta values and the potential power change in the domain:

```
Switch# energywise query importance 100 name * sum delta
EnergyWise query, timeout is 3 seconds:
```

Level	Label	Delta Power (W)
0	Shut	-12.9
1	Hibernate	+723.8
2	Sleep	+723.8
3	Standby	+723.8
4	Ready	+723.8
5	Low	+723.8
6	Frugal	+723.8
7	Medium	+723.8
8	Reduced	+723.8
9	High	+723.8
10	Full	+723.8

```
Queried: 48      Responded: 48      Time: 0.15 seconds
```

This example shows the power levels in the domain:

```
Switch# show energywise children
Interface  Role          Name           Usage     Lvl   Imp   Type
-----  ----          ---           -----     ---   ---   ---
                    control        SwitchA       86.0    (W)  10   100  parent
Gi1/0/1    interface     Gi1.0.1       0.0     (W)  10    20  child
.
.
.
Gi1/0/6    interface     Gi1.0.6       0.0     (W)  10    20  child
Gi1/0/7    role.lobbyaccess lobbyInterface.7 0.0     (W)  10    50  child
Gi1/0/8    interface     Gi1.0.8       0.0     (W)  10    20  child
<output truncated>
```

```
Switch# energywise query importance 100 name * set level 0
EnergyWise query, timeout is 3 seconds:
```

```
Success rate is (0/0) setting entities
```

```
Queried: 0      Responded: 0      Time: 0.996 seconds
```

```
Switch# energywise query importance 100 name * set level 10
EnergyWise query, timeout is 3 seconds:
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!
Success rate is (48/48) setting entities
```

This example shows how to assign keywords on entities:

```
Switch(config)# interface Gi1/2
Switch(config-if)# energywise keywords lobby,sattelite
Switch(config-if)# energywise keywords public
Switch(config-if)# end
Switch# show running-config interface gigabitethernet1/0/2
!
interface GigabitEthernet1/2
energywise level 0 recurrence importance 90 at 0 8 * * *
energywise level 10 recurrence importance 90 at 0 20 * * *
```

**■ energywise query**

```

energywise importance 50
energywise role role.lobbyaccess
energywise keywords lobby,satellite,public
energywise name lobbyInterface.2
end

Switch# energywise query keyword lobby collect usage
EnergyWise query, timeout is 3 seconds:

Host           Name          Usage
----          ----          -----
2.2.4.30      lobbyInterface.17 15.4 (W)

Queried: 1    Responded: 1     Time: 0.0 seconds

Switch# energywise query keyword satellite sum usage
EnergyWise query, timeout is 3 seconds:

Total Usage
-----
15.4 (W)

Queried: 1    Responded: 1     Time: 0.11 seconds

```

## erase

To erase a file system, use the **erase** command.

```
erase {/all [non-default | nvram:] | cat4000_flash | nvram: | startup-config}
```

### Syntax Description

<b>/all nvram:</b>	Erases everything in nvram:.
<b>/all non-default</b>	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.
<b>Note</b>	This command option is intended to work only on a standalone supervisor engine.
<b>cat4000_flash:</b>	Erases the VLAN database configuration file.
<b>nvram:</b>	Erases the startup-config and private-config file in NVRAM.
<b>startup-config:</b>	Erases the startup-config and private-config file in NVRAM.

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC mode

### Command History

	<b>Release</b>	<b>Modification</b>
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.

### 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-config** 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).

erase

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](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](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: Initialized 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
	<b>boot config</b> (refer to Cisco IOS documentation)	Specifies the device and filename of the configuration file.
	<b>delete</b> (refer to Cisco IOS documentation)	Deletes a file from a flash memory device or NVRAM.
	<b>show bootvar</b>	Displays BOOT environment variable information.
	<b>undelete</b> (refer to Cisco IOS documentation)	Recovers a file marked “deleted” on a Class a flash file system.

**errdisable detect**

# 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
vian | 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
vian | dhcp-rate-limit [action shutdown vlan] | dtp-flap | gbic-invalid | l2ptguard | link-flap
| pagp-flap}
```

**Syntax Description**

<b>cause</b>	Specifies error-disable detection to detect a specific cause.
<b>all</b>	Specifies error-disable detection for all error-disable causes.
<b>arp-inspection</b>	Specifies the detection for the ARP inspection error-disable cause.
<b>action shutdown vlan</b>	(Optional) Specifies per-VLAN error-disable for ARP inspection and DHCP rate limiting.
<b>bpduguard shutdown vlan</b>	Specifies per-VLAN error-disable for BPDU guard.
<b>dhcp-rate-limit</b>	Specifies the detection for the DHCP rate-limit error-disable cause.
<b>dtp-flap</b>	Specifies the detection for the DTP flap error-disable cause.
<b>gbic-invalid</b>	Specifies the detection for the GBIC invalid error-disable cause.
<b>l2ptguard</b>	Specifies the detection for the Layer 2 protocol-tunnel error-disable cause.
<b>link-flap</b>	Specifies the detection for the link flap error-disable cause.
<b>pagp-flap</b>	Specifies the detection for the PAgP flap error-disable cause.

**Defaults**

All error-disable causes are detected.

**Command Modes**

Global configuration mode

**Command History**

<b>Release</b>	<b>Modification</b>
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(52)SG	Added support for per-VLAN error-disable detection.

**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 occurred. 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  

bpdu-guard            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**

<b>Command</b>	<b>Description</b>
<a href="#">show errdisable detect</a>	Displays the error disable detection status.
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in error-disabled state.

**errdisable recovery**

# 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 |
    psecure-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 |
    psecure-violation | security-violation | storm-control | udld | unicastflood | vmps} |
    [arp-inspection] [interval {interval}]]
```

Syntax Description	
<b>cause</b>	(Optional) Enables the error-disable recovery to recover from a specific cause.
<b>all</b>	(Optional) Enables the recovery timers for all error-disable causes.
<b>arp-inspection</b>	(Optional) Enables the recovery timer for the ARP inspection cause.
<b>bpduguard</b>	(Optional) Enables the recovery timer for the BPDU guard error-disable cause.
<b>channel-misconfig</b>	(Optional) Enables the recovery timer for the channel-misconfig error-disable cause.
<b>dhcp-rate-limit</b>	(Optional) Enables the recovery timer for the DHCP rate limit error-disable cause.
<b>dtp-flap</b>	(Optional) Enables the recovery timer for the DTP flap error-disable cause.
<b>gbic-invalid</b>	(Optional) Enables the recovery timer for the GBIC invalid error-disable cause.
<b>l2ptguard</b>	(Optional) Enables the recovery timer for the Layer 2 protocol-tunnel error-disable cause.
<b>link-flap</b>	(Optional) Enables the recovery timer for the link flap error-disable cause.
<b>pagp-flap</b>	(Optional) Enables the recovery timer for the PAgP flap error-disable cause.
<b>psecure-violation</b>	(Optional) Enables the recovery timer for the psecure violation error-disable cause.
<b>security-violation</b>	(Optional) Enables the automatic recovery of ports disabled due to 802.1X security violations.
<b>storm-control</b>	(Optional) Enables the timer to recover from storm-control error-disable state.
<b>udld</b>	(Optional) Enables the recovery timer for the UDLD error-disable cause.
<b>unicastflood</b>	(Optional) Enables the recovery timer for the unicast flood error-disable cause.
<b>vmps</b>	(Optional) Enables the recovery timer for the VMPS error-disable cause.
<b>arp-inspection</b>	(Optional) Enables the ARP inspection cause and recovery timeout.
<b>interval interval</b>	(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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for the storm-control feature.

**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
vmpls                 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
```

**errdisable recovery**

```
Timer interval: 300 seconds
Interfaces that will be enabled at the next timeout:
Switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show errdisable detect</a>	Displays the error disable detection status.
	<a href="#">show errdisable recovery</a>	Displays error disable recovery timer information.
	<a href="#">show interfaces status</a>	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	<b>receive</b> Specifies that the interface processes pause frames.
<b>send</b>	Specifies that the interface sends pause frames.
<b>off</b>	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
<b>on</b>	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
<b>desired</b>	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

### Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

**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
<b>send on</b>	Enables a local port to send pause frames to remote ports. To obtain predictable results, use <b>send on</b> only when remote ports are set to <b>receive on</b> or <b>receive desired</b> .
<b>send off</b>	Prevents a local port from sending pause frames to remote ports. To obtain predictable results, use <b>send off</b> only when remote ports are set to <b>receive off</b> or <b>receive desired</b> .
<b>send desired</b>	Obtains predictable results whether a remote port is set to <b>receive on</b> , <b>receive off</b> , or <b>receive desired</b> .
<b>receive on</b>	Enables a local port to process pause frames that a remote port sends. To obtain predictable results, use <b>receive on</b> only when remote ports are set to <b>send on</b> or <b>send desired</b> .
<b>receive off</b>	Prevents remote ports from sending pause frames to a local port. To obtain predictable results, use <b>send off</b> only when remote ports are set to <b>receive off</b> or <b>receive desired</b> .
<b>receive desired</b>	Obtains predictable results whether a remote port is set to <b>send on</b> , <b>send off</b> , or <b>send desired</b> .

**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)#{/pre}
```

Related Commands	Command	Description
	<a href="#">interface port-channel</a>	Accesses or creates a port-channel interface.
	<a href="#">interface range</a>	Runs a command on multiple ports at the same time.
	<a href="#">show flowcontrol</a>	Displays the per-interface status and statistics related to flow control.
	<a href="#">show running-config</a>	Displays the running-configuration for a switch.
	<a href="#">speed</a>	Configures the interface speed.

**hardware statistics**

# 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

Command History	Release	Modification
	12.2(40)SG	Support for the Supervisor Engine 6-E and the Catalyst 4900M chassis is introduced.

**Usage Guidelines** The Supervisor Engine 6-E and Catalyst 4900 M chassis TCAM hardware do not have enough hardware statistics entries for every classification/QoS cam entry. Therefore, the statistics for each cam entry needs to be enabled as needed.

**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
	<b>ip access list</b> (refer to Cisco IOS documentation)	Creates an IP ACL (Access Control List).
	<b>ipv6 access list</b> (refer to Cisco IOS documentation)	Creates an IPv6 ACL.
	<b>mac access-list extended</b>	Defines the extended MAC access lists.

# hw-module port-group

To select either Gigabit Ethernet or 10-Gigabit Ethernet interfaces on your module, use the **hw-module port-group** command.

**hw-module module number port-group number select [gigabitethernet | tengigabitethernet]**

## Syntax Description

<b>module</b>	Specifies a line module.
<i>number</i>	Specifies a module which supports TwinGig converter.
<b>port-group</b> <i>number</i>	Port group number on a switch.
<b>select</b>	Specifies an interface type; valid values are Gigabit Ethernet and 10-Gigabit Ethernet.
<b>gigabitethernet</b>	(Optional) Specifies Gigabit Ethernet.
<b>tengigabitethernet</b>	(Optional) Specifies 10-Gigabit Ethernet.

## Defaults

10 Gigabit.

## Command Modes

Global configuration mode

## Command History

Release	Modification
12.2(40)SG	Support for TwinGig converter module introduced.

## Usage Guidelines

Support for this command is available on the Cisco Catalyst 4500 modules that support TwinGig converter modules, such as the Supervisor Engine 6-E and WS-X4606-10GE-E.

## Examples

This example shows how to select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the TwinGig Converter:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hw-module module 1 port-group 1 select gigabitethernet
Switch(config)# exit
```

Use the **show interfaces status** command to display your configuration.

## Related Commands

Command	Description
<a href="#">show hw-module port-group</a>	Displays how the X2 holes on a module are grouped.
<a href="#">show interfaces status</a>	Displays the interface status or a list of interfaces in error-disabled state.

**hw-module power**

# 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**

<b>Syntax Description</b>	<table border="0"> <tr> <td><b>slot</b></td><td>(Optional) Specifies a slot on a chassis.</td></tr> <tr> <td><b>module</b></td><td>(Optional) Specifies a line module.</td></tr> <tr> <td><b>number</b></td><td>Slot or module number.</td></tr> </table>	<b>slot</b>	(Optional) Specifies a slot on a chassis.	<b>module</b>	(Optional) Specifies a line module.	<b>number</b>	Slot or module number.
<b>slot</b>	(Optional) Specifies a slot on a chassis.						
<b>module</b>	(Optional) Specifies a line module.						
<b>number</b>	Slot or module number.						

<b>Defaults</b>	After a boot up, the power is on.
-----------------	-----------------------------------

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(18)EW	Add slot and module keywords.

<b>Examples</b>	This example shows how to shut off power to a module in slot 5:
	Switch(config)# <b>no hw-module slot 5 power</b>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>clear hw-module slot password</b></a>	Clears the password on an intelligent line module.

# hw-module uplink mode shared-backplane

To change the uplink mode so that you can use all four 10-Gigabit Ethernet ports as blocking ports on the Supervisor Engine 6-E and Catalyst 4900 M chassis when operating in redundant mode, use the **hw-module uplink mode shared-backplane** command. To disable shared-backplane uplink mode, use the **no** form of the command.

**hw-module uplink mode shared-backplane**

**no hw-module uplink mode shared-backplane**

**Syntax Description** This command has no keywords or arguments.

**Defaults** Only two 10-Gigabit Ethernet ports or four 1-Gigabit Ethernet ports can be used on the supervisor engine.

**Command Modes** Global configuration mode

Command History	Release	Modification
	12.2(44)SG	Support for this command was introduced on the Catalyst 4500 series switch.

**Usage Guidelines** When changing the uplink mode using the **hw-module uplink mode shared-backplane** command, you must reload the system. A message is printed on the console to reflect this.

**Examples** This example shows how to enable shared-backplane uplink mode:

```
Switch(config)# hw-module uplink mode shared-backplane
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```

This example shows how to disable shared-backplane uplink mode:

```
Switch(config)# no hw-module uplink mode shared-backplane
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```

This example shows how to display the current state of uplink-mode:

```
Switch# show hw-module uplink
Active uplink mode configuration is Default
(will be Shared-backplane after next reload)
```

A reload of active supervisor is required to apply the new configuration.

■ **hw-module uplink mode shared-backplane**

Related Commands	Command	Description
	<a href="#">show hw-module uplink</a>	Displays hardware-module uplink information.

# hw-module uplink select

To select the 10-Gigabit Ethernet or Gigabit Ethernet uplinks on the Supervisor Engine V-10GE within the W-C4510R chassis, use the **hw-module uplink select** command.

**hw-module uplink select { tengigabitethernet | gigabitethernet | all }**

Syntax Description	<b>tengigabitethernet</b> (Optional) Specifies the 10-Gigabit Ethernet uplinks.
	<b>gigabitethernet</b> (Optional) Specifies the Gigabit Ethernet uplinks.
	<b>all</b> (Optional) Specifies all uplinks (10-Gigabit Ethernet and Gigabit Ethernet).

Defaults	tengigabitethernet
----------	--------------------

Command Modes	Global configuration mode
---------------	---------------------------

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)SG	Support for the <b>all</b> keyword was added.

Usage Guidelines	On a Supervisor Engine V-10GE (WS-X4516-10GE) in a 10-slot chassis (Catalyst 4510R and 4510R-E), if a startup configuration with a new uplink mode is copied into flash memory and the system is power cycled, the system will not come up with the new uplink mode. After copying the startup configuration with the new uplink mode into flash memory, the uplink mode must be changed to the new uplink mode through the command interface before the system is power cycled. This ensures that the system comes up in the new uplink mode.
------------------	--

Supervisor Engine V-10GE and Supervisor Engine II+10GE support 10-Gigabit Ethernet and Gigabit Ethernet uplink ports. On the Supervisor Engine II+10GE, all uplink ports are always available. Similarly, when a Supervisor Engine V-10GE is plugged into a W-C4503, W-4506, or W-4507R chassis, all uplink ports are always available. When a Supervisor Engine V-10GE is plugged into a W-4510R chassis, you can choose to use the 10-Gigabit Ethernet uplink ports, the Gigabit Ethernet uplink ports, or all uplink ports. If you choose to use all uplink ports, then the tenth slot will support only the WS-X4302-GB switching linecard. Be aware that this command takes effect only after a reload (after you have executed the **redundancy reload shelf** command).

Because the uplink selection is programmed into hardware during initialization, changing the active uplinks requires saving the configuration and reloading the switch. When you are configuring a change to the uplinks, the system responds with a message informing you that the switch must be reloaded and suggesting the appropriate command (depending on redundancy mode) to reload the switch.

If you select the **all** keyword, ensure that the tenth slot is either empty or has a WS-X4302-GB switching module.

A **no** form of this command does not exist. To undo the configuration, you must configure the uplinks.

**hw-module uplink select****Examples**

This example shows how to select the Gigabit Ethernet uplinks:

```
Switch(config)# hw-module uplink select gigabitethernet
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```



The Gigabit Ethernet uplinks will be active after the next reload.

This example shows how to select the Gigabit Ethernet uplinks in a redundant system in SSO mode:

```
Switch(config)# hw-module uplink select gigabitethernet
A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new
configuration
Switch(config)# exit
Switch#
```



The Gigabit Ethernet uplinks will be active after the next reload of the chassis/shelf. Use the **redundancy reload shelf** command to reload the chassis/shelf.

This example shows how to select the Gigabit Ethernet uplinks in a redundant system in RPR mode:

```
Switch(config)# hw-module uplink select gigabitethernet
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```



The Gigabit Ethernet uplinks will be active on a switchover or reload of the active supervisor engine.

This example shows how to select all the uplinks in a redundant system in SSO mode:

```
Switch(config)# hw-module uplink select all
Warning: This configuration mode may disable slot10.
A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new
configuration
Switch(config)# exit
Switch#
```



If you select the **all** keyword, only the Drome board will be supported in the tenth slot of the supervisor engine.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show hw-module uplink</a>	Displays hardware-module uplink information.

# 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**

<b>Syntax Description</b>	<table border="0"> <tr> <td><i>instance-id</i></td><td>MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.</td></tr> <tr> <td><b>vlans</b> <i>vlan-range</i></td><td>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.</td></tr> </table>	<i>instance-id</i>	MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.	<b>vlans</b> <i>vlan-range</i>	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.
<i>instance-id</i>	MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.				
<b>vlans</b> <i>vlan-range</i>	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.				

<b>Defaults</b>	Mapping is disabled.
-----------------	----------------------

<b>Command Modes</b>	MST configuration mode
----------------------	------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

<b>Usage Guidelines</b>	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.
-------------------------	--

<b>Examples</b>	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)#
```

**instance****Related Commands**

Command	Description
<a href="#">name</a>	Sets the MST region name.
<a href="#">revision</a>	Sets the MST configuration revision number.
<a href="#">show spanning-tree mst</a>	Displays MST protocol information.
<a href="#">spanning-tree mst configuration</a>	Enters the MST configuration submode.