CHAPTER 2

Cisco IOS Commands for the Catalyst 4500 Series Switches

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

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

#macro keywords

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Global configuration

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 enteringthe **#macro keywords** command, you will receive a message indicating what you need to include to make the syntax valid.

Examples

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

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

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

Related Commands

macro apply cisco-desktop
macro apply cisco-phone
macro apply cisco-router
macro apply cisco-switch

aaa accounting dot1x default start-stop group radius

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

aaa accounting dot1x default start-stop group radius

no aaa accounting dot1x default start-stop group radius

Syntax Description

This command has no arguments or keywords.

Defaults

Accounting is disabled.

Command Modes

Global configuration

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
```

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

Related Commands

aaa accounting system default start-stop group radius

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
```

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

Related Commands

aaa accounting dot1x default start-stop group radius

access-group mode

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

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

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

Syntax Description

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

Defaults

PACL override mode

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

This example shows how to merge applicable ACL features:

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

Related Commands

show access-group mode interface
show ip interface (refer to Cisco IOS documentation)
show mac access-group interface

access-list hardware entries

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

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

Syntax Description

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

Defaults

The ACLs are programmed as packed.

Command Modes

Global configuration

Command History

Release	Modification
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

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

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

Syntax Description

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

Defaults

The default region balance for each TCAM is 50.

Command Modes

Global configuration

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

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

Defaults

This command has no default settings.

Command Modes

VLAN access-map

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)#
```

Related Commands

match
show vlan access-map
vlan access-map

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

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

abort (refer to Cisco IOS documentation)
exit (refer to Cisco IOS documentation)
reset
show vlan
shutdown vlan (refer to Cisco IOS documentation)
vtp (global configuration mode)

arp access-list

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

arp access-list *name*

Syntax Description

name	Specifies the access control list name.

Defaults

None

Command Modes

Configuration

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 define an ARP access list named static-hosts:

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

Related Commands

deny
ip arp inspection filter vlan
permit

attach module

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

attach module *mod*

Syntax Description

mod	Target module for the command.

Defaults

This command has no default settings.

Command Modes

Privileged

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Gateway>
```

Related Commands

remote login module
session module

auto qos voip

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

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

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

Syntax Description

cisco-phone	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.
trust	Connects the interface to a trusted switch or router and automatically configures QoS for VoIP. The CoS and DSCP labels of incoming packets are trusted.

Defaults

Auto-QoS is disabled on all interfaces.

Command Modes

Interface configuration

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.

- 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:

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# config 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 autoqos-voip-policy
Switchconfig-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
```

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

Related Commands

debug auto qos (refer to Cisco IOS documentation)
qos map cos
qos trust
show auto qos
show qos
show qos interface
show qos maps

auto-sync

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

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

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

Syntax Description

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

Defaults

Standard automatic synchronization of all configuration files

Command Modes

Redundancy main-cpu

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 configure-register
Switch (config-r-mc)#
```

Related Commands

redundancy

channel-group

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

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

no channel-group

Syntax Description

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

Defaults

No channel groups are assigned.

Command Modes

Interface configuration

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.

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

interface port-channel
show interfaces port-channel (refer to Cisco IOS documentation)

channel-protocol

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

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

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

Syntax Description

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

Defaults

PAgP

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine I.

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

channel-group
show etherchannel

class-map

To access the QoS class map configuration mode to configure QoS class maps, use the **class-map** command. To delete a class map, use the **no** form of this command.

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

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

Syntax Description

match-all	(Optional) Specifies that all match criteria in the class map must be matched.
match-any	(Optional) Specifies that one or more match criteria must match.
name	Name of the class map.

Defaults

Match all criteria.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The *name* and *acl_name* arguments are case sensitive.

Use the **class-map** command and its subcommands on individual interfaces to define packet classification, marking, aggregate, and flow policing as part of a globally named service policy.

These commands are available in QoS class map configuration mode:

- **exit**—Exits you from QoS class map configuration mode.
- **no**—Removes a match statement from a class map.
- **match**—Configures classification criteria.

  These optional subcommands are also available:

  - **access-group** {*acl_index* | **name** *acl_name*}
  - **ip** {**dscp** | **precedence**} *value1 value2... value8*
  - **any**

The following subcommands appear in the CLI help, but they are not supported on LAN interfaces:

- **input-interface** {*interface interface_number* | **null** *number* | **vlan** *vlan_id*}
- **protocol** *linktype*
- **destination-address mac** *mac_address*
- **source-address mac** *mac_address*
- **qos-group**

- **mpls**
- **no**

After you have configured the class map name and are in class map configuration mode, you can enter the **match** subcommands. The syntax for these subcommands is as follows:

match {[**access-group** {*acl_index* | **name** *acl_name*}] | [**ip** {**dscp** | **precedence**} *value1 value2... value8*]}

See Table 2-1 for a syntax description of the **match** subcommands.

Table 2-1 Syntax Description for the match Command

Optional Subcommand	Description
access-group *acl_index* | *acl_name*	Specifies the access list index or access list names; valid access list index values are from 1 to 2699.
access-group *acl_name*	Specifies the named access list.
ip dscp *value1 value2 ... value8*	Specifies the IP DSCP values to match; valid values are from 0 to 63. Enter up to eight DSCP values separated by white spaces.
ip precedence *value1 value2 ... value8*	Specifies the IP precedence values to match; valid values are from 0 to 7. Enter up to eight precedence values separated by white spaces.

Examples

This example shows how to access the **class-map** commands and subcommands and to configure a class map named ipp5 and enter a match statement for ip precedence 5:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map ipp5
Switch(config-cmap)# match ip precedence 5
Switch(config-cmap)#
```

This example shows how to configure the class map to match an already configured access list:

```
Switch(config-cmap)# match access-group IPacl1
Switch(config-cmap)#
```

Related Commands

policy-map
service-policy
show class-map
show policy-map
show policy-map interface

clear counters

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 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 **show interface counters** (refer to Cisco IOS documentation)

clear hw-module slot password

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

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

Syntax Description

slot_num	Slot on a line module.

Defaults

The password is not cleared.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

hw-module power

clear interface gigabitethernet

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

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

show interfaces status

clear interface vlan

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

clear interface vlan *number*

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 clear the hardware logic from a specific VLAN:

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

Related Commands

show interfaces status

clear ip access-template

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

clear ip access-template *access-list*

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 statistical information for an access list:

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

clear ip arp inspection log

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

clear ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 contents of the log buffer:

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

Related Commands

arp access-list
show ip arp inspection log

clear ip arp inspection statistics

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 DAI statistics from VLAN 1 and how to verify the removal:

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

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

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

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

Related Commands

arp access-list
clear ip arp inspection log
show ip arp inspection

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

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
Switch#
```

Related Commands

ip dhcp snooping
ip dhcp snooping binding interface (refer to Cisco IOS documentation)
ip dhcp snooping information option
ip dhcp snooping trust
ip dhcp snooping vlan
show ip dhcp snooping
show ip dhcp snooping binding

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

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

ip dhcp snooping
ip dhcp snooping binding
ip dhcp snooping information option
ip dhcp snooping trust
ip dhcp snooping vlan
show ip dhcp snooping
show ip dhcp snooping binding

clear ip igmp group

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
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 **ip host** (refer to Cisco IOS documentation)
show ip igmp groups (refer to Cisco IOS documentation)
show ip igmp interface

clear ip igmp snooping membership

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

clear ip igmp snooping membership [vlan *vlan_id*]

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

Examples

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

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

Related Commands

ip igmp snooping vlan explicit-tracking
show ip igmp snooping membership

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

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

show ip mfib

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

Command History

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

ip mfib fastdrop
show ip mfib fastdrop

clear lacp counters

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine I.

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

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

Examples

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

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

Related Commands

show lacp

clear mac-address-table

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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.
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

clear mac-address-table dynamic
mac-address-table aging-time
mac-address-table notification
main-cpu
show mac-address-table address
mac-address-table notification
snmp-server enable traps
snmp trap mac-notification change

clear mac-address-table dynamic

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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.

Usage Guidelines

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

Examples

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

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

Related Commands

mac-address-table aging-time
main-cpu
show mac-address-table address

clear pagp

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 port-channel information for a specific group:

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

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

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

Related Commands

show pagp

clear port-security

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

show port-security
switchport port-security

clear qos

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

show qos

clear vlan counters

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

show vlan counters

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

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

show vmps
vmps reconfirm (privileged EXEC)

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

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

class (refer to the *Cisco IOS Release 12.2 Command Reference*)
class-map
drop (refer to the *Cisco IOS Release 12.2 Command Reference*)
match access-group (refer to the *Cisco IOS Release 12.2 Command Reference*)
policy-map
service-policy
show policy-map control-plane

debug adjacency

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

debug adjacency [**ipc**]

no debug adjacency

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 display the information in the adjacency database:

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

Related Commands

undebug adjacency (same as **no debug adjacency**)

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

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

undebug backup (same as **no debug backup**)

debug condition interface

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

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 output to VLAN interface 1:

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

Related Commands

debug interface
undebug condition interface (same as **no debug condition interface**)

debug condition standby

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

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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.

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 **undebug condition standby** (same as **no debug condition standby**)

debug condition vlan

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

debug condition vlan {*vlan_id*}

no debug condition vlan {*vlan_id*}

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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.

Usage Guidelines

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

Examples

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

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

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

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

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

Related Commands

undebug condition vlan (same as **no debug condition vlan**)

debug dot1x

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

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

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

Syntax Description

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

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

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 802.1X debugging for all conditions:

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

Related Commands

show dot1x
undebug dot1x (same as **no debug dot1x**)

debug etherchnl

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

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

no debug etherchnl

Syntax Description

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

Defaults

The default settings are as follows:

- Debug is disabled.
- All messages are displayed.

Command Modes

Privileged EXEC

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#
```

This example shows how to disable the debugging:

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

Related Commands **undebug etherchnl** (same as **no debug etherchnl**)

debug interface

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

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

debug condition interface
undebug interface (same as **no debug interface**)

debug ipc

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

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug ipc (same as **no debug ipc**)

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

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

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

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

debug ip dhcp snooping event

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

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

ip dhcp snooping
ip dhcp snooping information option
ip dhcp snooping limit rate
ip dhcp snooping trust
ip verify source vlan dhcp-snooping (refer to Cisco IOS documentation)
show ip dhcp snooping
show ip dhcp snooping binding
show ip verify source (refer to Cisco IOS documentation)

debug lacp

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

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp

Syntax Description

all	(Optional) Enables all LACP debugging.
event	(Optional) Enables the debugging of the LACP events.
fsm	(Optional) Enables the debugging of the LACP finite state machine.
misc	(Optional) Enables the miscellaneous LACP debugging.
packet	(Optional) Enables the LACP packet debugging.

Defaults

Debugging of LACP activity is disabled.

Command Modes

Privileged EXEC

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

undebug pagp (same as **no debug pagp**)

debug monitor

To display the monitoring activity, use the **debug monitor** command. To disable the debugging output, use the **no** form of this command.

debug monitor {**all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests**}

no debug monitor {**all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests**}

Syntax Description

all	Displays all the SPAN debugging messages.
errors	Displays the SPAN error details.
idb-update	Displays the SPAN IDB update traces.
list	Displays the SPAN list tracing and the VLAN list tracing.
notifications	Displays the SPAN notifications.
platform	Displays the SPAN platform tracing.
requests	Displays the SPAN requests.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug monitor (same as **no debug monitor**)

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

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

undebug nvram (same as **no debug nvram**)

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** | **event** | **fsm** | **misc** | **packet**]

no debug pagp

Syntax Description

all	(Optional) Enables all PAgP debugging.
event	(Optional) Enables the debugging of the PAgP events.
fsm	(Optional) Enables the debugging of the PAgP finite state machine.
misc	(Optional) Enables the miscellaneous PAgP debugging.
packet	(Optional) Enables the PAgP packet debugging.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug pagp (same as **no debug pagp**)

debug platform packet protocol lacp

To debug the LACP protocol packets, use the **debug platform packet protocol lacp** command. To disable the debugging output, use the **no** form of this command.

debug platform packet protocol lacp [**receive** | **transmit** | **vlan**]

no debug platform packet protocol lacp [**receive** | **transmit** | **vlan**]

Syntax Description

receive	(Optional) Enables the platform packet reception debugging functions.
transmit	(Optional) Enables the platform packet transmission debugging functions.
vlan	(Optional) Enables the platform packet VLAN debugging functions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 platform packet protocol lacp
Switch#
```

Related Commands

undebug platform packet protocol lacp (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**]

Syntax Description

receive	(Optional) Enables the platform packet reception debugging functions.
transmit	(Optional) Enables the platform packet transmission debugging functions.
vlan	(Optional) Enables the platform packet VLAN debugging functions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 platform packet protocol pagp
Switch#
```

Related Commands

undebug platform packet protocol pagp (same as **no debug platform packet protocol pagp**)

debug pm

To debug the port manager (PM) activity, use the **debug pm** command. To disable the debugging output, use the **no** form of this command.

debug pm {**all** | **card** | **cookies** | **etherchnl** | **messages** | **port** | **registry** | **scp** | **sm** | **span** | **split** | **vlan** | **vp**}

no debug pm {**all** | **card** | **cookies** | **etherchnl** | **messages** | **port** | **registry** | **scp** | **sm** | **span** | **split** | **vlan** | **vp**}

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug pm (same as **no debug pm**)

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

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

switchport port-security

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

Syntax Description

errors	Enables the redundancy facility for error debugging.
fsm	Enables the redundancy facility for FSM event debugging.
kpa	Enables the redundancy facility for keepalive debugging.
msg	Enables the redundancy facility for messaging event debugging.
progression	Enables the redundancy facility for progression event debugging.
status	Enables the redundancy facility for status event debugging.
timer	Enables the redundancy facility for timer event debugging.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
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

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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#
```

Related Commands **undebug spanning-tree** (same as **no debug spanning-tree**)

debug spanning-tree backbonefast

To enable debugging of the spanning-tree BackboneFast events, use the **debug spanning-tree backbonefast** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree backbonefast [**detail** | **exceptions**]

no debug spanning-tree backbonefast

Syntax Description

detail	(Optional) Displays the detailed BackboneFast debugging messages.
exceptions	(Optional) Enables the debugging of spanning-tree BackboneFast exceptions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 debugging and to display the detailed spanning-tree BackboneFast debugging information:

```
Switch# debug spanning-tree backbonefast detail
Spanning Tree backbonefast detail debugging is on
Switch#
```

Related Commands

undebug spanning-tree backbonefast (same as **no debug spanning-tree backbonefast**)

debug spanning-tree switch

To enable the switch shim debugging, use the **debug spanning-tree switch** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree switch {**all** | **errors** | **general** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

no debug spanning-tree switch {**all** | **errors** | **general** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug spanning-tree switch (same as **no debug spanning-tree switch**)

debug spanning-tree uplinkfast

To enable the debugging of the spanning-tree UplinkFast events, use the **debug spanning-tree uplinkfast** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree uplinkfast [**exceptions**]

no debug spanning-tree uplinkfast

Syntax Description

exceptions	(Optional) Enables the debugging of the spanning-tree UplinkFast exceptions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 debug the spanning-tree UplinkFast exceptions:

```
Switch# debug spanning-tree uplinkfast exceptions
Spanning Tree uplinkfast exceptions debugging is on
Switch#
```

Related Commands

undebug spanning-tree uplinkfast (same as **no debug spanning-tree uplinkfast**)

debug sw-vlan

To debug the VLAN manager activities, use the **debug sw-vlan** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan {**badpmcookies** | **events** | **management** | **packets** | **registries**}

no debug sw-vlan {**badpmcookies** | **events** | **management** | **packets** | **registries**}

Syntax Description

badpmcookies	Displays the VLAN manager incidents of bad port-manager cookies.
events	Debugs the VLAN manager events.
management	Debugs the VLAN manager management of internal VLANs.
packets	Debugs the packet handling and encapsulation processes.
registries	Debugs the VLAN manager registries.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug sw-vlan (same as **no debug sw-vlan**)

debug sw-vlan ifs

To enable the VLAN manager Cisco IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

no debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug sw-vlan ifs (same as **no debug sw-vlan ifs**)

debug sw-vlan notification

To enable the debugging of the messages that trace the activation and deactivation of the ISL VLAN IDs, use the **debug sw-vlan notification** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

no debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug sw-vlan notification (same as **no debug sw-vlan notification**)

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

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

undebug sw-vlan vtp (same as **no debug sw-vlan vtp**)

debug udld

To enable the debugging of UDLD activity, use the **debug udld** command. To disable the debugging output, use the **no** form of this command.

debug udld {**events** | **packets** | **registries**}

no debug udld {**events** | **packets** | **registries**}

Syntax Description

events	Enables the debugging of UDLD process events as they occur.
packets	Enables the debugging of the UDLD process as it receives packets from the packet queue and attempts to transmit packets at the request of the UDLD protocol code.
registries	Enables the debugging of the UDLD process as it processes registry upcalls from the UDLD process-dependent module and other feature modules.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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

undebug udld (same as **no debug udld**)

debug vqpc

To debug the VLAN Query Protocol (VQP), use the **debug vqpc** command. To disable the debugging output, use the **no** form of this command.

debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

Syntax Description

all	(Optional) Debugs all the VQP events.
cli	(Optional) Debugs the VQP command-line interface.
events	(Optional) Debugs the VQP events.
learn	(Optional) Debugs the VQP address learning.
packet	(Optional) Debugs the VQP packets.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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 VQP debugging:

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

Related Commands

vmps reconfirm (privileged EXEC)

define interface-range

To create a macro of interfaces, use the **define interface-range** command.

define interface-range *macro-name interface-range*

Syntax Description

macro-name	Name of the interface range macro; up to 32 characters.
interface-range	List of valid ranges when specifying interfaces; see the "Usage Guidelines" section.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The macro name is a character string of up to 32 characters.

A macro can contain up to five ranges. An interface range cannot span modules.

When entering the *interface-range*, use these formats:

- *interface-type* {*mod*}/{*first-interface*} - {*last-interface*}
- *interface-type* {*mod*}/{*first-interface*} - {*last-interface*}

The valid values for *interface-type* are as follows:

- **FastEthernet**
- **GigabitEthernet**
- **Vlan** *vlan_id*

Examples

This example shows how to create a multiple-interface macro:

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

Related Commands

interface range

deny

To deny an ARP packet based on matches against the DHCP bindings, use the **deny** command. To remove the specified ACEs from the access list, use the **no** form of this command.

deny {[**request**] **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **response ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} [{**any** | **host** *target-ip* | *target-ip target-ip-mask*}] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [{**any** | **host** *target-mac* | *target-mac target-mac-mask*}]} [**log**]

no deny {[**request**] **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **response ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} [{**any** | **host** *target-ip* | *target-ip target-ip-mask*}] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [{**any** | **host** *target-mac* | *target-mac target-mac-mask*}]} [**log**]

Syntax Description

request	(Optional) Requests a match for the ARP request. When **request** is not specified, matching is performed against all ARP packets.
ip	Specifies the sender IP address.
any	Specifies that any IP or MAC address will be accepted.
host *sender-ip*	Specifies that only a specific sender IP address will be accepted.
sender-ip sender-ip-mask	Specifies that a specific range of sender IP addresses will be accepted.
mac	Specifies the sender MAC address.
host *sender-mac*	Specifies that only a specific sender MAC address will be accepted.
sender-mac sender-mac-mask	Specifies that a specific range of sender MAC addresses will be accepted.
response	Specifies a match for the ARP responses.
ip	Specifies the IP address values for the ARP responses.
host *target-ip*	(Optional) Specifies that only a specific target IP address will be accepted.
target-ip target-ip-mask	(Optional) Specifies that a specific range of target IP addresses will be accepted.
mac	Specifies the MAC address values for the ARP responses.
host *target-mac*	(Optional) Specifies that only a specific target MAC address will be accepted.
target-mac target-mac-mask	(Optional) Specifies that a specific range of target MAC addresses will be accepted.
log	(Optional) Logs a packet when it matches the access control entry (ACE).

Defaults

At the end of the ARP access list, there is an implicit **deny ip any mac any** command.

Command Modes

arp-nacl configuration

Command History

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

Usage Guidelines

Deny clauses can be added to forward or drop ARP packets based on some matching criteria.

Examples

This example shows a host with a MAC address of 0000.0000.abcd and an IP address of 1.1.1.1. This example shows howto deny both requests and responses from this host:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
Switch# show arp access-list

ARP access list static-hosts
    deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

Related Commands

arp access-list
ip arp inspection filter vlan
permit

diagnostic monitor action

To direct the action of the switch when it detects a packet memory failure, use the **diagnostic monitor action** command.

diagnostic monitor action [**conservative** | **normal** | **aggressive**]

Syntax Description

conservative	(Optional) Specifies that the bootup SRAM diagnostics log all failures and remove all affected buffers from the hardware operation. The ongoing SRAM diagnostics will log events, but will take no other action.
normal	(Optional) Specifies that the SRAM diagnostics operate as in conservative mode, except that an ongoing failure resets the supervisor engine; allows for the bootup tests to map out the affected memory.
aggressive	(Optional) Specifies that the SRAM diagnostics operate as in normal mode, except that a bootup failure only logs failures and does not allow the supervisor engine to come online; allows for either a redundant supervisor engine or network-level redundancy to take over.

Defaults

normal mode

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Use the **conservative** keyword when you do not want the switch to reboot so that the problem can be fixed.

Use the **aggressive** keyword when you have redundant supervisor engines, or when network-level redundancy has been provided.

Examples

This example shows how to configure the switch to initiate an RPR switchover when an ongoing failure occurs:

```
Switch# configure terminal
Switch (config)# diagnostic monitor action normal
```

Related Commands

show diagnostic result module test 2
show diagnostic result module test 3

diagnostic start

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

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:

```
This exec command starts the TDR test on specified interface
Switch# diagnostic start module 1 test cable-tdr port 3
diagnostic start module 1 test cable-tdr port 3
module 1: Running test(s) 5 Run interface level cable diags
module 1: Running test(s) 5 may disrupt normal system operation
Do you want to continue? [no]: yes
yes
Switch#
2d16h: %DIAG-6-TEST_RUNNING: module 1: Running online-diag-tdr{ID=5} ...
2d16h: %DIAG-6-TEST_OK: module 1: online-diag-tdr{ID=5} has completed successfully

Switch#
```

Note The **show cable-diagnostic tdr** command is used to display the results of a TDR test. The test results will not be available until approximately 1 minute after the test starts. If you type 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

show diagnostic content

dot1x auth-fail max-attempts

To configure the max number of attempts before a port is moved to the auth-fail VLAN, use the **dot1x auth-fail max-attempts** command. To return to the default setting, use the **no** form of this command.

dot1x auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts *max-attempts*

Syntax Description

max-attempts	Specifies a maximum number of attempts before a port is moved to the auth-fail VLAN in the range of 1 to 10.

Defaults

Default is 3.

Command Modes

Interface configuration

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 configure the maximum number of attempts before the port is moved to the auth-fail VLAN on Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail max-attempts 5
Switch(config-if)# end
Switch#
```

Related Commands

dot1x max-reauth-req
show dot1x

dot1x auth-fail vlan

To enable the auth-fail VLAN on a port, use the **dot1x auth-fail vlan** command. To return to the default setting, use the **no** form of this command.

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan *vlan-id*

Syntax Description

vlan-id	Specifies a VLAN in the range of 1 to 4094.

Defaults

None

Command Modes

Interface configuration

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 configure the auth-fail VLAN on Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

Related Commands

dot1x max-reauth-req
show dot1x

dot1x control-direction

To enable unidirectional port control on a per-port basis on a switch, use the **dot1x control-direction** command. Use the **no** form of this command to disable unidirectional port control.

dot1x control-direction [**in** | **both**]

no dot1x control-direction

Syntax Description

in	(Optional) Specifies controlling in-bound traffic on a port.
both	(Optional) Specifies controlling both in-bound and out-bound traffic on a port.

Defaults

Both in-bound and out-bound traffic will be controlled.

Command Modes

Interface configuration

Command History

Release	Modification
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 systems was turned off. In this state, the port only allowed the receipt and transmission of EAPoL packets. Therefore, there was no way for the unidirectional control magic packet to reach the host and without being turned on there was no way for the system to authenticate and open the port.

Examples

This example shows how to enable unidirectional control on incoming packets:

```
Switch(config-if)# dot1x control-direction in
Switch(config-if)#
```

Related Commands

show dot1x

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

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

dot1x critical eapol
dot1x critical recovery delay
dot1x critical vlan
show dot1x

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

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

dot1x critical
dot1x critical recovery delay
dot1x critical vlan
show dot1x

dot1x critical recovery delay

To set the time interval between port reinitializations, use the **dot1x critical recovery delay** command. To return to the default setting, use the **no** form of this command.

dot1x critical recovery delay *delay-time*

no dot1x critical recovery delay

Syntax Description

delay-time	Specifies the interval between port reinitializations when AAA transistion occurs; valid values are from 1 to 10,000 milliseconds.

Defaults

Delay time is set to 100 milliseconds.

Command Modes

Global configuration

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 set the 802.1x critical recovery delay time to 500:

```
Switch(config-if)# dot1x critical recovery delay 500
Switch(config-if)#
```

Related Commands

dot1x critical
dot1x critical eapol
dot1x critical vlan
show dot1x

dot1x critical vlan

To assign a critically authenticated port to a specific VLAN, use the **dot1x critical vlan** command. To return to the default setting, use the **no** form of this command

dot1x critical vlan *vlan-id*

no dot1x critical *vlan-id*

Syntax Description

vlan-id	(Optional) Specifies the VLANs; valid values are from 1 to 4094.

Defaults

Critical authentication is disabled on a ports VLAN.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The type of VLAN specified must match the type of the port. If the port is an access port, the VLAN must be a regular VLAN. If the port is a private-VLAN host port, the VLAN must be the secondary VLAN of a valid private-VLAN domain. If the port is a routed port, no VLAN may be specified.

This command is not supported on platforms such as Layer 3 switches that do not include the Critical Auth VLAN subsystem.

Examples

This example shows how to enable 802.1x critical authentication on a ports VLAN:

```
Switch(config-if)# dot1x critical vlan 350
Switch(config-if)#
```

Related Commands

dot1x critical
dot1x critical eapol
dot1x critical recovery delay
show dot1x

dot1x guest-vlan

To enable a guest VLAN on a per-port basis, use the **dot1x guest-vlan** command. To return to the default setting, use the **no** form of this command.

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan *vlan-id*

Syntax Description

vlan-id	Specifies a VLAN in the range of 1 to 4094.

Defaults

None; the guest VLAN feature is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
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.

Usage Guidelines

Guest VLANs can be configured only on ports that are statically configured as access ports or private VLAN host ports. Statically configured access ports can be configured with regular VLANs as guest VLANs; statically configured private VLAN host ports can be configured with secondary private VLANs as guest VLANs.

Examples

This example shows how to enable a guest VLAN on Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 26
Switch(config-if)# end
Switch(config)# end
Switch#
```

Related Commands

dot1x max-reauth-req
show dot1x

dot1x guest-vlan supplicant

To place an 802.1X-capable supplicant (host) into a guest VLAN, use the **dot1x guest-vlan supplicant** global configuration command. To return to the default setting, use the **no** form of this command.

dot1x quest-vlan supplicant

no dot1x quest-vlan supplicant

Syntax Description

This command has no arguments or keywords.

Defaults

802.1X-capable hosts are not put into a guest VLAN.

Command Modes

Global configuration

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

dot1x system-auth-control
show dot1x

dot1x host-mode

Use the **dot1x host-mode** interface configuration command on the switch stack or on a standalone switch to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port. Use the **multi-domain** keyword to enable multidomain authentication (MDA) on an IEEE 802.1x-authorized port. Use the **no** form of this command to return to the default setting.

dot1x host-mode {**multi-host** | **single-host** | **multi-domain**}

no dot1x host-mode [**multi-host** | **single-host** | **multi-domain**}

Syntax Description

multi-host	Enable multiple-hosts mode on the switch.
single-host	Enable single-host mode on the switch.
multi-domain	Enable MDA on a switch port.

Defaults

The default is single-host mode.

Command Modes

Interface configuration

Command History

Release	Modification
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.

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

show dot1x

dot1x initialize

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

dot1x initialize *interface*

Syntax Description

interface	Number of the interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command to initialize state machines and to set up the environment for fresh authentication.

Examples

This example shows how to initialize the 802.1X state machines on an interface:

```
Switch# dot1x initialize
Switch#
```

Related Commands

dot1x initialize
show dot1x

dot1x mac-auth-bypass

To enable the 802.1X MAC address bypassing on a switch, use the **dot1x mac-auth-bypass** command. Use the **no** form of this command to disable MAC address bypassing.

dot1x mac-auth-bypass [**eap**]

no dot1x mac-auth-bypass [**eap**]

Syntax Description

eap	(Optional) Specifies using EAP MAC address authentication.

Defaults

There is no default setting.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The removal of the **dot1x mac-auth-bypass** configuration from a port does not affect the authorization or authentication state of a port. If the port is in unauthenticated state, it remains unauthenticated, and if MAB is active, the authentication will revert back to the 802.1X Authenticator. If the port is authorized with a MAC address, and the MAB configuration is removed the port remains authorized until re-authentication takes place. When re-authentication occurs the MAC address is removed in favor of an 802.1X supplicant, which is detected on the wire.

Examples

This example shows how to enable EAP MAC address authentication:

```
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)#
```

dot1x max-reauth-req

To set the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process, use the **dot1x max-reauth-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-reauth-req *count*

no dot1x max-reauth-req

Syntax Description

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

Defaults

The switch sends a maximum of two retransmissions.

Command Modes

Interface configuration.

Command History

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

Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers. This setting impacts the wait before a non-dot1x-capable client is admitted to the guest VLAN, if one is configured.

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Examples

This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request/Identity frame before restarting the authentication process:

```
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)#
```

Related Commands

show dot1x

dot1x max-req

To set the maximum number of times that the switch retransmits an Extensible Authentication Protocol (EAP)-Request frame of types other than EAP-Request/Identity to the client before restarting the authentication process, use the **dot1x max-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-req *count*

no dot1x max-req

Syntax Description

count	Number of times that the switch retransmits EAP-Request frames of types other than EAP-Request/Identity before restarting the authentication process; valid values are from 1 to 10.

Defaults

The switch sends a maximum of two retransmissions.

Command Modes

Interface configuration

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)#
```

Related Commands

dot1x initialize
dot1x max-reauth-req
show dot1x

dot1x port-control

To enable manual control of the authorization state on a port, use the **dot1x port-control** command. To return to the default setting, use the **no** form of this command.

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

Syntax Description

auto	Enables 802.1X authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the switch and the client.
force-authorized	Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
force-unauthorized	Denies all access through the specified interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

Defaults

The port 802.1X authorization is disabled.

Command Modes

Interface configuration

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.

- 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 usingthe **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

show dot1x

dot1x re-authenticate

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port, use the **dot1x re-authenticate** command.

dot1x re-authenticate [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Module and port number of the interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

Examples

This example shows how to manually reauthenticate the device connected to Gigabit Ethernet interface 1/1:

```
Switch# dot1x re-authenticate interface gigabitethernet1/1
Starting reauthentication on gigabitethernet1/1
Switch#
```

dot1x re-authentication

To enable the periodic reauthentication of the client, use the **dot1x re-authentication** command. To return to the default setting, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

The periodic reauthentication is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You configure the amount of time between the periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples

This example shows how to disable the periodic reauthentication of the client:

```
Switch(config-if)# no dot1x re-authentication
Switch(config-if)#
```

This example shows how to enable the periodic reauthentication and set the number of seconds between the reauthentication attempts to 4000 seconds:

```
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout re-authperiod 4000
Switch#
```

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Related Commands

dot1x timeout
show dot1x

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

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

dot1x initialize
show dot1x

dot1x timeout

To set the reauthentication timer, use the **dot1x timeout** command. To return to the default setting, use the **no** form of this command.

dot1x timeout {**reauth-period** {*seconds* | **server**} | **quiet-period** *seconds* | **tx-period** *seconds* | **supp-timeout** *seconds* | **server-timeout** *seconds*}

no dot1x timeout {**reauth-period** | **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout**}

Syntax Description

reauth-period *seconds*	Number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the "Usage Guidelines" section for more information.
reauth-period server	Number of seconds between reauthentication attempts; valid values are from 1 to 65535 as derived from the Session-Timeout RADIUS attribute. See the "Usage Guidelines" section for more information.
quiet-period *seconds*	Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client; valid values are from 0 to 65535 seconds.
tx-period *seconds*	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request; valid values are from 1 to 65535 seconds.
supp-timeout *seconds*	Number of seconds that the switch waits for the retransmission of EAP-Request packets; valid values are from 30 to 65535 seconds.
server-timeout *seconds*	Number of seconds that the switch waits for the retransmission of packets by the back-end authenticator to the authentication server; valid values are from 30 to 65535 seconds.

Defaults

The default settings are as follows:

- Reauthentication period is 3600 seconds.
- Quiet period is 60 seconds.
- Transmission period is 30 seconds.
- Supplicant timeout is 30 seconds.
- Server timeout is 30 seconds.

Command Modes

Interface configuration

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

dot1x initialize
show dot1x

duplex

To configure the duplex operation on an interface, use the **duplex** command. To return to the default setting, use the **no** form of this command.

duplex {**auto** | **full** | **half**}

no duplex

Syntax Description

auto	Specifies the autonegotiation operation.
full	Specifies the full-duplex operation.
half	Specifies the half-duplex operation.

Defaults

Half-duplex operation

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Table 2-2 lists the supported command options by interface.

Table 2-2 Supported duplex Command Options

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	**duplex** [**half** | **full**]	**half**	If the speed is set to **auto**, you will not be able to set the **duplex** mode. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex mode is set to **half** duplex.
100-Mbps fiber modules	**duplex** [**half** | **full**]	**half**	
Gigabit Ethernet Interface	Not supported.	Not supported.	Gigabit Ethernet interfaces are set to **full** duplex.
10/100/1000	**duplex** [**half** | **full**]		If the speed is set to **auto** or **1000**, you will not be able to set **duplex**. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex mode is set to **half** duplex.

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to **1000**, the duplex mode is set to **full**. If the transmission speed is changed to **10** or **100**, the duplex mode stays at **full**. You must configure the correct duplex mode on the switch when the transmission speed changes to **10** or **100** from 1000 Mbps.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Table 2-3 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 2-3 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half or **duplex full**	**speed auto**	Autonegotiates both speed and duplex modes
duplex half	**speed 10**	Forces 10 Mbps and half duplex
duplex full	**speed 10**	Forces 10 Mbps and full duplex
duplex half	**speed 100**	Forces 100 Mbps and half duplex
duplex full	**speed 100**	Forces 100 Mbps and full duplex
duplex full	**speed 1000**	Forces 1000 Mbps and full duplex

Examples

This example shows how to configure the interface for full-duplex operation:

```
Switch(config-if)# duplex full
Switch(config-if)#
```

Related Commands

speed
interface (refer to Cisco IOS documentation)
show controllers (refer to Cisco IOS documentation)
show interfaces (refer to Cisco IOS documentation)

erase

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

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

Syntax Description

/all nvram:	Erases everything in nvram:.
/all non-default	Erases files and configuration in non-volatile storage including nvram:, bootflash:, cat4000_flash:, and crashinfo: of the local supervisor engine. Resets the Catalyst 4500 series switch to the factory default settings. **Note** This command option is intended to work only on a stand-alone supervisor engine.
cat4000_flash:	Erases the VLAN database configuration file.
nvram:	Erases the startup-config and private-config file in nvram.
startup-config:	Erases the startup-config and private-config file in nvram.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
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 (like slavenvram: and slavecat4000_flash:) appear in the command help messages on the dual supervisor redundancy switch.

The **erase nvram:** command replaces the **write erase** and the **erase startup-confg** commands. Like these two commands, it 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 non-volatile storage and resets the Catalyst 4500 series switch to the factory default settings. The default settings include those mentioned in the IOS library (below) 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).

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2, at this URL:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book.html
- *Cisco IOS Configuration Fundamentals Configuration Command Reference*, Release 12.2, at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html

Caution The erase /all non-default command can erase IOS images in bootflash:. Ensure that 1) an 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 2) 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 non-volatile storage and reset the switch to factory default settings:

```
Switch# erase /all non-default
Switch#
Erase and format operation will destroy all data in non-volatile storage.  Continue?
[confirm]
Formatting bootflash: ...

Format of bootflash complete
Erasing nvram:
Erasing cat4000_flash:
Clearing crashinfo:data
Clearing the last power failure timestamp
Clearing all ROMMON variables
Setting default ROMMON variables:
     ConfigReg=0x2101
     PS1=rommon ! >
     EnableAutoConfig=1
Setting vtp mode to transparent
%WARNING! Please reboot the system for the changes to take effect
Switch#
00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

This example shows how to erase the contents in nvram.

```
Switch# erase /all nvram:
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
00:38:10: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram
Switch#
```

This example shows how to erase filesystem cat4000_flash.

```
Switch# erase cat4000_flash:
Erasing the cat4000_flash filesystem will remove all files! Continue? [confirm]
[OK]
Erase of cat4000_flash:complete
Switch#
```

Related Commands

boot config (refer to Cisco IOS documentation)
delete (refer to Cisco IOS documentation)
more nvram:startup-config: (refer to Cisco IOS documentation)
show bootvar
undelete (refer to Cisco IOS documentation)

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** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap**}

no errdisable detect cause {**all** | **arp-inspection** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap**}

Syntax Description

cause	Specifies error-disable detection to detect from a specific cause.
all	Specifies error-disable detection for all error-disable causes.
arp-inspection	Specifies the detection for the ARP inspection error-disable cause.
dhcp-rate-limit	Specifies the detection for the DHCP rate-limit error-disable cause.
dtp-flap	Specifies the detection for the DTP flap error-disable cause.
gbic-invalid	Specifies the detection for the GBIC invalid error-disable cause.
l2ptguard	Specifies the detection for the Layer 2 protocol-tunnel error-disable cause.
link-flap	Specifies the detection for the link flap error-disable cause.
pagp-flap	Specifies the detection for the PAgP flap error-disable cause.

Defaults

All error-disable causes are detected.

Command Modes

Global configuration

Command History

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

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.

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 disable error-disable detection for DAI:

```
Switch(config)# no errdisable detect cause arp-inspection
Switch(config)# end
Switch# show errdisable detect
ErrDisable Reason    Detection status
-----------------    ----------------
udld                 Enabled
bpduguard            Enabled
security-violatio    Enabled
channel-misconfig    Disabled
psecure-violation    Enabled
vmps                 Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
l2ptguard            Enabled
gbic-invalid         Enabled
dhcp-rate-limit      Enabled
unicast-flood        Enabled
storm-control        Enabled
ilpower              Enabled
arp-inspection       Disabled
Switch#
```

Related Commands

show errdisable detect
show interfaces status

errdisable recovery

To configure the recovery mechanism variables, use the **errdisable recovery** command. To return to the default setting, use the **no** form of this command.

errdisable recovery [**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **storm-control** | **udld** | **unicastflood** | **vmps**} [**arp-inspection**] [**interval** {*interval*}]]

no errdisable recovery [**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **storm-control** | **udld** | **unicastflood** | **vmps**} [**arp-inspection**] [**interval** {*interval*}]]

Syntax Description

cause	(Optional) Enables the error-disable recovery to recover from a specific cause.
all	(Optional) Enables the recovery timers for all error-disable causes.
arp-inspection	(Optional) Enables the recovery timer for the ARP inspection cause.
bpduguard	(Optional) Enables the recovery timer for the BPDU guard error-disable cause.
channel-misconfig	(Optional) Enables the recovery timer for the channel-misconfig error-disable cause.
dhcp-rate-limit	(Optional) Enables the recovery timer for the DHCP rate limit error-disable cause.
dtp-flap	(Optional) Enables the recovery timer for the DTP flap error-disable cause.
gbic-invalid	(Optional) Enables the recovery timer for the GBIC invalid error-disable cause.
l2ptguard	(Optional) Enables the recovery timer for the Layer 2 protocol-tunnel error-disable cause.
link-flap	(Optional) Enables the recovery timer for the link flap error-disable cause.
pagp-flap	(Optional) Enables the recovery timer for the PAgP flap error-disable cause.
pesecure-violation	(Optional) Enables the recovery timer for the pesecure violation error-disable cause.
security-violation	(Optional) Enables the automatic recovery of ports disabled due to 802.1X security violations.
storm-control	(Optional) Enables the timer to recover from storm-control error-disable state.
udld	(Optional) Enables the recovery timer for the UDLD error-disable cause.
unicastflood	(Optional) Enables the recovery timer for the unicast flood error-disable cause.
vmps	(Optional) Enables the recovery timer for the VMPS error-disable cause.
arp-inspection	(Optional) Enables the ARP inspection cause and recovery timeout.
interval *interval*	(Optional) Specifies the time to recover from a specified error-disable cause; valid values are from 30 to 86400 seconds.

Defaults

Error disable recovery is disabled.

The recovery interval is set to 300 seconds.

Command Modes

Configuration

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
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Enabled
```

```
Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Switch#
```

Related Commands

show errdisable recovery
show interfaces status

flowcontrol

To configure a Gigabit Ethernet interface to send or receive pause frames, use the **flowcontrol** command. To disable the flow control setting, use the **no** form of this command.

flowcontrol {**receive** | **send**} {**off** | **on** | **desired**}

no flowcontrol {**receive** | **send**} {**off** | **on** | **desired**}

Syntax Description

receive	Specifies that the interface processes pause frames.
send	Specifies that the interface sends pause frames.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Obtains predictable results whether a remote port is set to on, off, or desired.

Defaults

The default settings for Gigabit Ethernet interfaces are as follows:

- Sending pause frames is off—non-oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—non-oversubscribed Gigabit Ethernet interfaces.
- Sending pause frames is on—Oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—Oversubscribed Gigabit Ethernet interfaces

Table 2-4 shows the default settings for the modules.

Table 2-4 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

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 2-5 describes the guidelines for using the different configurations of the **send** and **receive** keywords with the **flowcontrol** command.

Table 2-5 Keyword Configurations for send and receive

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

Table 2-6 identifies how the flow control will be forced or negotiated on the Gigabit Ethernet interfaces based on their speed settings.

Table 2-6 Send Capability by Switch Type, Module, and Port

Interface Type	Configured Speed	Advertised Flow Control
10/100/1000BASE-TX	Speed 1000	Configured flow control always
1000BASE-T	Negotiation always enabled	Configured flow control always negotiated
1000BASE-X	No speed nonegotiation	Configured flow control negotiated
1000BASE-X	Speed nonegotiation	Configured flow control forced

Examples

This example shows how to enable send flow control:

```
Switch(config-if)# flowcontrol receive on
Switch(config-if)#
```

This example shows how to disable send flow control:

```
Switch(config-if)# flowcontrol send off
Switch(config-if)#
```

This example shows how to set receive flow control to desired:

```
Switch(config-if)# flowcontrol receive desired
Switch(config-if)#
```

Related Commands

interface port-channel
interface range
interface vlan
show flowcontrol
show running-config (refer to Cisco IOS documentation)
speed

hw-module power

To turn the power off on a slot or line module, use the **no hw-module power** command. To turn the power back on, use the **hw-module power** command.

hw-module [**slot** | **module**] *number* **power**

no hw-module [**slot** | **module**] *number* **power**

Syntax Description

slot	(Optional) Specifies a slot on a chassis.
module	(Optional) Specifies a line module.
number	(Optional) Slot or module number.

Defaults

After a boot up, the power is on.

Command Modes

Global configuration

Command History

Release	Modification
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.

Examples

This example shows how to shut off power to a module in slot 5:

```
Switch# no hw-module slot 5 power
Switch#
```

Related Commands

clear hw-module slot password

hw-module uplink select

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

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

Syntax Description

tengigabitethernet	(Optional) Specifies the 10-Gigabit Ethernet uplinks.
gigabitethernet	(Optional) Specifies the Gigabit Ethernet uplinks.
all	(Optional) Specifies all uplinks (10-Gigabit Ethernet and Gigabit Ethernet).

Defaults

tengigabitethernet

Command Modes

Global configuration

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 **all** keyword was added.

Usage Guidelines

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.

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#
```

Note 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#
```

Note 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#
```

Note 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#
```

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

Related Commands **show hw-module uplink**

instance

To map a VLAN or a set of VLANs to an MST instance, use the **instance** command. To return the VLANs to the common instance default, use the **no** form of this command.

instance *instance-id* {**vlans** *vlan-range*}

no instance *instance-id*

Syntax Description

instance-id	MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.
vlans *vlan-range*	Specifies the number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.

Defaults

Mapping is disabled.

Command Modes

MST configuration

Command History

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

Usage Guidelines

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing ones.

Any unmapped VLAN is mapped to the CIST instance.

Examples

This example shows how to map a range of VLANs to instance 2:

```
Switch(config-mst)# instance 2 vlans 1-100
Switch(config-mst)#
```

This example shows how to map a VLAN to instance 5:

```
Switch(config-mst)# instance 5 vlans 1100
Switch(config-mst)#
```

This example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Switch(config-mst)# no instance 2 vlans 40-60
Switch(config-mst)#
```

This example shows how to move all the VLANs mapped to instance 2 back to the CIST instance:

```
Switch(config-mst)# no instance 2
Switch(config-mst)#
```

Related Commands

name
revision
show spanning-tree mst
spanning-tree mst configuration