rcv-queue bandwidth

To define the bandwidths for ingress (receive) WRR queues through scheduling weights, use the **rcv-queue bandwidth** command. To return to the default settings, use the **no** form of this command.

rcv-queue bandwidth *weight-1 ... weight-n*

no rcv-queue bandwidth

Syntax Description

weight-1 ... weight-n	WRR weights; valid values are from 0 to 255.

Command Default

The defaults are as follows:

- QoS enabled—4:255
- QoS disabled—255:1

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 2.

This command is supported on 2q8t and 8q8t ports only.

You can configure up to seven queue weights.

Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# rcv-queue bandwidth 3 1
Router(config-if)#
```

Related Commands

Command	Description
rcv-queue queue-limit	Sets the size ratio between the strict-priority and standard receive queues.
show queueing interface	Displays queueing information.

rcv-queue cos-map

To map the CoS values to the standard receive-queue drop thresholds, use the **rcv-queue cos-map** command. To remove the mapping, use the **no** form of this command.

rcv-queue cos-map *queue-id threshold-id cos-1 ... cos-n*

no rcv-queue cos-map *queue-id threshold-id*

Syntax Description

queue-id	Queue ID; the valid value is **1**.
threshold-id	Threshold ID; valid values are from 1 to 4.
cos-1 ... cos-n	CoS values; valid values are from 0 to 7.

Command Default

The defaults are listed in Table 2-30.

Table 2-30 CoS-to-Standard Receive Queue Map Defaults

queue	threshold	cos-map	queue	threshold	cos-map
With QoS Disabled			**With QoS Enabled**		
1	1	0,1, 2,3,4,5,6,7	1	1	0,1
1	2		1	2	2,3
1	3		1	3	4
1	4		1	4	6,7
2	1	5	2	1	5

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *cos-n* value is defined by the module and port type. When you enter the *cos-n* value, note that the higher values indicate higher priorities.

Use this command on trusted ports only.

For additional information on configuring receive-queue thresholds, see the QoS chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Examples

This example shows how to map the CoS values 0 and 1 to threshold 1 in the standard receive queue:

```
Router (config-if)# rcv-queue cos-map 1 1 0 1
  cos-map configured on:  Gi1/1 Gi1/2
Router(config-if)#
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue queue-limit

To set the size ratio between the strict-priority and standard receive queues, use the **rcv-queue queue-limit** command. To return to the default settings, use the **no** form of this command.

rcv-queue queue-limit {*q-limit-1*} {*q-limit-2*}

no rcv-queue queue-limit

Syntax Description

q-limit-1	Standard queue weight; valid values are from 1 and 100 percent.
q-limit-2	Strict-priority queue weight; see the "Usage Guidelines" section for valid values.

Command Default

The defaults are as follows:

- **80** percent is for low priority.
- **20** percent is for strict priority.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Valid strict-priority weight values are from 1 to 100 percent, except on 1p1q8t ingress LAN ports, where valid values for the strict-priority queue are from 3 to 100 percent.

The **rcv-queue queue-limit** command configures ports on a per-ASIC basis.

Estimate the mix of strict-priority-to-standard traffic on your network (for example, 80-percent standard traffic and 20-percent strict-priority traffic) and use the estimated percentages as queue weights.

Examples

This example shows how to set the receive-queue size ratio for Gigabit Ethernet interface 1/2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
Router#
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue random-detect

To specify the minimum and maximum threshold for the specified receive queues, use the **rcv-queue random-detect** command. To return to the default settings, use the **no** form of this command.

rcv-queue random-detect {**max-threshold** | **min-threshold**} *queue-id threshold-percent-1 ... threshold-percent-n*

no rcv-queue random-detect {**max-threshold** | **min-threshold**} *queue-id*

Syntax Description

max-threshold	Specifies the maximum threshold.
min-threshold	Specifies the minimum threshold.
queue-id	Queue ID; the valid value is **1**.
threshold-percent-1 threshold-percent-n	Threshold weights; valid values are from 1 to 100 percent.

Command Default

The defaults are as follows:

- **min-threshold**—80 percent
- **max-threshold**—20 percent

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on 1p1q8t and 8q8t ports only.

The 1p1q8t interface indicates one strict queue and one standard queue with eight thresholds. The 8q8t interface indicates eight standard queues with eight thresholds. The threshold in the strict-priority queue is not configurable.

Each threshold has a low- and a high-threshold value. The threshold values are a percentage of the receive-queue capacity.

For additional information on configuring receive-queue thresholds, refer to the QoS chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Examples

This example shows how to configure the low-priority receive-queue thresholds:

```
Router (config-if)# rcv-queue random-detect max-threshold 1 60 100
Router (config-if)#
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue threshold

To configure the drop-threshold percentages for the standard receive queues on 1p1q4t and 1p1q0t interfaces, use the **rcv-queue threshold** command. To return the thresholds to the default settings, use the **no** form of this command.

rcv-queue threshold *queue-id threshold-percent-1 ... threshold-percent-n*

no rcv-queue threshold

Syntax Description

queue-id	Queue ID; the valid value is **1**.
threshold- percent-1 ... threshold- percent-n	Threshold ID; valid values are from 1 to 100 percent.

Command Default

The defaults for the 1p1q4t and 1p1q0t configurations are as follows:

- QoS assigns all traffic with CoS 5 to the strict-priority queue.
- QoS assigns all other traffic to the standard queue.

The default for the 1q4t configuration is that QoS assigns all traffic to the standard queue.

If you enable QoS, the following default thresholds apply:

- 1p1q4t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue.
  - Using standard receive-queue drop threshold 1, the Catalyst 6500 series switch drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
  - Using standard receive-queue drop threshold 2, the Catalyst 6500 series switch drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
  - Using standard receive-queue drop threshold 3, the Catalyst 6500 series switch drops incoming frames with CoS 4 when the receive-queue buffer is 80 percent or more full.
  - Using standard receive-queue drop threshold 4, the Catalyst 6500 series switch drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Catalyst 6500 series switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- 1p1q0t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue. The Catalyst 6500 series switch drops incoming frames when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Catalyst 6500 series switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.

Note The 100-percent threshold may be actually changed by the module to 98 percent to allow BPDU traffic to proceed. The BPDU threshold is factory set at 100 percent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *queue-id* value is always **1**.

A value of **10** indicates a threshold when the buffer is 10 percent full.

Always set threshold 4 to 100 percent.

Receive thresholds take effect only on ports whose trust state is **trust cos**.

Configure the 1q4t receive-queue tail-drop threshold percentages with the **wrr-queue threshold** command.

Examples

This example shows how to configure the receive-queue drop thresholds for Gigabit Ethernet interface 1/1:

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
Router(config-if)#
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue threshold	Configures the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces.

reassign

To define the number of consecutive number of SYNs for a new connection that will go unanswered before the connection is attempted to a different real server, use the **reassign** command. To change the maximum number of connections to the default settings, use the **no** form of this command.

reassign *threshold*

no reassign

Syntax Description

threshold	Number of unanswered TCP SYNs that will be directed to a real server before the connection is reassigned to a different real server; valid values are from 1 to 4.

Command Default

threshold is **3**.

Command Modes

Real server configuration submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you do not specify the *threshold* value, the default value of the reassignment threshold is used.

Examples

This example shows how to define the reassignment threshold:

```
Router(config-if)# reassign 4
Router(config-if)#
```

This example shows how to revert to the default value:

```
Router(config-if)# no reassign
Router(config-if)#
```

Related Commands

Command	Description
faildetect numconns	Specifies the conditions that indicate a server failure.
inservice (real server)	Enables the real server for use by the Cisco IOS SLB feature.
retry	Defines the amount of time that must elapse before a connection is attempted to a failed server.
maxconns (real server configuration submode)	Limits the number of active connections to the real server.

redundancy

To enter redundancy configuration mode, use the **redundancy** command. From this mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Once you enter redundancy configuration mode, these options are available:

- **exit**—Exits from redundancy configuration mode.
- **main-cpu**—Enters the main CPU submode.
- **no**—Negates a command or sets its defaults.

From the main CPU submode, you can use the **auto-sync** command to use all of the redundancy commands that are applicable to the main CPU.

To select the type of redundacy mode, use the **mode** command.

NSF with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, IPX, and MPLS.

Examples

This example shows how to enter redundancy mode:

```
Router (config)# redundancy
Router(config-r)#
```

This example shows how to enter the main CPU submode:

```
Router (config)# redundancy
Router (config-r)# main-cpu
Router (config-r-mc)#
```

Related Commands

Command	Description
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
mode	Sets the redundancy mode.

redundancy force-switchover

To force a switchover from the active to the standby supervisor engine, use the **redundancy force-switchover** command.

redundancy force-switchover

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Before using this command, see the "Performing a Fast Software Upgrade (FSU)" section of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional information.

The **redundancy force-switchover** command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the new Cisco IOS image. The modules are reset and the module software is downloaded from the new active supervisor engine.

The old active supervisor engine reboots with the new image and becomes the redundant supervisor engine.

Examples

This example shows how to switch over manually from the active to the standby supervisor engine:

```
Router# redundancy force-switchover
Router#
```

Related Commands

Command	Description
mode	Sets the redundancy mode.
redundancy	Enters redundancy configuration mode.
show redundancy	Displays RF information.

reload

To reload the entire Catalyst 6500 series switch, use the **reload** command.

reload [*text* | **in** [*hh***:**]*mm* [*text*] | **at** *hh***:***mm* [*month day* | *day month*] [*text*] | **cancel**]

Syntax Description

text	(Optional) Reason for the reload; the string can be from 1 to 255 characters.
in [*hh***:**]*mm*	(Optional) Delays a Catalyst 6500 series switch reload for a specific amount of time.
at *hh***:***mm*	(Optional) Schedules a Catalyst 6500 series switch reload to take place at the specified time (using a 24-hour clock).
month	(Optional) Name of the month; any number of characters in a unique string.
day	(Optional) Number of the day; valid values are from 1 to 31.
cancel	(Optional) Cancels a scheduled reload.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **reload** command stops the system. If the system is set to restart on error, it reboots itself. Use the **reload** command after you enter configuration information into a file and the file is saved to the startup configuration.

When you schedule a reload to occur at a later time (using the **in** keyword), it must take place within approximately 24 days.

When specifying the reload time (using the **at** keyword), if you specify the month and day, the reload takes place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days.

If you modify your configuration file, the Catalyst 6500 series switch prompts you to save the configuration. During a save operation, the Catalyst 6500 series switch asks you if you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you say “yes” in this situation, the Catalyst 6500 series switch goes to setup mode upon reload.

You can use the **at** keyword if the system clock has been set on the MSM (either through NTP, the hardware calendar, or manually). To schedule reloads across several MSMs to occur simultaneously, you must synchronize the time on each MSM with NTP.

To display information about a scheduled reload, use the **show reload** command.

Examples

This example shows how to reload the Catalyst 6500 series switch immediately:

```
Router# reload
Router#
```

This example shows how to reload the Catalyst 6500 series switch in 10 minutes:

```
Router# reload in 10
Router# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reload? [confirm]
Router#
```

This example shows how to reload the Catalyst 6500 series switch at 1:00 p.m. today:

```
Router# reload at 13:00
Router# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
Router#
```

This example shows how to reload the Catalyst 6500 series switch on April 20 at 2:00 a.m.:

```
Router# reload at 02:00 apr 20
Router# Reload scheduled for 02:00:00 PDT Sat Apr 20 1996 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
Router#
```

This example shows how to cancel a pending reload:

```
Router# reload cancel
%Reload cancelled.
Router#
```

Related Commands

Command	Description
copy system:running-config nvram:startup-config	Saves configuration changes to the startup configuration.
show reload	Displays the reload status on the router.

remote command

To execute a Catalyst 6500 series switch command directly on the switch console or a specified module without having to log into the Catalyst 6500 series switch first, use the **remote command** command.

remote command {{**module** *num*} | **standby-rp** | **switch**} *command*

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.
command	Command to be executed.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on the standby supervisor engine only.

When you execute the **remote command switch** command, the prompt changes to Switch-sp#.

This command is supported on the supervisor engine only.

This command does not support command completion, but you can use shortened forms of the command (for example, entering **sh** for **show**).

Examples

This example shows how to execute the **show calendar** command from the standby route processor:

```
Router# remote command standby-rp show calendar
Switch-sp#
09:52:50 UTC Mon Nov 12 2001
Router#
```

Related Commands

Command	Description
remote login	Accesses the Catalyst 6500 series switch console or a specific module.

remote login

To access the Catalyst 6500 series switch console or a specific module, use the **remote login** command.

remote login {{**module** *num*} | **standby-rp** | **switch**}

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Caution When you enter the **attach** or **remote login** command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on the standby supervisor engine only.

When you execute the **remote login module** *num* command, the prompt changes depending on the type of module to which you are connecting.

When you execute the **remote login standby-rp** command, the prompt changes to Router-sdby#.

When you execute the **remote login switch** command, the prompt changes to Switch-sp#.

The **remote login module** *num* command is identical to the **attach** command.

There are two ways to end the session:

- You can enter the **exit** command as follows:

```
Switch-sp# exit

[Connection to Switch closed by foreign host]
Router#
```

- You can press **Ctrl-C** three times as follows:

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

Examples

This example shows how to perform a remote login to a specific module:

```
Router# remote login module 1
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session


Switch-sp#
```

This example shows how to perform a remote login to the Catalyst 6500 series switch processor:

```
Router# remote login switch
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the standby route processor:

```
Router# remote login standby-rp
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Router-sdby#
```

Related Commands

Command	Description
attach	Connects to a specific module from a remote location.

remote-span

To configure a VLAN as an RSPAN VLAN, use the **remote-span** command. To remove the RSPAN designation, use the **no** form of this command.

remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

config-VLAN (config-vlan)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is not supported in the VLAN database mode.

You can enter the **show vlan remote-span** command to display the RSPAN VLANs in the Catalyst 6500 series switch.

Examples

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Router(config-vlan)# remote-span
Router(config-vlan)
```

This example shows how to remove the RSPAN designation:

```
Router(config-vlan)# no remote-span
Router(config-vlan)
```

Related Commands

Connect	Description
show vlan remote-span	Displays a list of RSPAN VLANs.

reset

To leave the proposed new VLAN database, remain in VLAN configuration mode, and reset the proposed new database so that it is identical to the current VLAN database, use the **reset** command.

reset

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

VLAN configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to cause the proposed new VLAN database to be abandoned and reset to the current VLAN database:

```
Router(vlan)# reset
RESET completed.
Router(vlan)#
```

retry

To define the amount of time that must elapse before a connection is attempted to a failed server, use the **retry** command. To change the connection-reassignment threshold and client threshold to the default settings, use the **no** form of this command.

retry *retry-value*

no retry

Syntax Description

retry-value	Amount of time, in seconds, that must elapse after the detection of a server failure before a new connection is attempted to the server; valid values are from 1 to 3600.

Command Default

retry-value is **60**.

Command Modes

Real server configuration submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to define the retry timer:

```
Router(config-if)# retry 145
Router(config-if)#
```

This example shows how to revert to the default value:

```
Router(config-if)# no retry
Router(config-if)#
```

Related Commands

Command	Description
faildetect numconns	Specifies the conditions that indicate a server failure.
inservice (real server)	Enables the real server for use by the Cisco IOS SLB feature.
maxconns (real server configuration submode)	Limits the number of active connections to the real server.

revision

To set the revision number for the MST configuration, use the **revision** command. To return to the default settings, use the **no** form of this command.

revision *version*

no revision

Syntax Description

version	Revision number for the configuration; valid values are from 0 to 65535.

Command Default

version is **0**.

Command Default

MST configuration submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Two Catalyst 6500 series switches that have the same configuration but different revision numbers are considered to be part of two different regions.

Caution Be careful when using the **revision** command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

Examples

This example shows how to set the revision number of the MST configuration:

```
Router(config-mst)# revision 5
Router(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration submode)	Sets the name of an MST region.
show	Verifies the MST configuration.
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree mst configuration	Enters MST-configuration submode.

rmon alarm

To set an alarm on any MIB object, use the **rmon alarm** command. To disable the alarm, use the **no** form of this command.

rmon alarm *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]

no rmon alarm *number*

Syntax Description

number	Alarm number that is identical to the alarmIndex in the alarmTable in the RMON MIB; valid values are from 1 to 65535.
variable	MIB object to monitor; this value translates into the alarmVariable that is used in the alarmTable of the RMON MIB.
interval	Time in seconds that the alarm monitors the MIB variable. This value is identical to the alarmInterval that is used in the alarmTable of the RMON MIB; valid values are from 1 to 4294967295.
delta	Specifies the change between MIB variables; this value affects the alarmSampleType in the alarmTable of the RMON MIB.
absolute	Specifies each MIB variable directly; this value affects the alarmSampleType in the alarmTable of the RMON MIB.
rising-threshold *value*	Specifies the value at which the alarm is triggered; valid values are from –2147483648 to 2147483647.
event-number	(Optional) Event number to trigger when the rising or falling threshold exceeds its limit. This value is identical to the alarmRisingEventIndex or the alarmFallingEventIndex in the alarmTable of the RMON MIB; valid values are from 1 to 65535.
falling-threshold *value*	Specifies the value at which the alarm is reset; valid values are from –2147483648 to 2147483647.
owner *string*	(Optional) Specifies the owner for the alarm; this value is identical to the alarmOwner in the alarmTable of the RMON MIB.

Command Modes

No alarms are configured.

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must specify the MIB object as a dotted decimal value after the entry sequence (for example, ifEntry.10.1). You cannot specify the variable name and the instance (for example, ifInOctets.1) or the entire dotted decimal notation. The argument must be of the form entry.integer.instance.

To disable the RMON alarms, you must use the **no** form of the command on each configured alarm. For example, enter the **no rmon alarm 1** command, where the 1 identifies which alarm is to be removed.

Refer to RFC 1757 for more information about the RMON alarm group.

In the configuration that is shown in the example, the alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled and checks the change in the variable's rise or fall. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm triggers event number 1, which is configured with the **rmon event** command. Possible events include a log entry or an SNMP trap. If the *ifEntry.20.1* value changes by 0 (falling-threshold 0), the alarm is reset and can be triggered again.

Examples

This example shows how to configure an RMON alarm:

```
Router(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0
     owner jjohnson
```

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon event	Adds or removes an event in the RMON-event table that is associated with an RMON-event number.
show rmon	Displays the current RMON agent status on the router.

rmon event

To add or remove an event in the RMON-event table that is associated with an RMON-event number, use the **rmon event** command. To disable RMON on the interface, use the **no** form of this command.

rmon event *number* [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*]

no rmon event *number*

Syntax Description

number	Assigned event number that is identical to the eventIndex in the eventTable in the RMON MIB; valid values are from 1 to 65535.
log	(Optional) Generates an RMON log entry when the event is triggered and sets the eventType in the RMON MIB to log or log-and-trap.
trap *community*	(Optional) Specifies the SNMP community string that is used for this trap.
description *string*	(Optional) Specifies a description of the event that is identical to the event description in the eventTable of the RMON MIB.
owner *string*	(Optional) Specifies the owner of this event that is identical to the eventOwner in the eventTable of the RMON MIB.

Command Default

No alarms are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Refer to RFC 1757 for more information about the RMON MIB.

Use the **trap** *community* keyword and argument to configure the setting of the eventType in the RMON MIB for this row as either snmp-trap or log-and-trap. This value is identical to the eventCommunityValue in the eventTable in the RMON MIB.

Examples

This example shows how to add an event to the RMON-event table:

```
Router(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
sdurham
```

This example configuration creates RMON-event number 1, which is defined as High ifOutErrors, and generates a log entry when the event is triggered by an alarm. The user sdurham owns the row that is created in the event table by this command. This configuration also generates an SNMP trap when the event is triggered.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
rmon alarm	Sets an alarm on any MIB object.
show rmon	Displays the current RMON agent status on the router.

route-converge-interval

To configure the time interval after which the old FIB entries are purged, use the **route-converge-interval** command. To return to the default settings, use the **no** form of this command.

route-converge-interval *seconds*

Syntax Description

seconds	Time interval after which the old FIB entries are purged; valid values are from 60 to 3600 seconds.

Command Default

seconds is **120** seconds (2 minutes).

Command Modes

Main CPU submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The time interval for route-converge delay is needed to simulate the route-converge time when routing protocols restart on switchover.

Examples

This example shows how to set the time interval for the route-converge delay:

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-red-main)# route-converge-interval 90
Router(config-red-main)#
```

This example shows how to return to the default time interval for the route-converge delay:

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-red-main)# no route-converge-interval
Router(config-red-main)#
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.

router

To enable a routing process, use the **router** command. To terminate a routing process, use the **no** form of this command.

router {**bgp** *as-num*} | {**eigrp** *as-num*} | {**isis** *process-id*} | {**ospf** *process-id* [**vrf** *vrf-id*]}

no router ospf *process-id*

Syntax Description

bgp *as-num*	Specifies an autonomous BGP-system number; valid values are from 1 to 65535.
eigrp *as-num*	Specifies an autonomous EIGRP-system number; valid values are from 1 to 65535.
isis *routing-area-tag*	Specifies an ISO routing area designation.
ospf *process-id*	Specifies an internally used identification parameter for the routing process; valid values are from 1 to 65535.
vrf *vrf-id*	(Optional) Specifies a VRF instance name.

Command Default

No OSPF routing process is enabled or defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When you specify a *process-id,* it is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

You can specify multiple OSPF routing processes in each router.

Examples

This example shows how to configure an OSPF routing process and assign a process number of 109:

```
Router(config)# router ospf 109
Router(config)#
```

This example shows how to configure an OSPF routing process and assign a process number of 109 for a specific VRF instance:

```
Router(config)# router ospf 109 vrf 109
Router(config)#
```

Related Commands

Command	Description
nsf	Enables and configures Cisco NSF.

scheduler allocate

To guarantee the CPU time for the process tasks, use the **scheduler allocate** command. To return to the default settings, use the **no** form of this command.

scheduler allocate *interrupt-time process-time*

no scheduler allocate

Syntax Description

interrupt-time	Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network-interrupt context; valid values are from 400 to 60000 microseconds.
process-time	Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled; valid values are from 100 to 4000.

Command Default

The defaults are as follows:

- *interrupt-time* is **4000** microseconds.
- *process-time* is **800** microseconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Caution We recommend that you do not change the default settings.

Entering the **scheduler allocate** command without arguments is the same as entering the **no scheduler allocate** or the **default scheduler allocate** command.

Examples

This example shows how to make 20 percent of the CPU time available for the process tasks:

```
Router-config# scheduler allocate 2000 500
Router-config#
```

service counters max age

To set the time interval for retrieving statistics, use the **service counters max age** command. To return to the default settings, use the **no** form of this command.

service counters max age *seconds*

no service counters max age

Syntax Description

seconds	Maximum age of the statistics retrieved from the CLI or SNMP; valid values are from 0 to 60 seconds.

Command Default

seconds is **5** seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Note If you decrease the time interval for retrieving statistics from the default setting (5 seconds), traffic congestion may result in situations where frequent SNMP (SMNP bulk) retrievals occur.

If you configure the *seconds* value between 6 and 9 seconds, the counter update occurs at the 10-second default to ensure that the system is not too busy computing statistics. If the statistics collection uses more than 20 percent of the CPU time, the system automatically increases the time that the statistics process sleeps between counter updates.

If you configure the *seconds* value between 0 and 5 seconds, and if the CPU utility is low, the counter updates occur after the configured delay seconds which ensures that the system load is at 20 percent.

For example, if the statistics calculation time takes 4 seconds, and you have configured the service maximum age to 5 seconds, the period between statistics collections will be 20 seconds (the collection period equals the duration multiplied by 5) regardless of what you configured, which ensures that the statistics collection does not increase the CPU utility.

Examples

This example shows how to set the time interval for retrieving statistics:

```
Router(config)# service counters max age 10
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no service counters max age
Router(config)#
```

service-policy

To attach a policy map to an interface, use the **service-policy** command. To remove a policy map from an interface, use the **no** form of this command.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input *policy-map-name*	Specifies a previously configured input-policy map.
output *policy-map-name*	Specifies a previously configured output-policy map.

Command Default

No policy map is attached.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Do not attach a service policy to a port that is a member of an EtherChannel.

Although the CLI allows you to configure PFC-based QoS on the WAN ports on the OC-12 ATM OSMs and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs. OSMs are not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 32 PISA.

PFC QoS supports the optional **output** keyword only on VLAN interfaces. You can attach both an input-policy map and an output-policy map to a VLAN interface.

Examples

This example shows how to attach a policy map to a Fast Ethernet interface:

```
Router(config)# interface fastethernet 5/20
Router(config-if)# service-policy input pmap1
Router(config-if)#
```

Related Commands

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.

service-policy (control-plane)

To attach a policy map to a control plane for aggregate control plane services, use the **service-policy** command. To remove a service policy from a control plane, use the **no** form of this command.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input	Applies the specified service policy to the packets that are entering the control plane.
output	Applies the specified service policy to the packets that are exiting the control plane and enables the Catalyst 6500 series switch to silently discard packets.
policy-map-name	Name of a service policy map (created using the **policy-map** command) to be attached.

Command Default

No service policy is specified.

Command Modes

Control-plane configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *policy-map-name* can be a maximum of 40 alphanumeric characters.

After entering the **control-plane** command, you should use the **service-policy** command to configure a QoS policy. This policy is attached to the control plane interface for aggregate control plane services, which can control the number or rate of packets that are going to the process level.

Silent mode allows a router that is running Cisco IOS software to operate without sending any system messages. If a packet that is destined for the router is discarded for any reason, users will not receive an error message. Some events that will not generate error messages are as follows:

- Traffic that is being transmitted to a port in which that router is not listening
- A connection to a legitimate address and port that is rejected because of a malformed request

Examples

This example shows 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:

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
```

```
! Define class-map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# exit
```

This example shows how to configure trusted networks with source addresses 3.3.3.0 and 4.4.4.0 to receive Internet Control Message Protocol (ICMP) port-unreachable responses without constraint, while allowing all remaining ICMP port-unreachables to be dropped:

```
Router(config)# access-list 141 deny icmp host 3.3.3.0 0.0.0.255 any port-unreachable
! Allow 4.4.4.0 trusted network traffic.
Router(config)# access-list 141 deny icmp host 4.4.4.0 0.0.0.255 any port-unreachable
! Rate limit all other ICMP traffic.
Router(config)# access-list 141 permit icmp any any port-unreachable
Router(config)# class-map icmp-class
Router(config-cmap)# match access-group 141
Router(config-cmap)# exit
Router(config)# policy-map control-plane-out-policy
! Drop all traffic that matches the class "icmp-class."
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-policy
Router(config-cp)# exit
```

Related Commands

Command	Description
control-plane	Enters 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.
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
show policy-map control-plane	Displays the configuration either of a class or of all classes for the policy map of a control plane.

session slot

To open a session with a module (for example, the NAM), use the **session slot** command.

session slot *mod* {**processor** *processor-id*}

Syntax Description

mod	Slot number.
processor *processor-id*	Specifies the processor ID.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

To end the session, enter the **quit** command.

This command allows you to use the module-specific CLI.

Examples

This example shows how to open a session with an MSM (module 4):

```
Router# session slot 4 processor 2
Router#
```

set cos cos-inner (policy-map configuration)

To set the 802.1Q prioritization bits in the trunk VLAN tag of a QinQ-translated outgoing packet with the priority value from the inner customer-edge VLAN tag, use the **set cos cos-inner** command. To return to the default settings, use the **no** form of this command.

set cos cos-inner

no set cos cos-inner

Syntax Description

This command has no keywords or arguments.

Command Default

P bits are copied from the outer provider-edge VLAN tag.

Command Default

Policy-map class configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on the Gigabit Ethernet WAN interfaces on Catalyst 6500 series switches that are configured with an OSM-2+4GE-WAN+ OSM module only.

OSMs are not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 32.

The 802.1P prioritization bits are used in the VLAN tag for QoS processing.

When the router copies the double-tagged QinQ packets to the destination interface, by default it uses the P bits from the outer (provider) VLAN tag. To preserve the P bits that are in the inner (customer) VLAN tag, use the **set cos cos-inner** command.

For the **set cos cos-inner** command to be effective, you must configure the appropriate interface or subinterface as a trusted interface using the **mls qos trust** command. Otherwise, the interface or subinterface defaults to being untrusted, where the Layer 2 interface zeroes out the P bits of the incoming packets before the **set cos cos-inner** command can copy them to the outer VLAN tag.

The **set cos cos-inner** command is supported only for the subinterfaces that are configured with an inner (customer) VLAN. The **set cos cos-inner** command is not supported for the subinterfaces that use the **out-range** keyword on the **bridge-domain (subinterface configuration)** command or that are not configured with any form of the **bridge-domain (subinterface configuration)** command.

This behavior remains when you configure the **set cos cos-inner** command on a policy that is applied to a main interface. The **set cos cos-inner** command affects the subinterfaces that are configured with a specific inner VLAN but it does not affect the subinterfaces that are not configured with any VLAN or that are configured with the **out-range** keyword.

Examples

This example shows how to configure a policy map for voice traffic that uses the P bits from the inner VLAN tag:

```
Router(config-pmap-c)# set cos cos-inner
Router(config-pmap-c)#
```

This example shows how to configure the default policy map class to reset to its default value:

```
Router(config-pmap-c)# no set cos cos-inner
Router(config-pmap-c)#
```

This example shows the system message that appears when you attempt to apply a policy to a subinterface that is configured with the **bridge-domain (subinterface configuration)** command:

```
Router(config-if)# bridge-vlan 32 dot1q-tunnel out-range
Router(config-if)# service-policy output cos1

%bridge-vlan 32 does not have any inner-vlan configured. 'set cos cos-inner' is not
supported

Router(config-if)#
```

Related Commands

Command	Description
bridge-domain (subinterface configuration)	Binds a PVC to the specified *vlan-id*.
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
mode dot1q-in-dot1q access-gateway	Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation.
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
service-policy	Attaches a policy map to an interface.
set ip dscp (policy-map configuration)	Marks a packet by setting the IP DSCP in the ToS byte.
set ip precedence (policy-map configuration)	Sets the precedence value in the IP header.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

set ip dscp (policy-map configuration)

To mark a packet by setting the IP DSCP in the ToS byte, use the **set ip dscp** command. To remove a previously set IP DSCP, use the **no** form of this command.

set ip dscp *ip-dscp-value*

no set ip dscp *ip-dscp-value*

Syntax Description

ip-dscp-value	IP DSCP value; valid values are from 0 to 63. See the "Usage Guidelines" section for additional information.

Command Default

This command has no default settings.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can enter reserved keywords **EF** (expedited forwarding), **AF11** (assured forwarding class AF11), and **AF12** (assured forwarding class AF12) instead of numeric values for *ip-dscp-value*.

After the IP DSCP bit is set, other QoS services can operate on the bit settings.

You cannot mark a packet by the IP precedence using the **set ip precedence (policy-map configuration)** command and then mark the same packet with an IP DSCP value using the **set ip dscp** command.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set IP precedence at the edge of the network (or administrative domain); data is queued based on the precedence. WFQ can speed up handling for high-precedence traffic at congestion points. WRED ensures that high-precedence traffic has lower loss rates than other traffic during traffic congestion.

The **set ip precedence (policy-map configuration)** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not attached to an interface or to an ATM virtual circuit. See the **service-policy** command for information on attaching a service policy to an interface.

When configuring policy-map class actions, note the following:

- For hardware-switched traffic, PFC QoS does not support the **bandwidth**, **priority**, **queue-limit**, or **random-detect** policy-map class commands. You can configure these commands because they can be used for software-switched traffic.
- PFC QoS does not support the **set mpls** or **set qos-group** policy-map class commands.
- PFC QoS supports the **set ip dscp** and **set ip precedence** policy-map class commands (see the "Configuring Policy Map Class Marking" section in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*).

- You cannot do all three of the following in a policy-map class:
  - Mark traffic with the **set ip dscp** or **set ip precedence (policy-map configuration)** commands
  - Configure the trust state
  - Configure policing

  In a policy-map class, you can either mark traffic with the **set ip dscp** or **set ip precedence (policy-map configuration)** commands or do one or both of the following:
  - Configure the trust state
  - Configure policing

Examples

This example shows how to set the IP DSCP ToS byte to 8 in the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 8
```

All packets that satisfy the match criteria of class1 are marked with the IP DSCP value of 8. How packets that are marked with the IP DSCP value of 8 are treated is determined by the network configuration.

This example shows that after you configure the settings that are shown for voice packets at the edge of the network, all intermediate routers are then configured to provide low-latency treatment to the voice packets:

```
Router(config)# class-map voice
Router(config-cmap)# match ip dscp ef
Router(config)# policy qos-policy
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 24
```

Related Commands

Command	Description
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
service-policy	Attaches a policy map to an interface.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

set ip precedence (policy-map configuration)

To set the precedence value in the IP header, use the **set ip precedence** command. To leave the precedence value at the current setting, use the **no** form of this command.

set ip precedence *ip-precedence-value*

no set ip precedence

Syntax Description

ip-precedence-value	Precedence-bit value in the IP header; valid values are from 0 to 7. See Table 2-31 for a list of value definitions.

Command Default

This command is disabled by default.

Command Default

QoS policy-map configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Table 2-31 lists the value definitions for precedence values in the IP header. They are listed from least to most important.

Table 2-31 Value Definitions for IP Precedence

Values	Definitions
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

After the IP-precedence bits are set, other QoS services, such as WFQ and WRED, operate on the bit settings.

The network priorities (or some type of expedited handling) mark traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP precedence at the edge of the network (or administrative domain); data is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during traffic congestion.

The **set ip precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not attached to an interface or to an ATM virtual circuit. See the **service-policy** command for information on attaching a service policy to an interface.

Examples

This example shows how to set the IP precedence to 5 for packets that satisfy the match criteria of the class map called class1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip precedence 5
```

All packets that satisfy the match criteria of class1 are marked with the IP precedence value of **5**. How packets that are marked with the IP-precedence value of **5** are treated is determined by the network configuration.

Related Commands

Command	Description
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
service-policy	Attaches a policy map to an interface.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

set mpls experimental

To set the experimental value, use the **set mpls experimental** command. To return to the default settings, use the **no** form of this command.

set mpls experimental {{**imposition** | **topmost**} *experimental-value*}

Syntax Description

imposition	Specifies the experimental-bit value on IP to MPLS or MPLS input in all newly imposed labels.
topmost	Specifies the experimental-bit value on the topmost label on the input or output flows.
experimental-value	Experimental-bit value; valid values are from 0 to 7.

Command Default

This command is disabled by default.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to set the experimental-bit value on the topmost label on input or output:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set mpls experimental topmost 5
```

set qos-group

To set the trusted state of a Layer 2 WAN interface, use the **set qos-group** command. To return to the default settings, use the **no** form of this command.

set qos-group *group-value* {**cos** | **prec**}

Syntax Description

group-value	QoS group value; valid values are from 0 to 99.
cos	Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
prec	Specifies that the ToS bits in the incoming packets contain an IP-precedence value and derives the internal DSCP value from the IP-precedence bits.

Command Default

This command is disabled by default.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is entered in Pipe mode on the MPLS input to select the egress queue.

This command is supported on WAN interfaces only.

Use the **mls qos trust** command to set the trusted state on LAN interfaces.

Examples

This example shows how to set the trusted state of an interface to IP precedence:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 54 prec
Router(config-if)#
```

show

To verify the MST configuration, use the **show** command.

show [**current** | **pending**]

Syntax Description

current	(Optional) Displays the current configuration that is used to run MST.
pending	(Optional) Displays the edited configuration that will replace the current configuration.

Command Default

This command has no default settings.

Command Modes

MST configuration submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The display output from the **show pending** command is the edited configuration that will replace the current configuration if you enter the **exit** command to exit MST configuration mode.

Entering the **show** command with no arguments displays the pending configurations.

Examples

This example shows how to display the edited configuration:

```
Router(config-mst)# show pending
Pending MST configuration
Name      [zorglub]
Version   31415
Instance  Vlans Mapped
--------  ---------------------------------------------------------------------
0         4001-4096
2         1010, 1020, 1030, 1040, 1050, 1060, 1070, 1080, 1090, 1100, 1110
          1120
3         1-1009, 1011-1019, 1021-1029, 1031-1039, 1041-1049, 1051-1059
          1061-1069, 1071-1079, 1081-1089, 1091-1099, 1101-1109, 1111-1119
          1121-4000
-------------------------------------------------------------------------------
Router(config-mst)#
```

This example shows how to display the current configuration:

```
Router(config-mst)# show current
Current MST configuration
Name []
Revision 0
Instance Vlans mapped
-------- ---------------------------------------------------------------------
0 1-4094
---------------------------------------------------------------------------------
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration submode)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst configuration	Enters MST-configuration submode.

show adjacency

To display information about the hardware Layer 3-switching adjacency table, use the **show adjacency** command.

show adjacency [{*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*} | **detail** | **internal** | **summary**]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **ge-wan**, and **atm**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
port-channel *number*	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
vlan *vlan-id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
detail	(Optional) Displays the information about the protocol detail and timer.
internal	(Optional) Displays the information about the internal data structure.
summary	(Optional) Displays a summary of CEF-adjacency information.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Hardware Layer 3-switching adjacency statistics are updated every 60 seconds.

The information that is contained in the **show adjacency** commands includes the following:

- Protocol interface.
- Type of routing protocol that is configured on the interface.
- Interface address.
- Method of adjacency that was learned.
- MAC address of the adjacent router.
- Time left before the adjacency rolls out of the adjacency table. After it rolls out, a packet must use the same next hop to the destination.

Examples

This example shows how to display adjacency information:

```
Router# show adjacency
Protocol Interface                 Address
IP       FastEthernet2/3           172.20.52.1(3045)
IP       FastEthernet2/3           172.20.52.22(11)
Router#
```

This example shows how to display a summary of adjacency information:

```
Router# show adjacency summary
Adjacency Table has 2 adjacencies
  Interface                Adjacency Count
  FastEthernet2/3          2
Router#
```

This example shows how to display protocol detail and timer information:

```
Router# show adjacency detail
Protocol Interface                 Address
IP       FastEthernet2/3           172.20.52.1(3045)
                                   0 packets, 0 bytes
                                   000000000FF920000380000000000000
                                   00000000000000000000000000000000
                                   00605C865B2800D0BB0F980B0800
                                   ARP        03:58:12
IP       FastEthernet2/3           172.20.52.22(11)
                                   0 packets, 0 bytes
                                   000000000FF920000380000000000000
                                   00000000000000000000000000000000
                                   00801C93804000D0BB0F980B0800
                                   ARP        03:58:06
Router#
```

This example shows how to display adjacency information for a specific interface:

```
Router# show adjacency fastethernet 2/3
Protocol Interface                 Address
IP       FastEthernet2/3           172.20.52.1(3045)
IP       FastEthernet2/3           172.20.52.22(11)
Router#
```

Related Commands

Command	Description
show mls cef adjacency	Displays information about the MLS-hardware Layer 3-switching adjacency node.

show arp

To display the ARP table, use the **show arp** command.

show arp

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display the ARP table:

```
Router> show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.20.52.11           4   0090.2156.d800  ARPA   Vlan2
Internet  172.20.52.1           58   0060.5c86.5b28  ARPA   Vlan2
Internet  172.20.52.22         129   0080.1c93.8040  ARPA   Vlan2
Router>
```

show asic-version

To display the ASIC version for a specific module, use the **show asic-version** command.

show asic-version slot *number*

Syntax Description

number	Module number.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

In the **show asic-version** command output, the ASIC types are as follows:

- Lyra—Layer 2 forwarding engine
- Hyperion—Packet rewrite, multicast, and SPAN engine
- Polaris—Layer 3 CEF engine
- Pinnacle—4-port Gigabit Ethernet interface
- R2D2—Network interface (with combinations of 10/100/1000Mbps and 10Gbps), a receive packet buffer interface, a transmit packet buffer interface as well as an interface to a further upstream ASIC or FPGA.
- Titan—Packet rewrite and replication engine
- Vela—Constellation bus interface

Examples

This example shows how to display the ASIC type and version for a specific module:

```
Router# show asic-version slot 1
Module in slot 1 has 3 type(s) of ASICs
        ASIC Name      Count      Version
         PINNACLE          1      (2.0)
           MEDUSA          1      (2.0)
            TITAN          1      (0.1)
Router#
```

show bootflash:

To display information about the bootflash: file system, use the **show bootflash:** command.

show bootflash: [**all** | **chips** | **filesys**]

Syntax Description

all	(Optional) Displays all possible flash information.
chips	(Optional) Displays information about the flash chip.
filesys	(Optional) Displays information about the file system.

Command Default

This command has no default settings.

Command Modes

User EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to display information about the file system status:

```
Router> show bootflash: filesys

-------- F I L E   S Y S T E M   S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number          = 6887635   File System Vers = 10000    (1.0)
  Length                = 1000000   Sector Size      = 40000
  Programming Algorithm = 39        Erased State     = FFFFFFFF
  File System Offset    = 40000     Length = F40000
  MONLIB Offset         = 100       Length = C628
  Bad Sector Map Offset = 3FFF8     Length = 8
  Squeeze Log Offset    = F80000    Length = 40000
  Squeeze Buffer Offset = FC0000    Length = 40000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used     = 917CE8  Bytes Available = 628318
  Bad Sectors    = 0       Spared Sectors  = 0
  OK Files       = 2       Bytes = 917BE8
  Deleted Files  = 0       Bytes = 0
  Files w/Errors = 0       Bytes = 0
Router>
```

This example shows how to display image information:

```
Router> show bootflash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    8C5A393A  237E3C   14  2063804 Aug 23 1999 16:18:45 c6msfc-boot-mz
2   .. image    D86EE0AD  957CE8    9  7470636 Sep 20 1999 13:48:49 rp.halley
Router>
```

This example shows how to display all bootflash information:

```
Router> show bootflash: all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    8C5A393A  237E3C   14  2063804 Aug 23 1999 16:18:45 c6msfc-boot-
mz
2   .. image    D86EE0AD  957CE8    9  7470636 Sep 20 1999 13:48:49 rp.halley

6456088 bytes available (9534696 bytes used)

-------- F I L E   S Y S T E M   S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number          = 6887635   File System Vers = 10000    (1.0)
  Length                = 1000000   Sector Size      = 40000
  Programming Algorithm = 39        Erased State     = FFFFFFFF
  File System Offset    = 40000     Length = F40000
  MONLIB Offset         = 100       Length = C628
  Bad Sector Map Offset = 3FFF8     Length = 8
  Squeeze Log Offset    = F80000    Length = 40000
  Squeeze Buffer Offset = FC0000    Length = 40000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used     = 917CE8  Bytes Available = 628318
  Bad Sectors    = 0       Spared Sectors  = 0
  OK Files       = 2       Bytes = 917BE8
  Deleted Files  = 0       Bytes = 0
  Files w/Errors = 0       Bytes = 0
Router>
```

show bootvar

To display information about the BOOT environment variable, use the **show bootvar** command.

show bootvar

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

User EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **show bootvar** command output depends on how you configure the boot statement as follows:

- If you enter the **boot system flash bootflash:***sup720_image* command in the boot configuration, then the **show bootvar** command output displays the bootflash information.
- If you enter the **boot system flash sup-bootflash:***sup720_image* command in the boot configuration, then the **show bootvar** command output displays the sup-bootflash information. This action is the correct way of configuring the boot statement.

The **show bootvar** command is available from the switch processor CLI and the route processor CLI. From the switch processor CLI, the display is always bootflash. With either the bootflash or the sup-bootflash boot statement, the switch boots correctly. You should use sup-bootflash in the boot configuration statement because the image is stored in the switch processor bootflash; the route processor sees the image as sup-bootflash.

The number displayed after the image name (an example is c6sup12-js-mz.121-13.E,12) indicates the number of times that the Catalyst 6500 series switch tries to reboot the file before giving up.

Examples

This example shows how to display information about the BOOT environment variable:

```
Router# show bootvar
BOOT variable = sup-bootflash:c6sup12-js-mz.121-13.E,12
CONFIG_FILE variable =
BOOTLDR variable = bootflash:c6msfc2-boot-mz.121-13.E.bin
Configuration register is 0x2102

Standby is up
Standby has 112640K/18432K bytes of memory.
```

```
Standby BOOT variable = bootflash:c6sup12-js-mz.121-13.E,12
Standby CONFIG_FILE variable =
Standby BOOTLDR variable = bootflash:c6msfc2-boot-mz.121-13.E.bin
Standby Configuration register is 0x2102
Router#
```

Related Commands

Command	Description
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.