

policy-map

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

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

policy-map-name Policy map name. See the “Usage Guidelines” section for descriptions of the **policy-map** subcommands.

Defaults

The defaults are as follows:

- *extended-burst-bytes* is equal to *burst-bytes*.
- **conform-action** is transmit.
- **exceed-action** is drop.
- **violate-action** is equal to the **exceed-action**.
- **pir** *peak-rate-bps* is equal to the normal (**cir**) rate.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XE	Support for this command was introduced on the Catalyst 6500 series switches.
12.1(1)E	Support for this command on the Catalyst 6500 series switches was extended to the 12.1 E release.
12.1(5c)EX	This command was updated to do the following: <ul style="list-style-type: none"> • Increase the minimum <i>rate-bps</i> to 32000 bps and the maximum <i>rate-bps</i> to 4000000000 bps. • Add the pir <i>peak-rate-bps</i> and violate-action arguments.

Usage Guidelines

In QoS policy-map configuration mode, these configuration commands are available:

- **exit** exits QoS class map configuration mode.
- **no** removes a previously defined policy map.
- **class** *class-map* [*name*] accesses QoS class map configuration mode to specify a previously created class map to be included in the policy map or to create a class map (see the **class-map** command for additional information).

- **police** [**aggregate name**] [**flow**] *bits-per-second normal-burst-bytes [extended-burst-bytes] [pir peak-rate-bps]* [{**conform-action action**} {**drop [exceed-action action]**} | {**set-dscp-transmit [new-dscp]**} | {**set-prec-transmit [new-precedence]**} | {**transmit** [{**exceed-action action**}] | {**violate-action action**}}] defines a microflow or aggregate policer.
- **trust {cos | dscp | ip-precedence}** sets the specified class trust values. Trust values that are set in this command supercede trust values that are set on specific interfaces.

Table 2-20 describes the **class** syntax.

Table 2-20 class Syntax Description

Subcommand	Description
exit	(Optional) Exits from QoS class action configuration mode.
police	(Optional) Specifies flow policing.
aggregate name	(Optional) Specifies the aggregate policer for the current class.
flow	(Optional) Specifies a microflow policer.
<i>bits-per-second</i>	Bits per second; valid values are from 32000 to 4000000000 bps.
<i>normal-burst-bytes</i>	Burst bytes; valid values are from 1000 to 512000000 MB.
<i>extended-burst-bytes</i>	(Optional) Extended burst bytes; valid values are from 1000 to 512000000 MB (if entered, must be set equal to <i>normal-burst-bytes</i>).
pir peak-rate-bps	(Optional) Sets PIR peak rate; valid values are from 1000 to 512000000 MB.
conform-action action	(Optional) Sets the conform action; actions are drop , set-dscp-transmit , set-prec-transmit , and transmit .
exceed-action action	(Optional) Sets the exceed action; see the “Usage Guidelines” section for valid values.
violate-action action	(Optional) Sets the violate action; see the “Usage Guidelines” section for valid values.
set-dscp-transmit	(Optional) Conforms action to mark matched traffic with a new DSCP value.
set-prec-transmit	(Optional) Conforms action to mark matched traffic with a new IP precedence value.
trust state	(Optional) Configures the policy map class trust state. Trust states are cos , dscp , and ip-precedence .
cos	(Optional) Sets the internal DSCP value from a received or interface CoS.
dscp	(Optional) Sets QoS to use the received DSCP value.
ip-precedence	(Optional) Sets the DSCP value from the received IP precedence.

Valid values for *action* are as follows:

- **drop**—Drops all matched traffic.
- **policed-dscp-transmit**—Causes all out-of-profile traffic to be marked down as specified in the markdown map.
- **transmit**—Sets the DSCP as defined by the trust state of the traffic.

The **pir** *peak-rate-bps* corresponds to the extended burst rate.

The **pir**, *extended-burst-bytes*, and **violate-action** keywords and arguments are not supported in microflow policing or in systems configured with a Supervisor Engine 1 with Layer 3 Switching Engine (PFC), except for the default values.

The **violate-action** parameter is not supported in systems configured with a Supervisor Engine 1 with Layer 3 Switching Engine (PFC), but you can enter the command if the parameters match the **exceed-action** parameters.

PFC QoS does not support the **bandwidth**, **priority**, **queue-limit**, **random-detect**, or **set** keywords in policy map classes.

Examples

This example shows how to create a policy map named **max-pol-ipp5** that uses a previously configured class-map named **ipp5**, how to configure trust received IP precedence values, and configure a maximum-capacity aggregate policer and a microflow policer:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 200000000 200000 800000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit
Router(config-pmap-c)# end
Router#
```

Related Commands

[class-map](#)
[service-policy input](#)
[show class-map](#)
[show policy-map](#)
[show policy-map interface](#)

port-channel load-balance

To set the load-distribution method among the ports in the bundle, use the **port-channel load-balance** command. Use the **no** form of this command to reset the load distribution to the default settings.

port-channel load-balance *method*

no port-channel load-balance

Syntax Description	<i>method</i> Load-distribution method; see the “Usage Guidelines” section for a list of valid values.
---------------------------	--

Defaults	<i>method</i> is src-dst-ip .
-----------------	--------------------------------------

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

Command History	Release	Modification
	12.0(7)XE	Support for this command was introduced on the Catalyst 6500 series switches.
	12.1(1)E	Support for this command on the Catalyst 6500 series switches was extended to the 12.1 E release.
	12.1(5c)EX	This command was updated to correct the valid values for <i>method</i> .

Usage Guidelines	Valid <i>method</i> values are as follows:
-------------------------	--

- **dst-ip**—Load distribution on the destination IP address
- **dst-mac**—Load distribution on the destination MAC address
- **src-dst-ip**—Load distribution on the source XOR destination IP address
- **src-dst-mac**—Load distribution on the source XOR destination MAC address
- **src-ip**—Load distribution on the source IP address
- **src-mac**—Load distribution on the source MAC address
- **src-port**—Load distribution on the source port
- **dst-port**—Load distribution on the destination port
- **src-dst-port**—Load distribution on the source XOR destination port

Examples

This example shows how to set the load distribution method to **dst-ip**:

```
Router(config)# port-channel load-balance dst-ip
Router(config)#
```

Related Commands

[interface port-channel](#)
[show etherchannel](#)

power enable

To turn on power for the modules, use the **power enable** command. Use the **no** form of this command to power down a module.

power enable {*module slot*}

no power enable {*module slot*}

Syntax Description	module slot	Specifies a module slot number; see the “Usage Guidelines” section for valid values.
--------------------	--------------------	--

Defaults	Enabled
----------	---------

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

Command History	Release	Modification
	12.0(7)XE	Support for this command was introduced on the Catalyst 6500 series switches.
	12.1(1)E	Support for this command on the Catalyst 6500 series switches was extended to the 12.1 E release.
	12.1(23)E	This command was changed to allow you to disable power to empty slots.

Usage Guidelines	When you enter the no power enable module slot command to power down a module, the module’s configuration is not saved.
------------------	--

You can also use this command to disable power to an empty slot. This command allows you to reserve power that might have been supplied to in an empty slot and prevent higher consumption in the other slots.

The *slot* argument designates the module number. Valid values for *slot* depend on the chassis used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples	This example shows how to turn on the power for a module that was previously powered down:
----------	--

```
Router(config)# power enable module 5
Router(config)#
```

This example shows how to power down a module:

```
Router(config)# no power enable module 5
Router(config)#
```

Related Commands	show power
------------------	----------------------------

power inline

To configure the administrative mode of the inline power on an interface, use the **power inline** command.

power inline {auto | never}

Syntax Description	auto	never
	Turns on the device discovery protocol and applies power to the device, if found.	Turns off the device discovery protocol and stops supplying power to the device.

Defaults auto

Command Modes Interface configuration

Command History	Release	Modification
	12.1(13)E	Support for this command was introduced on the Catalyst 6500 series switches.

Examples This example shows how to set the inline power to the off mode on an interface:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline never
```

Related Commands [show power](#)

power redundancy-mode

To set the power-supply redundancy mode, use the **power redundancy-mode** command.

power redundancy-mode { **combined** | **redundant** }

Syntax Description	combined	Specifies no redundancy (combine power-supply outputs).
	redundant	Specifies redundancy (either power supply can operate the system).

Defaults **redundant**

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)XE	Support for this command was introduced on the Catalyst 6500 series switches.
	12.1(1)E	Support for this command on the Catalyst 6500 series switches was extended to the 12.1 E release.

Examples This example shows how to set power supplies to the no-redundancy mode:

```
Router(config)# power redundancy-mode combined
Router(config)#
```

This example shows how to set power supplies to the redundancy mode:

```
Router(config)# power redundancy-mode redundant
Router(config)#
```

Related Commands [show power](#)

ppp link

To generate PPP LCP down/keepalive failure link traps or enable calls to the interface reset vector, use the **ppp link** command. Use the **no** form of this command to disable PPP LCP down/keepalive failure link traps or calls to the interface reset vector.

```
ppp link {reset | trap}
```

```
no ppp link {reset | trap}
```

Syntax Description

reset	Specifies calls to the interface reset vector.
trap	Specifies the PPP LCP down/keepalive failure link traps.

Defaults

The defaults are as follows:

- The calls are sent to the interface reset vector.
- The traps are sent when the LCP goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(19)E	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **no ppp link trap** command disables the sending of the link traps when the LCP goes down.

In the event the PPP calls the interface reset vector while the LCP is configured or closed, Up/Down status messages will display on the console. If a leased-line configuration is up but the peer is not responding, PPP may call the interface reset vector once per minute. This situation may result in the Up/Down status messages on the console. Use the **no ppp link reset** command to disable calls to the interface reset vector. PPP will continue to attempt to negotiate with the peer, but the interface will not be reset between each attempt.

Examples

This example shows how to enable calls to the interface reset vector:

```
Router(config-if)# ppp link reset
Router(config-if)#
```

This example shows how to disable calls to the interface reset vector:

```
Router(config-if)# no ppp link reset
Router(config-if)#
```

This example shows how to generate PPP LCP down/keepalive failure link traps:

```
Router(config-if)# ppp link trap  
Router(config-if)#
```

This example shows how to disable the sending of the link traps when the LCP goes down:

```
Router(config-if)# no ppp link trap  
Router(config-if)#
```

private-vlan

To configure PVLANs and the association between a PVLAN and a secondary VLAN, use the **private-vlan** command. Use the **no** form of this command to return to the default settings.

private-vlan { **isolated** | **community** | **primary** }

private-vlan association *secondary-vlan-list* | { **add** *secondary-vlan-list* } |
{ **remove** *secondary-vlan-list* }

no private-vlan { **association** | **isolated** | **community** | **primary** }

Syntax Description

isolated	Designates the VLAN as an isolated PVLAN.
community	Designates the VLAN as a community PVLAN.
primary	Designates the VLAN as the primary PVLAN.
association	Creates an association between a secondary VLAN and a primary VLAN.
<i>secondary-vlan-list</i>	Number of the secondary VLAN.
add	Associates a secondary VLAN to a primary VLAN.
remove	Clears the association between a secondary VLAN and a primary VLAN.

Defaults

No PVLANs are configured.

Command Modes

config-VLAN submode

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines



Caution

If you enter the **shutdown** command and then the **no shutdown** command in the config-vlan mode on a PVLAN (primary or secondary), the PVLAN type and association information is deleted. You will have to reconfigure the VLAN to be a PVLAN.

You cannot configure VLAN 1 or VLANs 1001 to 1005 as PVLANs.

VTP does not support PVLANs. You must configure PVLANs on each device where you want PVLAN ports.

The *secondary-vlan-list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single PVLAN ID or a hyphenated range of PVLAN IDs. The *secondary-vlan-list* parameter can contain multiple community VLAN IDs.

The *secondary-vlan-list* parameter can contain only one isolated VLAN ID. A PVLAN is a set of private ports characterized by using a common set of VLAN number pairs. Each pair is made up of at least two special unidirectional VLANs and is used by isolated ports and/or by a community of ports to communicate with routers.

An isolated VLAN is a VLAN that is used by isolated ports to communicate with promiscuous ports. An isolated VLAN's traffic is blocked on all other private ports in the same VLAN. Its traffic can only be received by standard trunking ports and promiscuous ports that are assigned to the corresponding primary VLAN.

A promiscuous port is defined as a private port that is assigned to a primary VLAN.

A primary VLAN is defined as the VLAN that is used to convey the traffic from the routers to customer end stations on private ports.

A community VLAN is defined as the VLAN that carries the traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN.

For Ethernet 10-Mb, 10/100-Mb, and 100-Mb modules, within groups of 12 ports (1–12, 13–24, 25–36, and 37–48), you cannot configure ports as isolated or community PVLAN ports when one port is a trunk, a SPAN destination, or a promiscuous PVLAN port.

Only one isolated *vlan-id* may be specified, while multiple community VLANs are allowed. Isolated and community VLANs can only be associated with one VLAN. The associated VLAN list may not contain primary VLANs. Similarly, a VLAN that is already associated to a primary VLAN cannot be configured itself as a primary VLAN.

The **private-vlan** commands do not take effect until you exit the config-VLAN submode.

If you delete either the primary or secondary VLAN, the ports associated with the VLAN become inactive.

Examples

This example shows how to create a PVLAN relationship between the primary VLAN 14, the isolated VLAN 19, and the community VLANs 20 and 21:

```
Router(config) # vlan 19
Router(config-vlan) # private-vlan isolated
Router(config) # vlan 20
Router(config-vlan) # private-vlan community
Router(config-vlan) # private-vlan community
Router(config) # vlan 14
Router(config-vlan) # private-vlan primary
Router(config-vlan) # private-vlan association 19-21
```

This example shows how to remove an isolated VLAN and community VLAN 20 from the PVLAN association:

```
Router(config) # vlan 14
Router(config-vlan) # private-vlan association remove 18,20
Router(config-vlan) #
```

This example shows how to remove a PVLAN relationship and deletes the primary VLAN. The associated secondary VLANs are not deleted.

```
Router(config-vlan) # no private-vlan 14
Router(config-vlan) #
```

Related Commands

[show vlan](#)
[show vlan private-vlan](#)

private-vlan mapping

To create a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN SVI, use the **private-vlan mapping** command. Use the **no** form of this command to remove all PVLAN mappings from the SVI.

```
private-vlan mapping [{secondary-vlan-list | {add secondary-vlan-list} |
{remove secondary-vlan-list}]
```

```
no private-vlan mapping
```

Syntax Description	
<i>secondary-vlan-list</i>	(Optional) VLAN ID of the secondary VLANs to map to the primary VLAN.
add	(Optional) Maps the secondary VLAN to the primary VLAN.
remove	(Optional) Removes the mapping between the secondary VLAN and the primary VLAN.

Defaults No PVLAN SVI mapping is configured.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EX	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines The PVLAN mapping interface configuration command affects traffic that is switched in software on the MSFC or MSFC2. The **private-vlan mapping** interface configuration command does not configure Layer 3 switching on the PFC or PFC2.

The *secondary-vlan-list* parameter cannot contain spaces; it can contain multiple comma-separated items. Each item can be a single PVLAN ID or a hyphenated range of PVLAN IDs.

This command is valid in the interface configuration mode of the primary VLAN.

The SVI of the primary VLAN is created at Layer 3.

Traffic received on the secondary VLAN is routed by the SVI of the primary VLAN.

The SVIs of existing secondary VLANs do not function and are considered as down after you enter this command.

A secondary SVI can only be mapped to one primary SVI. If you configure the primary VLAN as a secondary VLAN, all the SVIs specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 association, the mapping configuration does not take effect.

Examples

This example shows how to map the interface of VLAN 20 to the SVI of VLAN 18:

```
Router(config)# interface vlan 18
Router(config-if)# private-vlan mapping 18 20
Router(config-if)#
```

This example shows how to permit routing of secondary VLAN ingress traffic from PVLANS 303 through 307, 309, and 440 and verify the configuration:

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan202 303 community
vlan202 304 community
vlan202 305 community
vlan202 306 community
vlan202 307 community
vlan202 309 community
vlan202 440 isolated
Router#
```

This example shows the displayed error message if the VLAN you are adding is already mapped to the SVI of VLAN 18. You must delete the mapping from the SVI of VLAN 18 first.

```
Router(config)# interface vlan 19
Router(config-if)# private-vlan mapping 19 add 21
Command rejected: The interface for VLAN 21 is already mapped as s secondary.
Router(config-if)#
```

This example shows how to remove all PVLAN mappings from the SVI of VLAN 19:

```
Router(config)# interface vlan 19
Router(config-if)# no private-vlan mapping
Router(config-if)#
```

Related Commands

[show interfaces private-vlan mapping](#)
[show vlan](#)
[show vlan private-vlan](#)

private-vlan synchronize

To map secondary VLANs to the same instance as the primary VLAN, use the **private-vlan synchronize** command.

private-vlan synchronize

Syntax Description This command has no keywords or arguments.

Defaults This command has no default settings.

Command Modes MST configuration submode

Command History	Release	Modification
	12.1(11b)EX	Support for this command was introduced on the Catalyst 6500 series switches.
	12.1(13)E	Support for this command on the Catalyst 6500 series switches was extended to the 12.1 E release.

Usage Guidelines If you do not map VLANs to the same instance as the associated primary VLAN when you exit the MST configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

Examples This example assumes that a primary VLAN 2 and a secondary VLAN 3 are associated to VLAN 2, and that all VLANs are mapped to the CIST instance 1. This example also shows the output if you try to change the mapping for the primary VLAN 2 only:

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 2
Router(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

This example shows how to initialize PVLAN synchronization:

```
Router(config-mst)# private-vlan synchronize
Router(config-mst)#
```

Related Commands [show](#)
[show spanning-tree mst](#)

protocol-filtering

To enable protocol filtering, use the **protocol-filtering** command. Use the **no** form of this command to disable protocol filtering.

protocol-filtering

no protocol-filtering

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)XE	Support for this command was introduced on the Catalyst 6500 series switches.
	12.1(1)E	Support for this command on the Catalyst 6500 series switches was extended to the 12.1 E release.

Usage Guidelines Layer 3 protocol filtering is supported with a Supervisor Engine 1.
Layer 3 protocol filtering is not supported with a Supervisor Engine 2.

Examples This example shows how to enable the protocol filtering feature:

```
Router(config)# protocol-filtering
Router(config)#
```

Related Commands [show protocol-filtering](#)