platform ip features pisa

To configure the Intelligent Traffic Redirect (ITR) feature, which filters traffic to the PISA, use the **platform ip features pisa** command in interface configuration mode.

platform ip features pisa access-group {*ip-acl-name* | *ip-acl-number*} {**input** | **output**} [**reverse-only**]

Syntax Description

access-group *ip-acl-name*	Specifies the name of the ITR ACL.
access-group *ip-acl-number*	Specifies the number of the ITR ACL. Range: 1 to 199 and from 1300 to 2699.
input	Applies the ITR ACL to ingress traffic.
output	Applies the ITR ACL to egress traffic.
reverse-only	(Optional) Specifies that the ITR ACL is applied only to the inspect direction traffic.

Command Default

This command has no default settings

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZYA1	Support for this command was introduced.

Usage Guidelines

If you do not configure the **platform ip features pisa** command, all traffic on interfaces where you configure a PISA-accelerated feature is sent to the PISA.

This command can be configured on Layer 2 and Layer 3 ports, Layer 2 and Layer 3 trunks, Layer 2 and Layer 3 port-channel interfaces, multi-VLAN access ports (MVAPs), Layer 3 subinterfaces, and SVIs only. You cannot enter this command on other types of interfaces. An error message is displayed if you try to configure it on other interface types.

When you enter this command on a Layer 3 interface, the software automatically attempts to map a reverse ACL (also known as a mirror ACL) to the opposite direction of the same interface if the packets need to be seen by the PISA bidirectionally.

If you enter this command on a Layer 2 interface, hardware limitations prevent the reverse ACL from being mapped in the egress direction. On Layer 2 interfaces, the LTL copy mechanism captures all the packets.

Actions required by PISA-accelerated features:

Feature	Keyword	Action on Ingress Traffic	Action on Egress Traffic
NBAR MQC	**input, input reverse-only**	Modify	Inspect
	output, **output reverse-only**	Inspect	Modify

NBAR protocol discovery	**input, input reverse-only**	Inspect	Inspect
	output, **output reverse-only**	Inspect	Inspect
NBAR tagging	**input, input reverse-only**	None	None
	output, **output reverse-only**	None	Modify
Flexible Packet Matching	**input, input reverse-only**	Modify	None
	output, **output reverse-only**	None	Modify
URL Filtering	**input, input reverse-only**	Modify	Modify
	output, **output reverse-only**	Modify	Modify

When a PISA-accelerated feature is configured on the interface, the ITR ACL does the following:

- **input**—The ITR ACL redirects ingress (modify-direction) traffic permitted by the ACL to the PISA for the action required by the PISA-accelerated feature. Not-permitted ingress traffic is processed by the PFC3.

  If automatically applied by the ITR feature, the reverse ITR ACL redirects egress (inspect-direction) traffic permitted by the reverse ACL to the PISA to collect statistics, maintain state, or collect other types of information.

- **input reverse-only**—All ingress (modify-direction) traffic goes to the PISA for the action required by the PISA-accelerated feature. The ITR ACL redirects egress (inspect-direction) traffic permitted by the ACL to the PISA to collect statistics, maintain state, or collect other types of information. With the **reverse-only** keyword, configure the ITR ACL only for the egress (inspect-direction) traffic.

- **output**—The ITR ACL redirects egress (modify-direction) traffic permitted by the ACL to the PISA for the action required by the PISA-accelerated feature. Not-permitted egress traffic is processed by the PFC3.

  If automatically applied by the ITR feature, the reverse ITR ACL redirects ingress (inspect-direction) traffic permitted by the reverse ACL to the PISA for the action required by the PISA-accelerated feature.

- **output reverse-only**—All egress (modify-direction) traffic goes to the PISA for the action required by the PISA-accelerated feature. The ITR ACL redirects ingress (inspect-direction) traffic permitted by the ACL to the PISA for the action required by the PISA-accelerated feature. With the **reverse-only** keyword, configure the ITR ACL only for the ingress (inspect-direction) traffic.

Configure the ITR ACL to not permit traffic to which you want to apply PFC QoS.

To avoid sending excess traffic to the PISA, ensure that non-PISA capture-based features, such as VACL capture, OAL, and traffic for the NAM and IDS service modules, are not enabled when ITR is configured.

Traffic being processed by NetFlow-based features (for example, NAT and WCCP) might not be sent to the PISA when ITR is configured.

Examples

This example shows how to redirect egress traffic to the PISA:

```
Router(config-if)# platform ip features pisa access-group pisa_egress_redirect out
Router(config-if)#
```

Related Commands

Command	Description
show platform software pisa fm interface	Displays per-interface Supervisor Engine 32 PISA-specific information.
show platform pisa np	Displays Supervisor Engine 32 PISA-specific information.
show running-config interface	Displays the contents of the currently running configuration file.

platform ip features sequential

To enable IP precedence-based or DSCP-based egress QoS filtering to use any IP precedence or DSCP policing or marking changes made by ingress PFC QoS, use the **platform ip features sequential** command. To return to the default settings, use the **no** form of this command.

platform ip features sequential [**access-group** {*ip-acl-name* | *ip-acl-number*}]

no platform ip features sequential [**access-group** {*ip-acl-name* | *ip-acl-number*}]

Syntax Description

access-group *ip-acl-name*	(Optional) Specifies the name of the ACL that is used to specify the match criteria for the recirculation packets.
access-group *ip-acl-number*	(Optional) Specifies the number of the ACL that is used to specify the match criteria for the recirculation packets; valid values are from 1 to 199 and from 1300 to 2699.

Command Default

IP precedence-based or DSCP-based egress QoS filtering uses received IP precedence or DSCP values and does not use any IP precedence or DSCP changes made by ingress QoS as the result of policing or marking.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The enhanced egress-QoS filtering enables the IP precedence-based or DSCP-based egress-QoS filtering to use any IP precedence or DSCP policing or marking changes made by ingress QoS.

The nonenhanced egress-QoS filtering behavior is the normal Catalyst 6500 series switch behavior when QoS is applied in the hardware.

The PFC3 provides egress PFC QoS only for Layer 3-switched and routed traffic on egress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

You configure enhanced egress QoS filtering on ingress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

To enable enhanced egress QoS filtering only for the traffic filtered by a specific standard, extended named, or extended numbered IP ACL, enter the IP ACL name or number.

If you do not enter an IP ACL name or number, enhanced egress QoS filtering is enabled for all IP ingress IP traffic on the interface.

Note

- When you configure enhanced egress-QoS filtering, the PFC3 processes traffic to apply ingress PFC QoS. The PFC3 applies ingress-QoS filtering and Catalyst 6500 series switch hardware ingress QoS. The PFC3 incorrectly applies any egress-QoS filtering and Catalyst 6500 series switch hardware egress QoS that is configured on the ingress interface.
- If you configure enhanced egress-QoS filtering on an interface that uses Layer 2 features to match the IP precedence or DSCP as modified by ingress-QoS marking, the packets are redirected or dropped and prevented from being processed by egress QoS.
- If you enable enhanced egress-QoS filtering, the hardware acceleration of NetFlow-based features such as reflexive ACL, NAT, and TCP intercept are disabled.

To verify configuration, use the **show running-config interface** command.

Examples

This example shows how to enable enhanced egress-QoS filtering:

```
Router(config-if)# platform ip features sequential
Router(config-if)#
```

This example shows how to disable enhanced egress-QoS filtering:

```
Router(config-if)# no platform ip features sequential
Router(config-if)#
```

Related Commands

Command	Description
show running-config interface	Displays the contents of the currently running configuration file.

platform ipv6 acl icmp optimize neighbor-discovery

To optimize TCAM support for IPv6 ACLs, use the **platform ipv6 acl icmp optimize neighbor-discovery** command. To disable optimization of TCAM support for IPv6 ACLs, use the **no** form of this command.

platform ipv6 acl icmp optimize neighbor-discovery

no platform ipv6 acl icmp optimize neighbor-discovery

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Note Use this command under the direction of the Cisco TAC only.

When you enable optimization of the TCAM support for IPv6 ACLs, the global ICMPv6 neighbor-discovery ACL at the top of the TCAM is programmed to permit all ICMPv6 neighbor-discovery packets. Enabling optimization prevents the addition of ICMPv6 ACEs at the end of every IPv6 security ACL, reducing the number of TCAM resources being used. Enabling this command reprograms IPv6 ACLs on all interfaces.

Note The ICMPv6 neighbor-discovery ACL at the top of the TCAM takes precedence over security ACLs for ICMP neighbor-discovery packets that you have configured, but has no effect if you have a bridge/deny that overlaps with the global ICMP ACL.

Examples

This example shows how to optimize TCAM support for IPv6 ACLs:

```
Router(config)# platform ipv6 acl icmp optimize neighbor-discovery
Router(config)#
```

This example shows how to disable optimization of TCAM support for IPv6 ACLs:

```
Router(config)# no platform ipv6 acl icmp optimize neighbor-discovery
Router(config)#
```

platform scp retry interval

To enable SCP fast retry and set the fast-retry interval, use the **platform scp retry interval** command. To disable SCP fast retry, use the **no** form of this command.

platform scp retry interval *timeout-value*

no platform scp retry interval

Syntax Description

timeout-value	Fast retry interval; valid values are from 200 to 2000 milliseconds.

Command Default

2000 milliseconds

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Note Use this command under the direction of the Cisco TAC only.

Examples

This example shows how to enable SCP fast retry and set the fast-retry interval:

```
Router(config)# platform scp retry interval 600
Router(config)#
```

platform vfi dot1q-transparency

To enable 802.1Q transparency mode, use the **platform vfi dot1q-transparency** command. To disable 802.1Q transparency, use the **no** form of this command.

platform vfi dot1q-transparency

no platform vfi dot1q-transparency

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command is supported on OSM modules only.

The 802.1Q transparency allows a service provider to modify the MPLS EXP bits for core-based QoS policies while leaving any VPLS customer 802.1p bits unchanged.

The dot1q Transparency for EoMPLS feature causes the VLAN-applied policy to affect only the IGP label (for core QoS) and leaves the VC label EXP bits equal to the 802.1p bits. On the egress PE, the 802.1p bits are still rewritten based on the received VC EXP bits, however, because the EXP bits now match the ingress 802.1p bits, a VPLS customer's 802.1p bits do not change.

Global configuration (config) applies to all virtual forwarding instance (VFI) and switched virtual interface (SVI) EoMPLS VCs configured on the Cisco 7600 series routers.

Interoperability requires applying the Dot1q Transparency for EoMPLS feature to all participating PE routers.

Examples

This example shows how to enable 802.1Q transparency:

```
Router (config)# platform vfi dot1q-transparency
Router (config)#
```

This example shows how to disable 802.1Q transparency:

```
Router (config)# no platform vfi dot1q-transparency
Router (config)#
```

police (policy map)

To create a per-interface policer and configure the policy-map class to use it, use the **police** command. To delete the per-interface policer from the policy-map class, use the **no** form of this command.

police {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*] [**pir** *peak-rate-bps*]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

no police {*bits-per-second* [*normal-burst-bytes*] [*extended-burst-bytes*] [**pir** *peak-rate-bps*]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

Syntax Description

bits-per-second	CIR bits per second; valid values are from 32000 to 2 Gbps bits per second.
normal-burst-bytes	(Optional) CIR token-bucket size; valid values are from 1000 to 512000000 bytes.
maximum-burst-bytes	(Optional) PIR token-bucket size; valid values are from 1000 to 32000000 bytes.
pir *peak-rate-bps*	(Optional) Sets the PIR peak rate; valid values are from 32000 to 2 Gbps bits per second.
conform-action *action*	(Optional) Specifies the action to be taken if the *bits-per-second* rate has not been exceeded; see the "Usage Guidelines" section for valid values.
exceed-action *action*	(Optional) Specifies the action to be taken when the *bits-per-second* rate has been exceeded; see the"Usage Guidelines" section for valid values.
violate-action *action*	(Optional) Specifies the action to be taken when the *bits-per-second* rate is greater than the *maximum-burst-bytes* rate; see the "Usage Guidelines" section for valid values.

Command Default

The defaults are as follows:

- *maximum-burst-bytes* is equal to *normal-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-burst-bytes* rate.

Command Modes

Policy-map subcommand

Command History

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

Usage Guidelines

On the Supervisor Engine 32 PISA, the **police** command is supported in software.

Named aggregate policers and microflow policers are not supported on the Supervisor Engine 32 PISA.

The *normal-burst-bytes* argument sets the CIR token bucket size.

The *maximum-burst-bytes* argument sets the PIR token bucket size (not supported with the **flow** keyword). You must set the *maximum-burst-bytes* argument to be equal to the *normal-burst-bytes* setting.

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

The valid values for *action* are as follows:

- **drop**—Drops packets that do not exceed the *bits-per-second* rate.
- **policed-dscp-transmit**—Causes all the out-of-profile traffic to be marked down as specified in the markdown map.
- **set-dscp-transmit** {*dscp-value* | *dscp-bit-pattern* | **default** | **ef**}—Marks the matched traffic with a new DSCP value where the valid values are as follows:
  - *dscp-value*—Specifies a DSCP value; valid values are from 0 to 63.
  - *dscp-bit-pattern*—Specifies a DSCP bit pattern; valid values are listed in Table 2-28.
  - **default**—Matches packets with default dscp (000000).
  - **ef**—Matches packets with EF dscp (101110).

Table 2-28 Valid dscp-bit-pattern Values

Keyword	Definition
af11	Matches packets with AF11 dscp (001010).
af12	Matches packets withAF12 dscp (001100).
af13	Matches packets with AF13 dscp (001110).
af21	Matches packets with AF21 dscp (010010).
af22	Matches packets with AF22 dscp (010100).
af23	Matches packets with AF23 dscp (010110).
af31	Matches packets with AF31 dscp (011010).
af32	Matches packets with AF32 dscp (011100).
af33	Matches packets with AF33 dscp (011110).
af41	Matches packets with AF41 dscp (100010).
af42	Matches packets with AF42 dscp (100100).
af43	Matches packets with AF43 dscp (100110).
cs1	Matches packets with CS1 (precedence 1) dscp (001000).
cs2	Matches packets with CS2 (precedence 2) dscp (010000).
cs3	Matches packets with CS3 (precedence 3) dscp (011000).
cs4	Matches packets with CS4 (precedence 4) dscp (100000).
cs5	Matches packets with CS5 (precedence 5) dscp (101000).
cs6	Matches packets with CS6 (precedence 6) dscp (110000).
cs7	Matches packets with CS7 (precedence 7) dscp (111000).

- **set-mpls-exp-imposition-transmit** *new-mpls-exp*—Rewrites the MPLS experimental bits on imposed label entries and transmits. The *new-mpls-exp* argument specifies the value used to set the MPLS EXP bits that are defined by the policy map; valid values for *new-mpls-exp* are from 0 to 7.
- **set-mpls-exp-topmost-transmit**—Rewrites the MPLS experimental bits on the topmost label entries and transmits. The *new-mpls-exp* argument specifies the value used to set the MPLS EXP bits that are defined by the policy map; valid values for *new-mpls-exp* are from 0 to 7.
- **set-prec-transmit** *new-precedence*—Marks the matched traffic with a new IP-precedence value and transmits; valid values for *new-precedence* are from 0 to 7.
- **transmit**—Transmits the packets that do not exceed the *bits-per-second* rate.

Examples

This example shows how to create a policy map named max-pol-ipp5 that uses the class map named ipp5, which is configured to trust received IP-precedence values and is configured with a maximum-capacity aggregate 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 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)#
```

Related Commands

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
service-policy	Attaches a policy map to an interface.
show class-map	Displays class-map information.
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.

police rate

To configure traffic policing for traffic that is destined for the control plane, use the **police rate** command. To remove traffic policing from the configuration, use the **no** form of this command.

police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**]

police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

no police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**]

no police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

no police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

Syntax Description

units	Police rate; see the "Usage Guidelines" section for valid values.
pps	Specifies that the rate at which traffic is policed is in packets per second.
burst *burst-in-packets* **packets**	(Optional) Specifies the burst rate that is used for policing traffic; valid values are from 1 to 512000 packets.
peak-rate *peak-rate-in-pps* **pps**	(Optional) Specifies the PIR that is used for policing traffic; valid values are from from 1 to 512000 packets.
peak-burst *peak-burst-in-packets* **packets**	(Optional) Specifies the peak-burst value that is used for policing traffic; valid values are from 1 to 512000 packets.
bps	Specifies that the rate at which traffic is policed is in bits per second.
burst *burst-in-bytes* **bytes**	(Optional) Specifies the burst rate that is used for policing traffic; valid values are from 1000 to 512000000 bits.
peak-rate *peak-rate-in-bps* **bps**	(Optional) Specifies the peak burst value that is used for the peak rate; valid values are from 1000 to 512000000 bits.
peak-burst *peak-burst-in-bytes* **bytes**	(Optional) Specifies the peak burst value that is used for policing traffic; valid values are from 1000 to 512000000 bits.
percent *percentage*	(Optional) Specifies the percentage of interface bandwidth that is used to determine the rate at which traffic is policed; valid values are from 1 to 100.
burst *ms* **ms**	(Optional) Specifies the burst rate that is used for policing traffic; valid values are from 1 to 2000 milliseconds.
peak-rate percent *percentage*	(Optional) Specifies the percentage of the interface bandwidth that is used to determine the PIR; valid values are from 1 to 100.
peak-burst *ms* **ms**	(Optional) Specifies the peak burst rate that is used for policing traffic; valid values are from 1 to 2000 milliseconds.

Command Default

Disabled

Command Modes

Policy-map class configuration

Command History

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

Usage Guidelines

The valid values for *units* are as follows:

- If the police rate is specified in pps, the valid values are from 1 to 2000000 pps.
- If the police rate is specified in bps, the valid values are from 8,000 to 10,000,000,000 bps.

pps is used to calculate the PIR *peak-rate-in-pps*.

Use the **police rate** command to limit traffic that is destined for the control plane on the basis of packets per second (pps), bytes per seconds (bps), or a percentage of interface bandwidth.

If the **police rate** command is entered, but the rate is not specified, traffic that is destined for the control plane will be policed on the basis of bps.

Examples

This example shows how to configure policing on a class to limit traffic to an average rate of 1500000 pps:

```
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 rate 1500000 pps bc 500000 packets
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
show policy-map	Displays information about the policy map.

policy-map

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

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.

Command Default

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 (config)

Command History

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

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).
- **class** {*class-name* | **class-default**} accesses the class configuration mode to specify the name of the class whose policy you want to create or change (see the **class (policy-map)** command for additional information).
- **police** [**aggregate** *name*] subcommand defines a microflow or aggregate policer (see the **police (policy map)** command for additional information) and provides the following syntaxes:
  - **police** {**aggregate** *name*}
  - **police flow** {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*] [**pir** *peak-rate-bps*]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

  - **police flow mask** {**dest-only** | **full-flow** | **src-only**} {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*]} [**conform-action** *action*] [**exceed-action** *action*]

- **trust** {**cos** | **dscp** | **ip-precedence**} sets the specified class trust values. Trust values that are set in this command supersede trust values that are set on specific interfaces.

Table 2-29 describes the **class** syntax.

Table 2-29 class Syntax Description

Subcommand	Description
exit	(Optional) Exits from QoS class action configuration mode.
police	(Optional) Specifies flow policing; see the **police (policy map)** command for additional information.
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.

If you do not specify an **exceed-action** in the policy-map, it defaults to drop and the violate-action follows.

The 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 how to 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 2000000000 2000000 8000000 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

Command	Description
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
class (policy-map)	Specifies the name of the class that has a policy that you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
service-policy	Attaches a policy map to an interface.

Command	Description
show class-map	Displays class-map information.
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.

port access-map

To create a port access map or enter port access-map command mode, use the **port access-map** command. To remove a mapping sequence or the entire map, use the **no** form of this command.

port access-map *name* [*seq#*]

no port access-map *name* [*seq#*]

Syntax Description

name	Port access-map tag.
seq#	(Optional) Map sequence number; valid values are 0 to 65535.

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

If you enter the sequence number of an existing map sequence, you enter port access-map mode. If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence.

If you enter the **no port access-map name** [*seq#*] command without entering a sequence number, the whole map is removed.

Once you enter port access-map mode, the following commands are available:

- **action**—Specifies the packet action clause; see the **action** command section.
- **default**—Sets a command to its defaults.
- **end**—Exits from configuration mode.
- **exit**—Exits from the port access-map configuration mode.
- **match**—Specifies the match clause; see the **match** command section.
- **no**—Negates a command or sets its defaults.

Examples

This example shows how to enter port access-map mode:

```
Router(config)# port access-map ted
Router(config-port-map)#
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.

port-channel load-balance

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

port-channel load-balance *method*

no port-channel load-balance

Syntax Description

method	Load-distribution method; see the "Usage Guidelines" section for a list of valid values.

Command Default

method is **src-dst-ip**.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Valid *method* values are as follows:

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

The **port-channel per-module load-balance** command allows you to enable or disable port-channel load-balancing on a per-module basis.

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

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

This example shows how to set the load-distribution method on a specific module:

```
Router(config)# port-channel load-balance dst-ip module 2
Router(config)#
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
port-channel per-module load-balance	Enables load-distribution on a per-module basis.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel load-balance mpls

To set the load-distribution method among the ports in the bundle for MPLS packets, use the **port-channel load-balance mpls** command. To return to the default settings, use the **no** form of this command.

port-channel load-balance mpls {**label** | **label-ip**}

no port-channel load-balance mpls

Syntax Description

label	Specifies using the MPLS label to distribute packets; see the "Usage Guidelines" section for additional information.
label-ip	Specifies using the MPLS label or the IP address to distribute packets; see the "Usage Guidelines" section for additional information.

Command Default

label-ip

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you select **label**, these guidelines apply:

- With only one MPLS label, the last MPLS label is used.
- With two or more MPLS labels, the last two labels (up to the fifth label) are used.

If you select **label-ip**, these guidelines apply:

- With IPv4 and three or fewer labels, the source IP address XOR-destination IP address is used to distribute packets.
- With four or more labels, the last two labels (up to the fifth label) are used.
- With non-IPv4 packets, the distribution method is the same as the **label** method.

Examples

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

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

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel min-links

To specify that a minimum number of bundled ports in an EtherChannel is required before the channel can be active, use the **port-channel min-links** command. To return to the default settings, use the **no** form of this command.

port-channel min-links *min-num*

no port-channel min-links

Syntax Description

min-num	Minimum number of bundled ports in a channel that is required before the channel can be active; valid values are from 2 to 8.

Command Default

min-num is **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 supported on LACP (802.3ad) ports only. More than one LACP secondary port channel can belong to the same channel group. This command is applied to all port channels in the same group.

If fewer links than the specified number are available, the port-channel interface does not become active.

Use the **show running-config** command to verify the configuration.

Examples

This example shows how to specify that a minimum number of bundled ports in an EtherChannel is required before the channel can be active:

```
Router(config-if)# port-channel min-links 3
Router(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

port-channel per-module load-balance

To enable load-distribution on a per-module basis, use the **port-channel per-module load-balance** command. To return to the default settings, use the **no** form of this command.

port-channel per-module load-balance

no port-channel per-module load-balance

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **port-channel load-balance** *method* **module** *slot* command is supported on DFC systems only.

The **port-channel per-module load-balance** command allows you to enable or disable port-channel load-balancing on a per-module basis. You can enter the **port-channel load-balance** *method* **module** *slot* command to specify the load-balancing method on a specific module after you have entered the **port-channel per-module load-balance** command.

Examples

This example shows how to enable load balancing on a per-module basis:

```
Router(config)# port-channel per-module load-balance
Router(config)#
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
port-channel load-balance module	Enables load-distribution on a specific module.
show etherchannel	Displays the EtherChannel information for a channel.

power enable

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

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.

Command Default

Enabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When you enter the **no power enable module** *slot* command to power down a module, the module's configuration is not saved.

When you enter the **no power enable module** *slot* command to power down an empty slot, the configuration is saved.

The *slot* argument designates the module number. Valid values for *slot* depend on the chassis that is 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

Command	Description
show power	Displays information about the power status.

power inline

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

power inline {**auto** [**max** *max-milliwatts*]} | **never** | {**static** [**max** *max-milliwatts*]}

Syntax Description

auto	Turns on the device discovery protocol and applies power to the device, if found.
max *max-milliwatts*	(Optional) Specifies the maximum amount of power that a device connected to a port can consume; valid values are from 4000 to 16800 milliwatts.
never	Turns off the device discovery protocol and stops supplying power to the device.
static	Allocates power from the system power pool to a port.

Command Default

The defaults are as follows:

- **auto**.
- *max-milli-watts* is 15400 milliwatts.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.
12.2(18)ZYA	This command was changed to increase the *max-milliwatts* from 15400 to 16800.

Usage Guidelines

When configuring inline power support with the power inline command, note the following information:

- To configure auto-detection of an inline-powered device and auto-allocation of port inline power, enter the **auto** keyword.
- To configure auto-detection of an inline-powered device but reserve a fixed inline power allocation, enter the **static** keyword.
- To specify the maximum power to allocate to a port, enter either the **auto** or **static** keyword followed by the **max** keyword and the power level in milliwatts.
- When the **auto** keyword is entered and CDP is enabled on the port, an inline-powered device that supports CDP can negotiate a different power level.
- To disable auto-detection of an inline-powered device, enter the **never** keyword.

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
```

This example shows how to allocate power from the system power pool to a port:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline static max 15000
```

Related Commands

Command	Description
show power	Displays information about the power status.

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).

Command Default

redundant

Command Modes

Global configuration (config)

Command History

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

Examples

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

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

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

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

Related Commands

Command	Description
show power	Displays information about the power status.

priority-queue cos-map

To map CoS values to the receive and transmit strict-priority queues, use the **priority-queue cos-map** command. To return to the default mapping, use the **no** form of this command.

priority-queue cos-map *queue-id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]

Syntax Description

queue-id	Queue number; the valid value is **1**.
cos1	CoS value; valid values are from 0 to 7.
. . . *cos8*	(Optional) CoS values; valid values are from 0 to 7.

Command Default

The default mapping is queue 1 is mapped to CoS 5 for the following receive and transmit strict-priority queues:

- 1p1q4t receive queues
- 1p1q0t receive queues
- 1p1q8t receive queues
- 1p2q2t transmit queues
- 1p3q8t transmit queues
- 1p7q8t transmit queues
- 1p3q1t transmit queues
- 1p2q1t transmit queues

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

When mapping CoS values to the strict-priority queues, note the following information:

- The queue number is always **1**.
- You can enter up to 8 CoS values to map to the queue.

Examples

This example shows how to map CoS value 7 to the strict-priority queues on Gigabit Ethernet port 1/1:

```
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)#
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

priority-queue queue-limit

To se the priority-queue size on an interface, use the **priority-queue queue-limit** command.

priority-queue queue-limit *weight*

Syntax Description

weight	Priority-queue size weight; valid values are from 1 and 100 percent.

Command Default

The default settings are as follows:

- Global QoS is enabled—15
- Global QoS is disabled—0

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

See the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for a list of modules that support this command.

Examples

This example shows how to allocate available buffer space to a priority queue:

```
Router(config-if)# priority-queue queue-limit 15
Router(config-if)#
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

private-vlan

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

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

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

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

no private-vlan association

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.
secondary-vlan-list	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.

Command Default

No PVLANs are configured.

Command Modes

config-VLAN submode

Command History

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

Usage Guidelines

You cannot configure PVLANs on a port-security port.

If you enter a **pvlan** command on a port-security port, this error message is displayed:

```
Command rejected: Gix/y is Port Security enabled port.
```

Within groups of 12 ports (1–12, 13–24, 25–36, and 37–48), do not configure the ports as isolated or as community VLAN ports when one of the ports is a trunk, a SPAN destination, or a promiscuous private VLAN port. If one port is a trunk, a SPAN destination, or a promiscuous private VLAN port, any isolated or community VLAN configuration for the other ports within the 12 ports is inactive. To reactivate the ports, remove the isolated or community VLAN-port configuration and enter the **shutdown** and **no shutdown** commands.

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.

Note This restriction applies to Ethernet 10-Mb, 10/100-Mb, and 100-Mb modules except WS-X6548-RJ-45 and WS-X6548-RJ-21.

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* argument 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* argument can contain only one isolated VLAN ID. A PVLAN is a set of private ports that are 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.

You can specify only one isolated *vlan-id*, 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, you cannot configure a VLAN that is already associated to a primary VLAN 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 that are associated with the VLAN become inactive.

Refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional configuration guidelines.

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 delete the primary VLAN. The associated secondary VLANs are not deleted.

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

Related Commands

Command	Description
show vlan	Displays VLAN information.
show vlan private-vlan	Displays PVLAN information.

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. To remove all PVLAN mappings from the SVI, use the **no** form of this command.

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

no private-vlan mapping

Syntax Description

secondary-vlan-list	(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.

Command Default

No PVLAN SVI mapping is configured.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **private-vlan mapping** command affects traffic that is switched in the software on the PISA.

The *secondary-vlan-list* argument 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 that is 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 that are 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 that 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

Command	Description
show interfaces private-vlan mapping	Displays the information about the PVLAN mapping for VLAN SVIs.
show vlan	Displays VLAN information.
show vlan private-vlan	Displays PVLAN information.

private-vlan synchronize

To map the 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.

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

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

Command	Description
show	Verifies the MST configuration.
show spanning-tree mst	Displays information about the MST protocol.

process-min-time percent

To specify the minimum percentage of CPU process time OSPF takes before trying to release the CPU for other processes, use the **process-min-time percent** command. To return to the default settings, use the **no** form of this command.

process-min-time percent *percent*

no process-min-time

Syntax Description

percent	Percentage of CPU process time to be used before trying to release the CPU for other processes; valid values are from 1 to 100.

Command Default

percent is **25**.

Command Modes

Router configuration

Command History

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

Usage Guidelines

Note Use this command under the direction of Cisco TAC only.

This command is supported by OSPFv2 and OSPFv3.

Use the **process-min-time** command to configure the minimum percentage of the process maximum time. Once the percentage has been exceeded, CPU control may be given to a higher priority process.

The process maximum time is set using the **process-max-time** command. Use the **process-min-time** command with the **process-max-time** command.

Examples

This example shows how to set the percentage of CPU process time to be used before releasing the CPU:

```
Router> configure terminal
Router(configure)# router ospf
Router(config-router)# process-min-time percent 35
Router(config-router)#
```

This example shows how to return to the default setting:

```
Router> configure terminal
Router(configure)# router rip
Router(config-router)# no process-min-time
Router(config-router)#
```

Related Commands

Command	Description
process-max-time	Configures the amount of time after which a process should voluntarily yield to another process.