

Punt Policing and Monitoring

Punt policing protects the Route Processor (RP) from having to process noncritical traffic, which increases the CPU bandwidth available to critical traffic. Traffic is placed into different CPU queues based on various criteria. The Punt Policing and Monitoring feature allows you to police the punt rate on a per-queue basis.

- Feature Information for Punt Policing and Monitoring, on page 1
- Information About Punt Policing and Monitoring, on page 1
- Restrictions for Per-Interface Per-Cause Punt Policer, on page 2
- How to Configure Punt Policing and Monitoring, on page 2
- Verifying Punt Policing, on page 6
- Configuration Examples for Punt Policing and Monitoring, on page 9
- Additional References, on page 10

Feature Information for Punt Policing and Monitoring

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Punt Policing and Monitoring

Information About Punt Policing and Monitoring

Overview of Punt Policing and Monitoring

Packets received on an interface are punted to the Router Processor (RP) for various reasons. Some examples of these various reasons include, unicast and multicast control plane traffic that are destined for a routing protocol process running on the RP, and IP packets that generate Internet Control Message Protocol (ICMP) exceptions such as a Time to live (TTL) expiration. The RP has a limited capacity to process the punted packets, and while some of them are critical for the router operation and should not be dropped, some can be dropped without impacting the router operation.

Punt policing frees the RP from having to process noncritical traffic. Traffic is placed in queues based on various criteria, and you can configure the maximum punt rate for each queue which allows you to configure the system so that packets are less likely to be dropped from queues that contain critical traffic.

Note Traffic on certain CPU queues could still be dropped, regardless of the configured punt rate, based on other criteria such as the queue priority, queue size, and traffic punt rate.

Per-Interface Per-Cause Punt Policer

Per-interface per-cause (PIPC) punt policing is an enhancement to the Punt Policing and Monitoring feature that allows you to control and limit traffic per interface. From Cisco IOS XE Release 17.5.1, you can set the PIPC rate for all the control plane-punted traffic. When you set the PIPC rate, any traffic beyond the set limit is dropped, thereby enabling you to control the traffic during conditions such as L2 storming.

The PIPC punt policer configuration is supported for the following interfaces:

- Main interface
- Subinterface
- Port channel
- Port channel subinterface
- Tunnels
- PPPoE interface

Restrictions for Per-Interface Per-Cause Punt Policer

- PIPC punt policing is not supported for L2 Ethernet Flow Points (EFPs).
- This configuration supports only two policies per interface.

How to Configure Punt Policing and Monitoring

Configuring Punt Policing

Note Traffic on a specific CPU queue may be dropped irrespective of the configured maximum punt rate, based on the queue priority, queue size, and the configured traffic punt rate.

Perform this task to specify the maximum punt rate on the specified queue.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform qos-policer queue** *queue-id cir bc*
4. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters the global configuration mode.
Step 3	**platform qos-policer queue** *queue-id cir bc* **Example:** Device(config)# platform qos-policer queue 20 384000 8000	Enables punt policing on a queue, and specifies the maximum punt rate on a per-queue basis. *cir*— Indicates Committed Information Rate (CIR). The range is 384000-20000000 bps. *bc*— Indicates Committed Burts (BC). The range is 8000-16000000 bps. **Note** The **platform qos-policer** command is supported on Cisco Aggregation Services Router 920 devices that are equipped with the Route Switch Processor 2 module and utilize the XE Cylon-based chipset.
Step 4	**end** **Example:** Device(config)# end	(Optional) Returns to privileged EXEC mode.

Configuring Punt Policing on an Interface

Note At an interface level, punt control can be enabled or disabled by the **no punt-control enable** command. You can configure the rate, however, by default, it uses the global configuration if the rate is not configured.

Perform this task to enable or disable punt control on an interface:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform punt-interface rate***rate*
4. **punt-control enable** *rate*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**platform punt-interface rate***rate* **Example:** Device(config)# platform punt-interface rate 10	Sets the global punt-interface policer rate.
Step 4	**punt-control enable** *rate* **Example:** Device(config)# interface Port-channel 1.2 Device(config-if)# punt-control enable	Punt control is enabled at an interface level.
Step 5	**end** **Example:**	(Optional) Returns to privileged EXEC mode.

Configuring Punt Policing Per Interface Per Cause

SUMMARY STEPS

1. enable
2. configure terminal
3. **punt-control cause <cause> <rate>**
4. end

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Device> enable`	This enables the privileged EXEC mode. Enter the password, if prompted.
Step 2	configure terminal **Example:** `Device# configure terminal`	This enables the Global Configuration mode.
Step 3	**punt-control cause <cause> <rate>** **Example:** `Device(config-if)# punt-control cause arp 80`	This sets the PIPC rate for the interface that you specify, for example, **punt-control cause arp 80**.
Step 4	end	This exits the current configuration.

Example

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface GigabitEthernet 1
Device(config-if)# punt-control cause arp 80
```

Configuring the Default PIPC Rate for an Interface

Procedure

	Command or Action	Purpose

Step 1	To set a default global PIPC rate for at an interface level, enter the platform punt-intf per-cause rate <rate> command.
	Example:
	`platform punt-intf per-cause rate 100  // Global PIPC rate`
	`interface Port-channel1.100`
	`punt-control cause bfd-control // PIPC rate 100`
	`punt-control cause arp 200 // PIPC rate 200`
		Sets the default global PIPC rate for the interface that you specify. Here, the default rate for BFD is set to 100, while the default rate for ARP is 200. If there's an inflow beyond the specified rate for this interface, the traffic is dropped.

Verifying Punt Policing

Verifying Queue-Based Punt Policing

Use the **show platform software infrastructure punt statistics** to display punt police statistics:

```
Router# show platform software infrastructure punt statistics
UEA Punt Statistics

Global drops : 0

 Queue Name              | Rx count                    |  Drop count
-------------------------+-----------------------------+------------------------
 SW FORWARDING Q         | 0                           | 0
 ROUTING PROTOCOL Q      | 0                           | 0
 ICMP Q                  | 0                           | 0
 HOST Q                  | 57115                       | 0
 ACL LOGGING Q           | 0                           | 0
 STP Q                   | 0                           | 0
 L2 PROTOCOL Q           | 6571                        | 0
 MCAST CONTROL Q         | 208839                      | 0
 BROADCAST Q             | 4                           | 0
 REP Q                   | 0                           | 0
 CFM Q                   | 0                           | 0
 CONTROL Q               | 0                           | 0
 IP MPLS TTL Q           | 0                           | 0
 DEFAULT MCAST Q         | 0                           | 0
 MCAST ROUTE DATA Q      | 0                           | 0
 MCAST MISMATCH Q        | 0                           | 0
 RPF FAIL Q              | 0                           | 0
 ROUTING THROTTLE Q      | 87                          | 0
 MCAST Q                 | 0                           | 0
 MPLS OAM Q              | 0                           | 0
 IP MPLS MTU Q           | 0                           | 0
 PTP Q                   | 0                           | 0
 LINUX ND Q              | 0                           | 0
 KEEPALIVE Q             | 0                           | 0
 ESMC Q                  | 0                           | 0
 FPGA BFD Q              | 0                           | 0
 FPGA CCM Q              | 0                           | 0
 FPGA CFE Q              | 0                           | 0
 L2PT DUP Q              | 0                           | 0
```

Verifying Punt Policing Statistics

Use the **show platform hardware pp active infrastructure pi npd rx policer** command to display the punt policing statistics for all queues.

```
Ring |           Queue Name |            Punt rate |           Burst rate
-----+----------------------+----------------------+---------------------
 0   |      SW FORWARDING Q |                  500 |                 1000
 1   |   ROUTING PROTOCOL Q |                  500 |                 1000
 2   |               ICMP Q |                  500 |                 1000
 3   |               HOST Q |                 1000 |                 2000
 4   |        ACL LOGGING Q |                  500 |                 1000
 5   |                STP Q |                 3000 |                 6000
 6   |        L2 PROTOCOL Q |                 1000 |                 2000
```

```
 7   |     MCAST CONTROL Q |                1000 |                2000
 8   |         BROADCAST Q |                1000 |                2000
 9   |               REP Q |                3000 |                6000
10   |           BGP LDP Q |                3000 |                6000
11   |           CONTROL Q |                1000 |                2000
12   |       IP MPLS TTL Q |                1000 |                2000
13   |     DEFAULT MCAST Q |                 500 |                1000
14   |  MCAST ROUTE DATA Q |                 500 |                1000
15   |    MCAST HIGH PRI Q |                1000 |                2000
16   |          RPF FAIL Q |                 500 |                1000
17   |  ROUTING THROTTLE Q |                 500 |                1000
18   |             MCAST Q |                 500 |                1000
19   |          MPLS OAM Q |                1000 |                2000
20   |       IP MPLS MTU Q |                 500 |                1000
21   |               PTP Q |                3000 |                6000
22   |          LINUX ND Q |                 500 |                1000
23   |         KEEPALIVE Q |                1000 |                2000
24   |              ESMC Q |                3000 |                6000
25   |          FPGA BFD Q |                4000 |                8000
26   |          FPGA CCM Q |                4000 |                8000
27   |          FPGA CFE Q |                1000 |                2000
28   |          L2PT DUP Q |                4000 |                8000
29   |          TDM CTRL Q |                3000 |                6000
30   |  ICMP UNREACHABLE Q |                 500 |                1000
31   |             SSFPD Q |                6000 |               12000
```

Use the **show platform software infrastructure punt statistics** command to view the statistics on the RSP3 module.

```
Router#

Global drops : 0

 Queue Name              | Rx count                     |  Drop count
-------------------------+------------------------------+-----------------------
 SW FORWARDING Q         | 0                            | 0
 ROUTING PROTOCOL Q      | 0                            | 0
 ICMP Q                  | 0                            | 0
 HOST Q                  | 0                            | 0
 ACL LOGGING Q           | 0                            | 0
 STP Q                   | 0                            | 0
 L2 PROTOCOL Q           | 0                            | 0
 MCAST CONTROL Q         | 0                            | 0
 BROADCAST Q             | 0                            | 0
 REP Q                   | 0                            | 0
 BGP LDP Q               | 0                          | 0
 CONTROL Q               | 0                            | 0
 IP MPLS TTL Q           | 0                            | 0
 DEFAULT MCAST Q         | 0                            | 0
 MCAST ROUTE DATA Q      | 0                            | 0
 MCAST MISMATCH Q        | 0                          | 0
 RPF FAIL Q              | 0                            | 0
 ROUTING THROTTLE Q      | 0                            | 0

MCAST Q                 | 0                            | 0
 MPLS OAM Q              | 0                            | 0
 IP MPLS MTU Q           | 0                            | 0
 PTP Q                   | 0                            | 0
 LINUX ND Q              | 0                            | 0
 KEEPALIVE Q             | 0                          | 0
 ESMC Q                  | 0                            | 0
 FPGA BFD Q              | 0                            | 0
 FPGA CCM Q              | 0                            | 0
 FPGA CFE Q              | 0                            | 0
 L2PT DUP Q              | 0                            | 0
```

```
 TDM CTRL Q              | 0                          | 0
 ICMP UNREACHABLE Q      | 0                      | 0
 SSFP Q                  | 0                          | 0
 MIRROT Q                | 0                          | 0
```

Use the **show platform hardware pp active feature qos policer cpu all 1** command to clear the statistics of all the CPU queues.

Use the **show platform hardware pp active feature qos policer cpu all 0** command to clear the statistics of a particular CPU queue.

```
########## Stats for CPU queue 0 ##########
Internal Qnum: 1         Queue Name: SW FORWARDING Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000

########### Stats for CPU queue 1 ##########
Internal Qnum: 2         Queue Name: ROUTING PROTOCOL Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000
_______
_______
_______
########### Stats for CPU queue 30 ##########
Internal Qnum: 31        Queue Name: ICMP UNREACHABLE Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000

########### Stats for CPU queue 31 ##########
Internal Qnum: 32        Queue Name: SSFPD Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000
```

Use **show platform hardware pp active feature qos policer cpu 3 0** to display the queue specific statistics.

```
########### Stats for CPU queue 3 ##########
Internal Qnum: 4         Queue Name: HOST Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 12000000, Policer burst commit is 3000000

3 —— queueId of CPU   and 0 — show stats
```

Use the **show platform hardware pp active feature qos policer cpu all 0** to display the output after adding the drop cause. Following commands are applicable only for RSP3 module:

```
########### Stats for CPU queue 0 ##########
Internal Qnum: 8000CPU
Port num: 0
Policer conform: 0 (packets) 0 (bytes)
Policer exceed:  0 (packets) 0 (bytes)
Policer commit rate is: 500000 bps, Policer burst commit is 16000 bytes
########### Stats for CPU queue 1 ##########
Internal Qnum: 8008CPU
Port num: 0
```

```
Policer conform: 0 (packets) 0 (bytes)
Policer exceed:  0 (packets) 0 (bytes)
Policer commit rate is: 1000000 bps, Policer burst commit is 100000 bytes
########### Stats for CPU queue 2 ##########
Internal Qnum: 8016CPU
Port num: 0
Policer conform: 0 (packets) 0 (bytes)
Policer exceed:  0 (packets) 0 (bytes)
Policer commit rate is: 1000000 bps, Policer burst commit is 100000 bytes
```

Verifying Per-Interface Per-Cause Punt Policer

Procedure

Step 1 To verify whether the global PIPC rate has been successfully attached, run the **show run | in platform** command:

Example:

```
Device# show run | in platform
platform punt-intf per-cause rate 100
```

Step 2 To verify whether the PIPC configuration is enabled, run the **show run int <interface>** command. In the following sample configuration, the punt-control cause in the output verifies that the PIPC rate of 80 for ARP is successfully applied:

Example:

```
Device# show run int GigabitEthernet 1
Building configuration...
Current configuration : 100 bytes
!
interface GigabitEthernet1
punt-control cause arp 80
!
End
```

Example

What to do next

-

Configuration Examples for Punt Policing and Monitoring

Example: Configuring Punt Policing

The following example shows how to enable punt-policing:

```
Router# enable
Router# configure terminal
```

```
Router(config)# platform qos-policer queue 3 384000 8000
```

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Traffic marking	"Marking Network Traffic" module
Traffic policing	"Traffic Policing" module
Traffic policing and shaping concepts and overview information	"Policing and Shaping Overview" module
Modular quality of service command-line interface (MQC)	"Applying QoS Features Using the MQC" module

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html