



# Cisco 10000 Series Router Control Plane Policing—Platform Enhancement

---

**First Published: April, 2008**

During a denial of service (DoS) attack, a high volume of traffic can be sent (punted) to the route processor (RP). To protect the RP, the Control Plane Policing (CoPP) feature and the platform-specific features divert-cause policer and To-RP queues work together to classify and rate-limit the packets punted to the RP. While these features provide a good method of protecting the RP from DoS attacks, they might impact the services of innocent users. The Control Plane Policing—Platform Enhancement feature addresses this issue of user fairness, providing you the ability to monitor malicious users so you can take action to drop or rate-limit the traffic at the user level.

In addition to the CoPP enhancements, Cisco IOS Release 12.2(33)SB also provides the following features and functions to enhance security:

- Loose mode unicast reverse path forwarding (uRFP) for IPv4
- Input classification using the **match protocol arp** command on all interface types that support the modular QoS CLI (MQC)
- DHCP as a separate divert cause in the divert cause policer

For more information about uRFP, see the *Unicast Reverse Path Forwarding* feature module, Release 12.2(33)SB.

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for CoPP—Platform Enhancement](#)” section on page 23.

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

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



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

# Contents

- [Information About Control Plane Policing—Platform Enhancement, page 2](#)
- [Restrictions for CoPP—Platform Enhancement, page 6](#)
- [Configuring the Rate and Burst Size of the Divert Cause Policer, page 6](#)
- [Examples of Configuring the Rate and Burst Size of the Divert Cause Policer, page 7](#)
- [Example of Handling an ARP Storm Attack, page 8](#)
- [Verifying and Monitoring Packets Diverted to the RP, page 8](#)
- [Verification Examples for Diverted Packets, page 9](#)
- [Additional References, page 11](#)
- [Command Reference, page 12](#)
- [Feature Information for CoPP—Platform Enhancement, page 23](#)

## Information About Control Plane Policing—Platform Enhancement

The Control Plane Policing (CoPP)—Platform Enhancement feature enhances CoPP by providing the following functionality:

- [User-Level Punt Monitoring, page 4](#)
- [Configurable Rate and Burst Size for the Divert Cause Policer, page 5](#) for
- [Drop Alarms for Packet Drops by the To-RP Queues and Divert Cause Policer, page 5](#)

Cisco IOS Release 12.2(31)SB introduced the divert cause policer and reorganized the To-RP queues. The following sections review these concepts, which are basic to understanding the CoPP—Platform Enhancement feature:

- [Divert Cause Policer, page 2](#)
- [Divert Causes, page 3](#)
- [To-RP Queues, page 4](#)

## Divert Cause Policer

The *divert cause policer* is a set of policers that provide aggregated DoS protection by regulating the traffic sent (punted) to the router processor (RP) based on the traffic divert causes. The divert policer is a single-rate, two-color PXF policer that applies rate-limiting to punted traffic for each of the divert causes.

In releases prior to Cisco IOS Release 12.2(33)SB, the policer is statically set and you cannot change it.

## Divert Causes

A *divert cause* is a PXF classification of the packets being punted to the RP. The divert cause enables the PXF to group punted traffic by packet type. Cisco supports over 80 packet types. Each divert cause has its own unique divert policer instance.

In Cisco IOS Release 12.2(33)SB, the router supports the following divert causes:

- divert\_all
- encap
- clns\_isis
- clns
- cdp
- cgmp
- arp
- rarp
- mpls\_ctl
- keepalive
- ppp\_cntrl
- fr\_lmi
- atm\_ilmi
- pppoeoa\_disc
- oam\_f4
- oam\_f5\_ete
- oam\_f5\_seg
- mlfr\_lmi
- mlfr\_lpi
- srp\_topo
- srp\_ips
- ip\_version
- ip\_options
- fib\_glean
- hsc
- tfib\_flag
- tfib\_ip\_opt
- mfib\_224
- mfib\_igmp
- bridge\_pdu
- mfib\_assert
- mfib\_null\_out
- mfib\_direct
- mfib\_join\_spt
- mfib\_register
- mfib\_no\_fast
- mfib\_local\_mem
- lacp\_pdu
- mfib\_no\_group
- acl\_log\_ipc
- pbr\_arp
- ipc\_resp
- netflow\_ipc
- pppoe\_disc
- atm\_crl
- fr\_peek
- ppp\_keepalive
- l2tp\_cntrl
- acl\_punt
- iedge\_debug
- iedge\_punt
- iedge\_no\_xlt
- mpls\_echo
- mpls\_ttl
- mpls\_vcev
- mfib\_host\_mode
- mfib\_tun\_frag
- v6\_src\_link\_local
- v6\_hop\_opts
- v6\_glean
- v6\_icmp
- v6\_lng\_ext\_hdr
- v6\_mfib\_assert
- v6\_mfib\_null\_out
- v6\_mfib\_direct\_src
- v6\_mfib\_join\_spt
- v6\_mfib\_register
- v6\_mfib\_no\_fast
- v6\_mib\_local\_mem
- v6\_mfib\_no\_group
- v6\_mfib\_tun\_frag
- v6\_mfib\_lnk\_if\_loc
- v6\_mfib\_site\_local
- iedge\_ips\_fsol
- v6\_dst\_mcast
- v6\_dst\_linklocal
- dhcp
- fib\_dest
- fib\_rp
- fib\_bcast
- v6\_rp\_dest
- v6\_rp\_punt
- v6\_mcast\_rsvd

To display punted packets by the divert cause, use the **show pxf cpu statistics diversion pxf** command.

## To-RP Queues

The router aggregates the punted traffic from all users, and uses CoPP and the divert cause policer in the PXF to process the traffic. The PXF places the punted packets in one of eight To-RP queues. The packets in the queue have different bandwidths and are subject to being dropped if the queue becomes congested, except for high priority packets.

The To-RP queues are static queues that segment diverted traffic, providing additional protection for the RP. The To-RP queues are organized into the following eight queues:

- Layer 2 control
- Layer 3 control
- Access control lists (ACLs)
- Netflow
- IPC
- Normal Layer 2
- Normal Layer 3
- Default

The PXF sends packets for each divert cause to one of the To-RP queues. The router uses weighted round robin to service the queues and provides more bandwidth and weight to the control queues. To see statistical information from the dequeue and drop counters, use the **show pxf cpu queue** command.

## User-Level Punt Monitoring

One of the CoPP enhancements introduced in Cisco IOS Release 12.2(33)SB is user-level punt monitoring.

User-level punt monitoring enhances your ability to monitor users and traffic to prevent a denial of service (DoS) attack. Using this feature, you can monitor individual users and display statistical information about traffic that the parallel express forwarding (PXF) engine sends (punts) to the route processor (RP). This information allows you to see when a DoS attack occurs. You can then take action by dropping or rate-limiting the punted traffic.

In Cisco IOS Release 12.2(31)SB and later releases, you can address DoS attacks by classifying and rate-limiting the packets that the PXF engine punts to the RP for further processing. This protects the RP, but might impact the services of innocent users because this method drops all packets without differentiating between malicious users and innocent users. For example, when one or more users with malicious intentions flood the router with Layer 2 or Layer 3 control packets (for example ARP or DHCP packets), the PXF drops not only the packets of the malicious users, but also the packets of other users with the same protocol type. User-level punt monitoring addresses this issue of user fairness by allowing you to display information about the punted traffic of specific users.

In Cisco IOS Release 12.2(33)SB and later releases, user-level punt monitoring makes it possible to collect and display per-user statistical information about the packets punted to the RP. Using this feature, you can determine if a particular user has a high rate of punted packets, in which case you might choose to take action, such as rate-limiting the packets of that particular user or if the offending user is a PPP session, you might terminate the session and disable the user's ability to log in. In this way, you can limit the impact of malicious users on innocent user services.

User-level punt monitoring enables you to:

- Monitor punted traffic at the per-user level to help you identify possible DoS attackers
- Display the types of traffic from an inbound interface, subinterface, or session that the PXF punts to the RP

To determine a user's identity, the router monitors the Layer 2 header information of the control packets and the inbound interface, subinterface, or session. User-level punt monitoring for both Layer 2 and per-input interface is enabled by default.

User-level punt monitoring is available on the PRE2, PRE3, and PRE4.

## Configurable Rate and Burst Size for the Divert Cause Policer

Another CoPP enhancement introduced in Cisco IOS Release 12.2(33)SB is the ability to configure the rate and burst size of the divert cause policer.

Cisco IOS Release 12.2(31)SB introduces the divert cause policer. However, you cannot configure the rate and burst size.

In Cisco IOS Release 12.2(33)SB and later releases, you can configure the rate and burst size of the policer, using the **platform c10k divert-policer** command. The rate is specified in packets per second (pps) and the burst size in number of packets. The rate has an internal granularity of 125 pps, which means that the rate must be a multiple of 125. You may specify any rate desired; however, the router rounds the specified rate to a multiple of 125.

## Drop Alarms for Packet Drops by the To-RP Queues and Divert Cause Policer

A final CoPP enhancement introduced in Cisco IOS Release 12.2(33)SB is the ability to send drop alarms for packet drops by the To-RP queues and divert cause policer.

To help you monitor possible DoS attacks, the router sends warning messages (alarms) to the console and the syslog log file to alert you when a change in drop activities occurs, such as packet drops due to congestion in the To-RP queues or due to aggregated traffic that violates the divert cause policer. The information these alarms provide depends on the condition that caused the drop alarm to occur.

[Table 1](#) describes the kinds of information provided in the drop alarms.

**Table 1** Information Provided in Drop Alarms

Condition	Information Provided	Basis of the Message
Divert cause police violation	Logging time Divert cause of the drop (due to police rate exceeded)	Per-divert cause based
To-RP queue drops	Time Queue name	Per-queue based

The router displays an alarm similar to the following when a change in drop activities occurs for the divert cause policer. The alarm includes the name of the divert cause (for example, ARP or DHCP) that has a change in its drop status. In this example, arp is the divert cause experiencing dropped traffic. If no more drops occur for a period of 10 minutes, the router clears the alarms to avoid flooding the log file with messages.

```
00:01:06: %C10K_ALARM-6-COPP: DIV-POLICE arp drops asserted
00:02:10: %C10K_ALARM-6-COPP: DIV-POLICE arp drops de-asserted
```

The router displays an alarm similar to the following for To-RP queue dropped traffic. In this sample alarm, the RP queue experiencing the drops is the default queue. Anytime the To-RP queues have a change in drop status, the router raises an alarm. The alarms clear if no more drops occur for a period of 10 minutes.

```
00:03:06: %C10K_ALARM-6-COPP: TO-RP-Q default drops asserted
00:05:10: %C10K_ALARM-6-COPP: TO-RP-Q default drops de-asserted
```

The router periodically checks for divert cause police violations and To-RP queue drops, and logs only changed drop activities (for example, drops are present during this time period, but were not present in the previous period or no drops are present in this time period, but were present in the previous period). The router generates the alarms on the first status change from the last monitoring period to the current monitoring period. The corresponding drop counter changes from zero to a non-zero value or from a non-zero value to zero. Logging only changed activities avoids possible flooding of the log files.

**Note**


---

You can use the Embedded Event Manager (EEM) to generate SNMP traps for the syslog messages.

---

## Restrictions for CoPP—Platform Enhancement

- The router does not support issuing the **show pxf cpu statistics diversion top** command in multiple Telnet sessions. If you do, erroneous output displays.
- For broadband applications, when you issue the **show pxf cpu statistics diversion top** command on a router configured for multihop, the output of the command might display invalid user session information.

## Configuring the Rate and Burst Size of the Divert Cause Policer

To configure the rate and burst size of the divert cause policer, use the following procedure.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform c10k divert-policer *divert-cause-name* rate *rate* [*burst burst-size*]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; <b>enable</b></p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# <b>configure terminal</b></p>	Enters global configuration mode.
Step 3	<pre>platform c10k divert-policer divert-cause-name rate rate [burst burst-size]</pre> <p><b>Example:</b> Router(config)# <b>platform c10k divert-policer</b> <b>arp rate 1250 burst 300</b></p>	Specifies the rate and burst size of the divert cause policer. <i>divert-cause-name</i> is the name of the diversion cause for which you are enabling the policer. <p><b>rate</b> <i>rate</i> is the police rate, expressed in packets per second (pps) and rounded to a multiple of 125. Valid values are from 0 to 8,191,874 pps.</p> <p><b>Note</b> The police rate has a granularity of 125 pps. If you specify a rate that is not a multiple of 125, the router rounds the rate down. If you specify a rate that is between 1 and 124 inclusive, the router uses a rate of 125 pps.</p> <p><b>burst</b> <i>burst-size</i> specifies the burst size, expressed in number of packets. Valid values are from 1 to 65,534 packets.</p>

## Examples of Configuring the Rate and Burst Size of the Divert Cause Policer

The following example shows how to configure the divert cause policer for the **arp** diversion cause with a police rate of 200 pps and a burst size of 100 packets:

```
Router# config terminal
Router(config)# platform c10k divert-policer arp rate 200 burst 100
```

**Note**

The provisioned rate of 200 pps is rounded down to 125 pps by the router because the PXF can only handle rates that are a multiple of 125. If the input rate value is between 1 and 124, the policer uses the minimum value of 125 pps.

The following example also shows how to configure the rate and burst size of the divert cause policer. The example specifies the **arp** diversion cause, a police rate of 2000 pps, and a burst size of 500 packets:

```
Router# config terminal
Router(config)# platform c10k divert-policer arp rate 2000 burst 500
```

## Example of Handling an ARP Storm Attack

The following example describes how the CoPP—Platform Enhancement feature can help you to handle an ARP storm attack:

1. A message similar to the following displays at the console or in the syslog log file:
 

```
00:01:06: %C10K_ALARM-6-COPP: DIV-POLICE arp drops asserted
```
2. You enter the **show pxf cpu statistics diversion top 20** command to display the top 20 punters (interfaces, subinterfaces, and sessions) that divert or punt packets to the RP at the fastest rate. In this example, interface GigabitEthernet 3/1/0.1 is one of the top 20 punters.
3. You enter the **show pxf cpu statistics diversion pxf interface** command to determine who among the top punters (interfaces, subinterface, and sessions) is punting lots of ARP packets. In this example, VLAN interface GigabitEthernet 3/1/0.1 is punting the ARP packets.
4. You add a policy map or a new class to interface GigabitEthernet 3/1/0.1 to rate-limit the ARP packets. For example, the following sample configuration adds the traffic class named `c_arp` to police ARP packets at a rate of 8000 bps. The policy map named `p_in` is applied to interface GigabitEthernet 3/1/0.1.

```
Class-map c_arp
  Match protocol arp

Policy-map p_in
  Class c_arp
    Police 8000

interface GigabitEthernet3/1/0.1
  service-policy input p_in
```

## Verifying and Monitoring Packets Diverted to the RP

To verify and monitor packets diverted to the RP, use any of the following commands in privileged EXEC mode:

Command	Purpose
Router# <b>show pxf cpu statistics diversion</b>	Displays statistical information about the packets received by the RP from the PXF. This command shows the number of packets the RP receives for each divert cause and the rate of the punted packets.  <b>Note</b> To see an accurate rate, execute this command multiple times, back-to-back.
Router# <b>show pxf cpu statistics diversion pxf</b>	Displays PXF CPU statistics for the packets the PXF diverted to the RP.  The output of this command was enhanced in Cisco IOS Release 12.2(33)SB to display the provisioned burst size for any divert causes.

Command	Purpose
Router# <b>show pxf cpu statistics diversion pxf interface</b> [ <i>interface</i>   <i>vcci-number</i> ]	<p>Displays divert cause policer counters for the specified interface. <i>interface</i> is the type and number of the interface on which the divert cause policer is configured (for example, GigabitEthernet 1/0/0.10). <i>vcci-number</i> is the VCCI number of the interface.</p> <p><b>Note</b> The PXF collects the VCCI-based counts after the VCCI is created using the CLI. Therefore, the divert packet numbers displayed by this command only represent the counts during the polling period.</p>
Router# <b>show pxf cpu statistics diversion top</b> [ <i>number</i> ]	<p>Displays the top punters (interfaces, subinterfaces, and sessions) who are punting the most packets to the RP. The output displays the top punters by interface and by Layer 2 flow. <i>number</i> is the number of top punters to display. Valid values are from 1 to 100.</p> <p><b>Note</b> If there are fewer punters than you specify, the router displays the interfaces, subinterfaces, and sessions that are currently punting traffic.</p>
Router# <b>show running-config</b>	Displays the current router configuration in the running-configuration file.

## Verification Examples for Diverted Packets

The following example shows sample output from the **show pxf cpu statistics diversion** command. This example displays the number of packets punted to the RP for each diversion cause and the rate of the packets when the RP received them.

```
Router# show pxf cpu statistics diversion
```

```

Diversion Cause   Packet   Rate (pps)
divert_all        = 0      0
encap             = 0      0
clns_isis         = 0      0
clns              = 0      0
cdp               = 0      0
cgmp              = 0      0
arp               = 46     0
rarp              = 0      0
mpls_ctl          = 0      0
keepalive         = 0      0
ppp_cntrl         = 0      0
fr_lmi            = 0      0
atm_ilmi          = 0      0

```

The following example shows sample output from the **show pxf cpu statistics diversion pxf** command. This example displays PXF CPU data and statistics for the packets the PXF diverted to the RP.

```
Router# show pxf cpu statistics diversion pxf
```

PXF Divert Policer data and stats (in pps):

Diversion Cause	Diverted		Dropped		Max Rate	Burst	Class Name
	packet	byte	packet	byte			
divert_all	= 0	0	0	0	-	-	default
encap	= 0	0	0	0	250	1000	default
clns_isis	= 0	0	0	0	5000	1000	l3_ctrl
clns	= 0	0	0	0	5000	1000	l3
cdp	= 0	0	0	0	1000	3000	l2
cgmp	= 0	0	0	0	1000	1000	l2ctrl
arp	= 1	70	0	0	125	100	l2_ctrl
rarp	= 0	0	0	0	1000	500	l2
mpls_ctl	= 0	0	0	0	1000	500	l3_ctrl
keepalive	= 0	0	0	0	10000	5000	l2_ctrl

The following example shows sample output from the **show pxf cpu statistics diversion pxf interface** command. The example displays divert cause policer counts for Gigabit Ethernet interface 3/1/0.

```
Router# show pxf cpu statistics diversion pxf interface gigabitethernet3/1/0
```

Divert counts for GigabitEthernet3/1/0:

Diversion Cause	Diverted		Dropped	
	packet	byte	packet	byte
divert_all	= 0	0	0	0
encap	= 0	0	0	0
clns_isis	= 0	0	0	0
clns	= 0	0	0	0
cdp	= 0	0	0	0
cgmp	= 0	0	0	0
arp	= 998	95808	0	0



#### Note

The information displayed for this command is similar to the information displayed at the aggregated level.

The following example shows sample output from the **show pxf cpu statistics diversion top** command. This example displays the top 10 punters.

```
Router# show pxf cpu statistics diversion top 10
```

Top 10 punters by interface are:

Rate(pps)	Packets(diverted/dropped)	vcci	Interface
18051	20000 /0	2525	GigabitEthernet3/0/0.1
Last diverted packet type is arp			
... ..			

Top 10 punters by layer 2 flow are:

Rate(pps)	Packets(diverted/dropped)	Interface	Layer 2 info
18053	20000 /0	GigabitEthernet3/0/0.10009.b68d.9348/0x0806000108000604	
Last diverted packet type is arp			



#### Note

If there are fewer punters than you specify, the router displays the interfaces, subinterfaces, and sessions that are currently punting traffic.

The following example shows sample output from the **show running-config** command. The sample output displays the divert cause policer configured for the **arp** diversion cause. The policer rate, originally provisioned at 200 pps, is rounded down to 125 pps because the PXF can only handle rates that are multiples of 125.

```
Router# show running-config
Building configuration...

... ..
platform c10k divert-policer arp rate 125 burst 100
... ..
```

## Additional References

The following sections provide references related to the Control Plane Policing—Platform Enhancement feature.

## Related Documents

Related Topic	Document Title
Control Plane Policing	<a href="#">Control Plane Policing, Release 12.2SB</a>
show Commands	Cisco IOS Command Reference, Release 12.2SB
DoS Attacks	<i>Cisco 10000 Series Router Software Configuration Guide</i> <a href="#">Protecting the Router from DoS Attacks</a>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This section documents new and modified commands for the Control Plane Policing—Platform Enhancement feature.

For information about these and all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup>.

- [platform c10k divert-policer](#)
- [show pxf cpu statistics](#)

## platform c10k divert-policer

To set the rate and burst size of the divert-policer on a Cisco 10000 series router, use the **platform c10k divert-policer** command in global configuration mode. To disable the divert-policer for the specified divert-cause, use the **no** form of this command.

**platform c10k divert-policer** *divert-cause-name* **rate** *rate* [**burst** *burst-size*]

**no platform c10k divert-policer** *divert-cause-name* **rate** *rate* [**burst** *burst-size*]

Syntax Description		
	<i>divert-cause-name</i>	Name of the diversion cause for which you are enabling the policer.
	<b>rate</b> <i>rate</i>	Specifies the police rate, expressed in packets per second (pps) and rounded to a multiple of 125. Valid values for <i>rate</i> are from 0 to 8,191,874 pps.
	<b>burst</b> <i>burst-size</i>	Specifies the burst size, expressed in number of packets. Valid values for <i>burst-size</i> are from 1 to 65,534 packets.

**Command Default** Enabled

**Command Modes** Global configuration (config)#

Command History	Release	Modification
	12.2(33)SB	This command was introduced on the Cisco 10000 series router for the PRE2, PRE3, and PRE4.

**Usage Guidelines** The police rate has a granularity of 125 pps. If you specify a rate that is not a multiple of 125, the router rounds the rate down. If you specify a rate that is between 1 and 124 inclusive, the policer uses a rate of 125 pps.

**Examples** The following example shows how to configure the divert-policer for the arp diversion cause with a police rate of 200 pps and a burst size of 100 packets:

```
Router# config terminal
Router(config)# platform c10k divert-policer arp rate 200 burst 100
```



**Note**

The specified police rate of 200 pps is not a multiple of 125; therefore, the policer rounds the rate down to 125 pps.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show pxf cpu statistics diversion pxf interface</b>	Displays PXF statistical information about the divert-cause policer for a specific interface or VCCI.
<b>show pxf cpu statistics diversion top</b>	Displays PXF statistical information about the top specified number of punted packets.



# show pxf cpu statistics

To display Parallel eXpress Forwarding (PXF) CPU statistics, use the **show pxf cpu statistics** command in privileged EXEC mode.

```
show pxf cpu statistics [atom | backwalk | clear | diversion | drop [interface | vcci] | ip | ipv6 |
l2tp | mlp | qos [interface] | queue | rx [vcci] | security | arp-filter | drl [ cable-wan-ip |
wan-non-ip ]]
```

## Cisco 10000 Series Router

```
show pxf cpu statistics diversion [ pxf [interface {interface | vcci}] | top number]
```

Syntax	Description
<b>atom</b>	(Optional) Displays Any Transport over MPLS (AToM) statistics.
<b>backwalk</b>	(Optional) Displays backwalk requests statistics.
<b>clear</b>	(Optional) Clears PXF CPU statistics.
<b>diversion</b>	(Optional) Displays packets that the PXF diverted to the Route Processor (RP) for special handling.
<b>drop</b> [interface] [vcci]	(Optional) Displays packets dropped by the PXF for a particular interface or Virtual Circuit Connection Identifier (VCCI).
<b>ip</b>	(Optional) Displays IP statistics.
<b>ipv6</b>	(Optional) Displays IPv6 statistics.
<b>l2tp</b>	(Optional) Displays packet statistics for an L2TP Access Concentrator (LAC) (Optional) and L2TP Network Server (LNS).
<b>mlp</b>	(Optional) Displays multilink PPP (MLP) statistics.
<b>pxf</b>	(Optional) Displays packets that the PXF diverted to the Route Processor (RP). Available on the Cisco 10000 series router only.
<b>pxf interface</b> interface	(Optional) Displays per-interface PXF statistical information for the divert cause policer on a particular interface. Available on the Cisco 10000 series router only.
<b>pxf interface</b> vcci	(Optional) Displays per-VCCI PXF statistical information for the divert cause policer on a particular Virtual Circuit Connection Identifier (VCCI). Available on the Cisco 10000 series router only.
<b>qos</b> [interface]	(Optional) Displays match statistics for a service policy on an interface.
<b>queue</b>	(Optional) Displays queueing counters for all interfaces.
<b>rx</b> [vcci]	(Optional) Displays receive statistics for a VCCI.
<b>security</b>	(Optional) Displays ACL matching statistics.
<b>top number</b>	(Optional) Displays PXF statistical information for the number of top punters you specify. Available on the Cisco 10000 series router only. Valid values are from 1 to 100.
<b>arp-filter</b>	(Optional) Displays the ARP filter statistics.
<b>drl</b>	(Optional) Displays the divert rate limit.
<b>cable-wan-ip</b>	(Optional) Displays cable / wan-ip statistics for dropped packets.
<b>wan-non-ip</b>	(Optional) Displays DRL wan-non-ip statistics for dropped packets.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
	12.2(28)SB	This command was introduced on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(28)SB.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SB	This command was enhanced to display per-interface or per-VCCI PXF statistical information for the divert cause policer on a particular interface or VCCI, to display the top punters on an interface, and to display the provisioned burst size for any divert causes. These enhancements were implemented on the Cisco 10000 series router for the PRE2, PRE3, and PRE4.
	12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers. Support for the Cisco uBR7225VXR router was added. The <b>arp-filter</b> , <b>drl</b> , <b>cable-wan-ip</b> , and <b>wan-non-ip</b> keywords were added .

### Usage Guidelines

#### Cisco 10000 Series Router Usage Guidelines

- The **show pxf cpu statistics diversion** command displays statistical information about diverted packets. Divert causes with the string "ipv6..." display as "v6..." in the output of all **show pxf cpu statistics diversion** commands
- The output from the **show pxf cpu statistics diversion pxf** command was enhanced in Cisco IOS Release 12.2(33)SB to display the provisioned burst size for any divert causes.
- The **show pxf cpu statistics diversion pxf interface *interface*** command displays statistical information about the divert cause policer on a specific interface. The output of this command is similar to the output displayed at the aggregated level. This command enables you to see the traffic types being punted from an inbound interface, subinterface, and session.
- The **show pxf cpu statistics diversion pxf interface *vcci*** command displays statistical information about the divert cause policer on a specific VCCI. The output of this command is similar to the output displayed at the aggregated level. This command enables you to see the traffic types being punted from an inbound interface, subinterface, and session.
- The **show pxf cpu statistics diversion top *number*** command displays the interfaces, subinterfaces, and sessions with the highest number of punter packets.

### Examples

The following example shows PXF queuing counters information. These are aggregate counters for all interfaces. The Total column is the total for all columns.

**Note**

If you are troubleshooting link utilization issues, the `deq_vtp_req`, `deq_flow_off`, and `deq_ocq_off` counters may indicate what is causing the versatile time management scheduler (VTMS) to slow down.

If you are troubleshooting overall PXF throughput issues, look at the High Next Time, Low Next Time, High Wheel Slot, and Low Wheel Slot counters.

Router# **show pxf cpu statistics queue**

Column 6 Enqueue/Dequeue Counters by Rows:

dbg Counters	0	1	2	3	4	5	6	7	
Total									
===== =====									
enq_pkt 0x0007EE55	0x0000FD9B	0x0000FC77	0x0000FE4A	0x0000FF81	0x0000FC53	0x0000FD2E	0x0000FF19	0x0000FDDE	
tail_drop_pkt 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
deq_pkt 0x0007EE55	0x0000FD47	0x0000FEF2	0x0000FCB3	0x0000FF65	0x0000FCE7	0x0000FC45	0x0000FEE7	0x0000FDF1	
deq_vtp_req 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
deq_flow_off 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
deq_ocq_off 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
enqdeq_conflict 0x000001F0	0x0000003A	0x00000043	0x0000004A	0x00000039	0x0000003A	0x0000004F	0x00000036	0x00000031	
bndl_pkt 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
frag_pkt 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
dbg_frag_drop 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
dbg_bndl_sem 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
context_inhibit 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
bfifo_enq_fail 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
dbg1 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
dbg2 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
dbg3 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
dbg4 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
dbg5 0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	
dbg6 0x0000	0x0000	0x0000	0x0000	0x0000	0x0000	0x0000	0x0000	0x0000	
dbg7	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00

Column 7 Rescheduling State Counters by Rows:

dbg Counters	0	1	2	3	4	5	6	7
Total								

```

=====
=====
High Next Time 0x524E1100 0x524E1140 0x524E1140 0x524E1180 0x524E11C0 0x524E11C0 0x524E1200 0x524E1240 -
Low Next Time 0x524E1100 0x524E1140 0x524E1140 0x524E1180 0x524E11C0 0x524E1200 0x524E1200 0x524E1240 -
High Wheel Slot 0x00000844 0x00000845 0x00000846 0x00000846 0x00000847 0x00000848 0x00000848 0x00000849 -
Low Wheel Slot 0x00000844 0x00000845 0x00000846 0x00000846 0x00000847 0x00000848 0x00000848 0x00000849 -
DEQ_WHEEL 0x0001F5D0 0x0001F4BD 0x0001F56B 0x0001F6BF 0x0001F396 0x0001F3E8 0x0001F6BF 0x0001F4A7
0x000FA99B
DQ-lock Fails 0x0000039F 0x000003FD 0x000003B2 0x000003E1 0x000003CB 0x000003E2 0x000003FD 0x000003CD
0x00001EA6
TW_ENQ Fails 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
Q_SCHED 0x0000FACD 0x0000FC6B 0x0000FA38 0x0000FCE4 0x0000FA66 0x0000F994 0x0000FC62 0x0000FB8B
0x0007DA3B
FAST_SCHED 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
Q_DEACT 0x0000FB03 0x0000F852 0x0000FB33 0x0000F9DB 0x0000F930 0x0000FA54 0x0000FA5D 0x0000F91C
0x0007CF60
Q_ACTIVATE 0x0000F9B6 0x0000F8D4 0x0000FA6C 0x0000FBA9 0x0000F87E 0x0000F95B 0x0000FB0A 0x0000F9DE
0x0007CF60
Q_CHANGE 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG2 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG3 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG4 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG5 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000

```

Table 2 describes the significant fields shown in the display.

**Table 2** *show pxf cpu statistics queue Field Descriptions*

Field	Description
Column 6 Enqueue/Dequeue Counters by Rows:	
enq_pkt	Packets the PXF enqueued.
tail_drop_pkt	Packets the PXF tails dropped.
deq_pkt	Packets the PXF dequeued.
deq_vtp_req	Number of times a dequeue was inhibited due to the virtual traffic policer.
deq_flow_off	Numbers of times a dequeue was inhibited due to a flowoff from the line card.
deq_ocq_off	Number of times a dequeue was inhibited due to link level flow control.
enqdeq_conflict	Shows a dequeue failed due to an enqueue to the same queue in progress.
bndl_pkt	Count of packets that were fragmented.
frag_pkt	Count of fragments sent.
dbg_frag_drop	Count of invalid multilink PPP (MLP) fragment handles.
dbg_bndl_sem	Count of semaphore collision (used for MLP).

**Table 2** *show pxf cpu statistics queue Field Descriptions (continued)*

Field	Description
context_inhibit	Number of times multilink transmit fragment processing was inhibited due to a lack of DMA resources.
bfifo_enq_fail	Count of bundle FIFO (BFIFO) enqueue failures.
Column 7 Rescheduling State Counters by Rows:	
High Next Time	Current next send time for the high priority wheel.
Low Next Time	Current next send time for the low priority wheel.
High Wheel Slot	Current high priority slot number.
Low Wheel Slot	Current low priority slot number.
DEQ_WHEEL	Count of successful dequeues from the timing wheel.
DQ-lock Fails	Count of timing wheel dequeue failures (both queue empty and race conditions).
TW ENG Fails	Timing wheel enqueue failures.
Q_SCHED	Count of queues scheduled/rescheduled onto the timing wheel.
FAST_SCHED	Count of queues fast scheduled/rescheduled onto the timing wheel.
Q_DEACT	Count of queue deactivations.
Q_ACTIVATE	Count of queue activations (activate state).
Q_CHANGE	Count of queue changes; for example, Route Processor (RP) inspired rates changes.

The following example displays PXF L2TP packet statistics.

**Note**

For L2TP Access Concentrator (LAC) operation, all statistics are applicable. For L2TP Network Server (LNS) operation, only the PPP Control Packets, PPP Data Packets, and PPP Station Packets statistics are meaningful.

```
Router# show pxf cpu statistics l2tp

LAC Switching Global Debug Statistics:
  PPP Packets          51648
  PPP Control Packets  51647
  PPP Data Packets     1
  Not IPv4 Packets    1
  IP Short Hdr Packets 1
  IP Valid Packets     0
  IP Invalid Packets   1
  DF Cleared Packets   0
  Path MTU Packets     0
  No Path MTU Packets  0
  Within PMTU Packets  0
  Fraggable Packets    0
  PMTU Pass Packets    0
  PMTU Fail Packets    0
  Encapped Packets     51648
```

```
L2TP Classification Global Debug Statistics:
LAC or Multihop Packets 151341
Multihop Packets        0
PPP Control Packets     51650
PPP Data Packets        99691
PPP Station Packets     151341
```

The following example displays match statistics for the police\_test policy on an ATM interface. The Classmap Index differentiates classes within a policy while the Match Number differentiates match statements within a class.

```
Router# show pxf cpu statistics qos atm 6/0/0.81801
```

Classmap Index	Match Number	Pkts Matched	Bytes Matched
police_test (Output) service-policy :			
police_class (0)	0	0	0
	1	0	0
	2	0	0
	3	0	0
class-default (1)	0	0	0

### Cisco 10000 Series Router

The following example displays the top 10 packet types diverted to the RP. The output displays the top punters by interface and by Layer 2 packet flow.

```
Router# show pxf cpu statistics diversion top 10
```

Top 10 punters by interface are:

Rate (pps)	Packets (diverted/dropped)	vcci	Interface
1	10/0	2606	Virtual-Access2.1

Last diverted packet type is none.

Top 10 punters by Layer 2 flow are:

Rate (pps)	Packets (diverted/dropped)	Interface	Layer 2 info
1	15/0	ATM2/0/3	vpi 128/vci 4096/vcci 2591

Last diverted packet type is oam\_f4.

1	15/0	ATM2/0/3	vpi 128/vci 4096/vcci 2593
---	------	----------	----------------------------

Last diverted packet type is oam\_f4.

### Related Commands

Command	Description
<b>platform c10k divert-policer</b>	Configures the rate and burst size of the divert-policer.
<b>show pxf statistics</b>	Displays a summary of statistics in the PXF.



# Feature Information for CoPP—Platform Enhancement

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for Control Plane Policing—Platform Enhancement

Feature Name	Releases	Feature Information
Control Plane Policing—Platform Enhancement	12.2(33)SB	<p>This feature provides the following CoPP enhancements: user-level punt monitoring, configurable rate and burst size for the divert cause policer, and drop alarms for packet drops by the To-RP queues and the divert cause policer. This feature also adds DSCP as a divert cause.</p> <p>In 12.2(33)SB, this feature was introduced on the Cisco 10000 series router for the PRE2, PRE3, and PRE4.</p> <p>The following commands were introduced or modified:  <b>platform c10k divert-policer, show pxf cpu statistics diversion, show pxf cpu statistics diversion pxf interface, show pxf cpu statistics diversion top.</b></p> <p>The output of the following command was modified:  <b>show pxf cpu statistics pxf</b></p>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0804R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

