PXF Divert Rate Limit Enhancement on the Cisco CMTS Routers

First Published: December 18, 2008

Last Updated: January 28, 2016

This document describes the Parallel eXpress Forwarding (PXF) Divert Rate Limit (DRL) Enhancement on the Cisco Cable Modem Termination System (CMTS). This feature prevents congestion of packets on the forwarding processor (FP) or the PXF processor to the Route Processor (RP) interface, which can be caused by denial of service (DoS) attacks directed at the CMTS or by faulty hardware.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Contents

Prerequisites for PXF DRL Enhancement

The PXF DRL Enhancement feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.2(33)SCB. The table shows the Cisco CMTS hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 1: PXF DRL Enhancement Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Line Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later** • PRE2	**Cisco IOS Release 12.2(33)SCB and later** • Cisco uBR10-MC5X20S/U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V [1]

[1] Cisco uBR3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

Restrictions for PXF DRL Enhancement

- DRL cannot be configured on a cable bundle interface.
- The trusted-site list can contain a maximum of four sites.
- WAN-IP entities are identified using a hash, and hash collisions can occur between two (or more) entities.
- The DRL feature is always on; it cannot be turned off.
- The PXF DRL Enhancement feature is not applicable to Address Resolution Protocol (ARP) packets arriving from a cable interface. These packets are rate limited by the ARP filter feature.

Information About PXF DRL Enhancement

The PXF DRL Enhancement feature prevents congestion of the FP-to-RP interface by identifying and rate-limiting entities that would otherwise cause congestion.

Diverted packets are sent from the forwarding processor to the Route Processor through the FP-to-RP interface. This interface gets congested when packets (that require diversion) arrive at the FP at a faster rate than they can be transmitted to the RP. When the interface gets congested, valid packets in the FP-to-RP queues are tail-dropped. This situation can be caused deliberately by DoS attacks directed at the CMTS, or by faulty external hardware.

The PXF DRL Enhancement feature identifies packet streams that cause congestion on the FP-to-RP interface. Packets in the stream are then dropped according to the configured rate-limiting parameters. Rate-limiting occurs before the packets are placed in the FP-to-RP queues, thereby allowing other valid packets to reach the RP.

The PXF DRL Enhancement feature applies to both cable and WAN interfaces.

Even if the DRL (per source based divert rate limit) is configured on the WAN interface, sometimes the RP gets overloaded due to Distributed Dos (DDos) attack. The DDos attack is seen when the following occurs:

- When the packets are being pointed to the CMTS directly.
- When the packets are being pointed to a CPE. If the CPE goes down and all traffic gets punted to PRE.

Effective with Cisco IOS Release 12.2(33)SCH3, when the DDos occurs and the flooding packets have one of the support divert codes, the DRL Max-Rate Per Divert-Code on WAN Interface can be configured to reduce the CPU utilization.

PXF DRL Enhancement on a Cable Interface

The PXF DRL Enhancement feature applies to upstream packets from a cable interface. In cable, the entities must be rate-limited on a deterministic basis. Because certain entities (for example, VoIP calls) must be able to divert packets successfully, a probabilistic model cannot be used. As a result, the Media Access Control (MAC)-domain and service identifier (SID) identifies the subscribers. DRL aggregates and limits all diverted traffic originating from a subscriber.

PXF DRL Enhancement on a WAN Interface

The PXF DRL Enhancement feature applies to packets from a non-cable interface (typically a Gigabit Ethernet line card.) WAN-side entities cannot be rate-limited on a deterministic basis due to the large number of entities that can exist. Therefore, a probabilistic model (that is, a hash) is used to identify packet streams. This means that not all entities will be uniquely identified.

IP packet streams are identified and rate-limited by a hash of the source IP address, the fib-root (for example, the VPN routing and forwarding [VRF] name), and the divert code. Non-IP packet streams are not expected on the WAN interface, and are therefore rate-limited on a divert code basis.

A WAN-side “trusted-site” list can be maintained, with a maximum of four trusted sites. Each entry in the “trusted-site” list contains an IP address and mask, an IP type of service (ToS) value and mask, and a VRF name. Packets matching a trusted site will not be subject to rate-limiting. In addition, packets from trusted sites will not affect the rate-limiting of packets from other entities.

How to Configure PXF DRL Enhancement on the Cisco CMTS Routers

This section describes the following required and optional procedures:

Configuring US Cable Divert-Rate-Limit

The cable side DRL is configured on the physical cable interface. It cannot be configured on a cable bundle interface. To configure cable DRL, use the **cable divert-rate-limit** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface* **Example:** `Router(config)# interface C5/0/0`	Enters interface configuration mode for the specified interface. - **interface—**Specifies the name of the physical Cable interface.
Step 4	**cable divert-rate-limit rate** *rate* **limit** *limit* **Example:** `Router(config-if)#` **cable divert-rate-limit rate 1 limit 4**	Specifies the DRL rate and limit. - **rate—**Specifies the divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. The default rate is 2000 packets per second. - **limit—**Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. The default limit is 2000 packets.

Step 5	end
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN IPv4 Rate and Limit

To configure DRL for WAN-side IPv4 packet streams, use the **service divert-rate-limit ip** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit ip** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)#` **service divert-rate-limit ip fib-rp-glean rate 1 limit 4**	Specifies the DRL rate and limit for the WAN interface. • **divert-code—**Specifies the applicable divert code. • **rate—**Specifies the divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. For WAN-IP packets, the default rate is 4000 packets per second. • **limit—**Specifies the number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. For WAN-IP packets, the default limit is 4000 packets.

Step 4	end
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN IPv6 Rate and Limit

To configure DRL for WAN-side IPv6 packet streams, use the **service divert-rate-limit ipv6** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit ipv6** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)# service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit 10`	Specifies the DRL rate and limit for the WAN interface. • *divert-code*—Applicable divert code. Refer to the list of divert codes in Cisco IOS CMTS Cable Command Reference • **rate**—Divert rate in packets per second. The minimum rate is 1 packet per second and the maximum rate is 65535 packets per second. For WAN-IP packets, the default rate is 4000 packets per second. • **limit**—Number of packets to be diverted in an initial burst of packets. The minimum limit is 4 packets and the maximum limit is 4194 packets. For WAN-IP packets, the default limit is 4000 packets.

Step 4	end
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN Non-IP Rate and Limit

To configure DRL for WAN-side non-IP packet streams, use the **service divert-rate-limit non-ip** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**service divert-rate-limit non-ip** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)#` **service divert-rate-limit non-ip cgmp rate 1 limit 4** **Example:**	Specifies the DRL rate and limit for the WAN interface. - **divert-code—**Applicable divert code. - **rate—**Divert rate in packets per second. Minimum rate is 1 packet per second. Maximum rate is 65535 packets per second. For WAN non-IP packets, the default rate is 2000 packets per second. - **limit—**Number of packets to be diverted in an initial burst of packets. Minimum limit is 4 packets. Maximum limit is 4194 packets. For WAN non-IP packets, the default limit is 2000 packets.

Step 4	end
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring an IPv4 Trusted Site

Each entry in the IPv4 trusted-site list contains a source IP address and mask, an IP ToS value and mask, and a VRF name. The IPv4 “trusted-site” list applies only to WAN-side IPv4 packets. A maximum of four IPv4 trusted sites can be configured.

To configure a trusted-site list, use the **service divert-rate-limit trusted-site** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **Example:**	Adds entries to the IPv4 trusted-site list using the specified parameters. **Note** If no VRF name is specified, the trusted site applies to all VRF and the global Internet.

	Command or Action	Purpose
	Example: **service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **global** **Example:** **Example:** **service divert-rate-limit trusted-site** *source-ip ip-mask* **tos** *tos-value* **mask** *tos-mask* **vrf** *vrf-name* **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3** **Example:** **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3 global** **Example:** **Example:** `Router(config)#` **service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255** **Example:** **tos 0xD0 mask 0xF3 vrf name1**	• **source-ip—**Specifies the source IP address that should be matched. • **ip-mask—**Specifies the mask to apply to the source IP address of the packet before testing if it matches. There are no restrictions on the mask-ip-address value. • **tos tos-value—**Specifies the ToS value of the trusted site. There are no restrictions on the tos-value value. • **mask tos-mask—**Specifies the mask to apply to the IP ToS value and the trusted-site tos value before testing whether it matches. There are no restrictions on the tos-mask value. • **global—**Specifies that the trusted-site is applicable to the global internet, but not to other VRF names. • **vrf vrf-name—**Specifies the VPN routing and forwarding (VRF) name that applies to this trusted site. **Note** Only four entries are allowed in the IPv4 trusted site list.

Step 4	end
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring an IPv6 Trusted Site

Each entry in the IPv6 'trusted site' list contains a 128-bit source IP address & mask, an 8-bit traffic-class value & mask, and a VRF name. The IPv6 trusted-site list applies only to WAN-side IPv6 packets. A maximum of four IPv6 trusted site can be configured.

To configure a IPv6 trusted-site list, use the service divert-rate-limit trusted-site-ipv6 command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **Example:** **Example:** **service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **global** **Example:** **Example:** **service divert-rate-limit trusted-site-ipv6** *ip-address traffic-class tc_value mask tc-mask* **vrf** *vrf-name* **Example:** `Router(config)#service divert-rate-limit trusted-site-ipv6 2001:420:3800:800:21F:29FF::1/128 traffic-class 0x3 mask 0xFF global`	Adds IPv6-specific entries to the trusted-site list using the specified parameters. **Note** If no VRF name is specified, the trusted site applies to all VRF and the global Internet. • ip-address/prefix-length—The source IPv6 address/ prefix-length that should be matched. • traffic-class tc_value—The 8-bit traffic-class of the trusted site. There are no restrictions on the tc_value. • mask tc-mask—The mask to apply to the packet traffic-class and the trusted-site tc_value before testing if it matches. • **global**—The trusted-site is applicable to the global internet, but not to other VRF names. • **vrf vrf-name**—VPN routing and forwarding (VRF) name that applies to this trusted site. **Note** Only four entries are allowed in the trusted site list.

	Command or Action	Purpose

Step 4	end
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring DRL Max-Rate Per Divert-Code on WAN Interface

Effective with Cisco IOS Release 12.2(33)SCH3, per-divert-code rate limit can be configured on the WAN interface to reduce the CPU utilization.

The DRL Max-Rate Per Divert-Code on WAN Interface can be configured, when the DDos occurs and the flooding packets have one of the support divert codes.

This procedure provides information to configure per-divert-code rate limit on the WAN interface.

Before You Begin

Before you configure the service divert-rate-limit max-rate command, it is recommended to configure the source based DRL first.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>` **`enable`**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router#` **`configure terminal`**	Enters global configuration mode.
Step 3	**service divert-rate-limit max-rate wan** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)#` **`service divert-rate-limit max-rate wan fib_rp_dest rate 5000 limit 100`**	Specifies the DRL rate and limit for the WAN interface per divert-code. • **divert-code—**Specifies the applicable divert code. ◦ fib_rp_dest— IPv4 packets targeting to CMTS. ◦ fib_rp_glean—FIB glean adjacency used for IPv4 adjacency resolving. ◦ fib_rp_punt—FIB punt adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_dest—IPv4 packets targeting to CMTS. ◦ ipv6_rp_glean—IPv6 receive adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_punt—IPv6 punt adjacency used for IPv4 adjacency resolving.

	Command or Action	Purpose
		Starting from Cisco IOS Release 12.2(33)SCJ, the following divert codes were supported: ◦ mfib_224_0_0_x—The Packet whose destination IP is 224.0.0.x. ◦ icmpv6—IPv6 ICMP ◦ mfib_igmp—IGMP protocol packet ◦ ipv6_nd_na_mcast—IPv6 ND NA (multicast) ◦ ipv6_nd_na_ucast—IPv6 ND NA (unicast) ◦ ipv6_nd_ns_mcast—IPv6 ND NS (multicast) ◦ ipv6_nd_ns_ucast—IPv6 ND NS (unicast) ◦ ipv6_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IPV6 header. ◦ ipv6_src_linklocal—IPv6 SRC LinkLocal ◦ fib_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IP header. • **rate**—Specifies the divert rate in packets/sec. The range is from 1 to 65535. The default value is 4194. • **limit**—Specifies the limit for the number of packets that will be diverted in an initial burst of packets. The range is from 4 to 4194.The default value is 4194.

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring DRL Max-Rate Per Divert-Code on Upstream Cable Interface

Effective with Cisco IOS Release 12.2(33)SCJ, per-divert-code rate limit can be configured on the upstream cable interface to reduce the CPU utilization.

The DRL Max-Rate Per Divert-Code on upstream cable interface can be configured, when the DDos occurs and the flooding packets have one of the support divert codes.

This procedure provides information to configure per-divert-code rate limit on the upstream cable interface.

Before You Begin

Before you configure the service divert-rate-limit max-rate command, it is recommended to configure the source based DRL first.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service divert-rate-limit max-rate us-cable** *divert-code* **rate** *rate* **limit** *limit* **Example:** `Router(config)# service divert-rate-limit max-rate us-cable fib_rp_dest rate 5000 limit 100`	Specifies the DRL rate and limit for the upstream cable interface per divert-code. • **divert-code**—Specifies the applicable divert code. ◦ mfib_224_0_0_x—The Packet whose destination IP is 224.0.0.x. ◦ icmpv6—IPv6 ICMP ◦ mfib_igmp—IGMP protocol packet ◦ ipv6_nd_na_mcast—IPv6 ND NA (multicast) ◦ ipv6_nd_na_ucast—IPv6 ND NA (unicast) ◦ ipv6_nd_ns_mcast—IPv6 ND NS (multicast) ◦ ipv6_nd_ns_ucast—IPv6 ND NS (unicast) ◦ fib_rp_dest— IPv4 packets targeting to CMTS. ◦ fib_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IP header. ◦ fib_rp_glean—FIB glean adjacency used for IPv4 adjacency resolving. ◦ fib_rp_punt—FIB punt adjacency used for IPv4 adjacency resolving. ◦ src_ver_leasequery_req—Divert to RP due to zero MD and sid value and need to send lease query to DHCP server for those packets. ◦ src_ver_unknown_ip_addr—Divert to RP due to zero MD and sid value and no adjacency information for source IP address of those packets. ◦ ipv6_rp_dest—IPv4 packets targeting to CMTS. ◦ ipv6_rp_dest_precedence—The packet whose destination is RP and has non-zero precedence value in IPV6 header. ◦ ipv6_rp_glean—IPv6 receive adjacency used for IPv4 adjacency resolving. ◦ ipv6_rp_punt—IPv6 punt adjacency used for IPv4 adjacency resolving. ◦ ipv6_src_linklocal—IPv6 SRC LinkLocal ◦ ipv6_src_ver_mac_req—Divert to RP due to zero MD and sid value.

	Command or Action	Purpose
		• **rate**—Specifies the divert rate in packets/sec. The range is from 1 to 65535. The default value is 4194. • **limit**—Specifies the limit for the number of packets that will be diverted in an initial burst of packets. The range is from 4 to 4194.The default value is 4194.

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Verifying US Cable Dropped Packets

To view and verify the number of upstream cable packets that are dropped from the CMTS, use the show pxf cpu statistics drl us-cable command as shown in the following examples:

```
Router# show pxf cpu statistics drl us-cable
Divert-Rate-Limit US-cable statistics
   dropped   identifier
       361   interface: Cable6/0/1   SID: 28
      2457   interface: Cable6/0/0   SID: 1
Router# show pxf cpu statistics drl us-cable threshold 400
Divert-Rate-Limit US-cable statistics :: threshold = 400
   dropped   identifier
      2457   interface: Cable6/0/0   SID: 1
Router#
```

Verifying WAN IPv4 Dropped Packets

To verify drop counters for WAN-IPv4 packets, use the show pxf cpu statistics drl ipv4 commands as shown in the following examples:

```
Router# show pxf cpu statistics drl ipv4
Divert-Rate-Limit WAN-IPv4 statistics
   dropped   identifier
       460   11.12.13.10  VRF: global  divert_code: fib_rp_dest
       150   11.12.13.10  VRF: global  divert_code: fib_limited_broadcast
Router#
Router# show pxf cpu statistics drl ipv4 threshold 400
Divert-Rate-Limit WAN-IPv4 statistics :: threshold = 400
   dropped   identifier
       460   11.12.13.10  VRF: global  divert_code: fib_rp_dest
```

Verifying WAN IPv6 Dropped Packets

To verify drop counters for WAN-IPv6 packets, use the show pxf cpu statistics drl ipv6 commands as shown in the following examples:

```
Router# show pxf cpu statistics drl ipv6
Divert-Rate-Limit WAN-IPv6 statistics
   dropped   identifier
       460   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_dest
       150   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_punt
Router#
Router# show pxf cpu statistics drl ipv6 threshold 400
Divert-Rate-Limit Cable/WAN-IP statistics :: threshold = 400
   dropped   identifier
       460   10FA:6604:8136:6502::/64  VRF: global  divert_code: ipv6_rp_dest
Router#
```

Verifying WAN Non-IP Dropped Packets

To verify drop counters for WAN non-IP packets, use the **show pxf cpu statistics drl non-ip or** show pxf cpu statistics drl non-ip threshold commands as shown in the following examples:

```
Router# show pxf cpu statistics drl non-ip
Divert-Rate-Limit WAN-non-IP statistics
   dropped divert_code
         5 cdp
        17 cgmp
Router# show pxf cpu statistics drl non-ip threshold 10
Divert-Rate-Limit WAN-non-IP statistics :: threshold = 10
   dropped divert_code
        17 cgmp
```

Verifying the Trusted-Site List

To verify the trusted-site configuration, use the **show pxf cpu drl trusted-sites** command as shown in the following example:

```
Router# show pxf cpu drl trusted-sites
Divert-Rate-Limit IPv4 Trusted-Site list
 IP-addr          IP-addr mask     ToS   ToS mask  VRF
 60.0.1.0         255.255.255.0    0x18  0xF8      blue
 50.0.1.0         255.255.255.240  0x01  0xFF      <all>
 50.0.0.0         255.255.255.0    0x18  0xF8      <global internet>
Divert-Rate-Limit IPv6 Trusted-Site list
 5436:6AB4:2344::1/128  tc 0xA3  tc_mask 0xFF  VRF <all>
Router#
```

Verifying WAN DRL Max-Rate Dropped Packets

To verify drop counters for the DRL max-rate on the WAN interface, use the **show pxf cpu statistics drlmax-rate** command as shown in the following examples:

```
Router#show pxf cpu  statistics drl max-rate wan threshold 1
dropped   divert_code
      2617    cable_filter_us
```

Verifying US Cable DRL Max-Rate Dropped Packets

To verify drop counters for the DRL max-rate on the US cable interface, use the **show pxf cpu statistics drlmax-rate** command as shown in the following examples:

```
Router#show pxf cpu statistics drl max-rate us-cable
Load for five secs: 44%/4%; one minute: 45%; five minutes: 28%
Time source is hardware calendar, 16:52:36.953 CST Thu Dec 17 2015

Divert-Rate-Limit max-rate US-cable statistics
   dropped   divert_code
 No max-rate US-cable drops.
```

Clearing Statistics

Use **clear** commands to do the tasks listed in the table:

Command	Description
clear pxf statistics drl all	To clear all the entries in all the DRL statistics table
clear pxf statistics drl us-cable	To clear all the entries in the US-cable statistics table
clear pxf statistics drl ipv4	To clear all the entries in the WAN IPv4 statistics table
clear pxf statistics drl ipv6	To clear all the entries in the WAN IPv4 statistics table
clear pxf statistics drl non-ip	To clear all the entries in the WAN non-IP statistics table
clear pxf statistics drl max-rate	Clears the DRL max-rate statistics on the WAN interface

Note Starting from Cisco IOS Release 12.2(33)SCJ, only the **clear pxf statistics drl all** command is supported.

Configuration Examples for PXF DRL Enhancement

This section provides the following configuration examples:

Example: Configuring Cable Divert Rate Limit

The following example shows how to configure a cable DRL.

```
Router(config)# interface C5/0/0
Router(config-if)#cable divert-rate-limit rate 1 limit 4
```

Example: Configuring WAN IPv4 Rate and Limit

The following example shows how to configure a WAN-IPv4 rate and limit.

```
service divert-rate-limit
service divert-rate-limit ip
service divert-rate-limit ip fib_rp_glean
service divert-rate-limit ip fib_rp_glean rate
service divert-rate-limit ip fib_rp_glean rate 65530
service divert-rate-limit ip fib_rp_glean rate 65530 limit
service divert-rate-limit ip fib_rp_glean rate 65530 limit 4194
```

Example: Configuring WAN IPv6 Rate and Limit

The following example shows how to configure a WAN-IPv6 rate and limit.

```
service divert-rate-limit
service divert-rate-limit ipv6
service divert-rate-limit ipv6 ipv6_rp_glean
service divert-rate-limit ipv6 ipv6_rp_glean rate
service divert-rate-limit ipv6 ipv6_rp_glean rate 20
service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit
service divert-rate-limit ipv6 ipv6_rp_glean rate 20 limit 10
```

Example: Configuring WAN Non-IP Rate and Limit

The following example shows how to configure a WAN Non-IP rate and limit.

```
service divert-rate-limit
service divert-rate-limit non-ip
service divert-rate-limit non-ip cgmp
service divert-rate-limit non-ip cgmp rate
service divert-rate-limit non-ip cgmp rate 65535
service divert-rate-limit non-ip cgmp rate 65535 limit
service divert-rate-limit non-ip cgmp rate 65535 limit 4100
```

Example: Configuring an IPv4 Trusted Site

The following example shows how to configure an IPv4 trusted site.

```
service divert-rate-limit trusted-site 64.12.13.0 255.255.0.255
  tos 0xD0 mask 0xF3
```

Example: Configuring an IPv6 Trusted Site

The following example shows how to configure a IPv6 trusted site.

```
service divert-rate-limit trusted-site-ipv6 2001:420:3800:800:21F:29FF::1/128 traffic-class
 0x3 mask 0xFF global
```

Example: Configuring DRL Max-Rate Per Divert-Code on WAN Interface

The following example shows how to configure DRL max-rate per divert-code on WAN interface

```
Router> enable
Router# configure terminal
Router(config)# service  divert-rate-limit max-rate wan fib_rp_dest rate 5000 limit 100
Router(config)# end
```

Example: Configuring DRL Max-Rate Per Divert-Code on US Cable Interface

The following example shows how to configure DRL max-rate per divert-code on upstream cable interface.

```
Router> enable
Router# configure terminal
Router(config)# service divert-rate-limit max-rate us-cable fib_rp_dest rate 5000 limit 100
Router(config)# end
```

Additional References

The following sections provide references related to the PXF Divert Rate Limit Enhancement feature.

Related Documents

Related Topic	Document Title
CMTS cable commands	Cisco IOS CMTS Cable Command Reference
Cable ARP Filtering	Cisco IOS CMTS Cable Software Configuration Guide

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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
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

Feature Information for PXF DRL Enhancement

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

Note The below 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.

Table 2: Feature Information for PXF DRL Enhancement

Feature Name	Releases	Feature Information
PXF DRL Enhancement on the Cisco CMTS Routers	12.2(33)SCB	The PXF DRL Enhancement feature prevents congestion of the FP-to-RP interface by identifying and rate-limiting entities that would otherwise cause congestion. The following sections provide information about this feature: The following commands were introduced or modified: cable divert-rate-limit, • **service serviceip** • **service servicenon-ip** • **service divert-rate-limit trusted-site** • **clear pxf statistics drl cable-wan-ip** • **show pxf cpu statistics**, **show pxf cpu drl-trusted-sites**

Feature Name	Releases	Feature Information
PxF Accelerated for IPv6 Forwarding	12.2(33)SCE	The PXF Accelerated for IPv6 Forwarding feature for the Cisco uBR10000 series router includes support for the following IPv6 features: • IPv6 Security and QoS ACLs • IPv6 over IPv4 Tunnels • IPv6 Packet Filter Groups • IPv6 QoS Classifiers • ToS Overwrite for IPv6 • IPv6 Source Verify • IPv6 Packet Intercept • IPv6 SAV The following commands were introduced: service divert-rate-limit trusted-site-ipv6, **service divert-rate-limit ipv6,** show pxf cpu statistics drl us-cable, show pxf cpu statistics drl ipv6, show pxf cpu statistics drl ipv4, and **show pxf cpu statistics drl non-ip**.
DDoS attack solution	12.2(33)SCH3	The DDOS attack solution feature helps reduce the CPU utilization when the DDos occurs. The following commands were introduced: • **service divert-rate-limit max-rate** • **clear pxf statistics drl max-rate** • **show pxf cpu statistics drlmax-rate**

Feature Name	Releases	Feature Information
IPv6 DRL Punt Codes	12.2(33)SCJ	The feature applies rate limit to traffic from upstream cable. The following commands were introduced: • **service divert-rate-limit max-rate us-cable** • **show pfx cpu statistics drl max-rate us-cable** • **clear pfx statistics drl all**