



Source-Based Rate Limit

The Source-Based Rate Limit (SBRL) feature prevents congestion of packets on the forwarding processor (FP) to the Route Processor (RP) interface, which can be caused by denial of service (DoS) attacks directed at the Cisco CMTS or by faulty hardware.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- [Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1](#)
- [Prerequisites for Source-Based Rate Limit, on page 2](#)
- [Restrictions for Source-Based Rate Limit, on page 2](#)
- [Information About Source-Based Rate Limit, on page 3](#)
- [How to Configure Source-Based Rate Limit, on page 3](#)
- [Verifying the Source-Based Rate Limit Configuration, on page 11](#)
- [Configuration Example for Source-Based Rate Limit, on page 15](#)
- [Conversion of Divert Rate Limit Configuration on the Cisco uBR10012 Router to SBRL Configuration on the Cisco cBR Series Routers, on page 16](#)
- [Additional References, on page 19](#)
- [Feature Information for Source-Based Rate Limit, on page 19](#)

Hardware Compatibility Matrix for the Cisco cBR Series Routers



Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	<p>Cisco IOS-XE Release 16.5.1 and Later Releases</p> <p>Cisco cBR-8 Supervisor:</p> <ul style="list-style-type: none"> • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC 	<p>Cisco IOS-XE Release 16.5.1 and Later Releases</p> <p>Cisco cBR-8 CCAP Line Cards:</p> <ul style="list-style-type: none"> • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R <p>Cisco cBR-8 Downstream PHY Modules:</p> <ul style="list-style-type: none"> • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD <p>Cisco cBR-8 Upstream PHY Modules:</p> <ul style="list-style-type: none"> • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for Source-Based Rate Limit

- You must configure Control-Plane Policing (CoPP) for WAN-side SBRL.

Restrictions for Source-Based Rate Limit

- WAN-IP and Subscriber MAC address entities are identified using a hash, and hash collisions can occur between two (or more) entities.
- On the WAN-side there is no special processing for hash collisions. Sources that hash-collide are rate-limited as if they are the same source.
- The QOS group 99 is reserved for SBRL and cannot be used for other class maps.

Information About Source-Based Rate Limit

Source-Based Rate Limit (SBRL) feature operates on the punt path in CPP. SBRL identifies and rate-limits the packet streams that can overload the punt path or RP.

Punted packets are sent from the FP to the RP through the FP-to-RP queues. Denial of service (DoS) can occur when:

- The FP-to-RP queues are congested
- The RP cannot process punted packets fast enough

In both cases, the valid punted packets are not processed properly. These situations can be caused deliberately by DoS attacks or by faulty external hardware.

Packet streams identified by SBRL are rate-limited according to configured parameters. Rate-limiting occurs in CPP before the packets reach the FP-to-RP queues. This protects the RP, and also allows other valid punted packets to reach the RP.

SBRL has a separate configuration for the WAN-side and the subscriber-side. WAN-side SBRL is disabled by default. Subscriber-side SBRL has default settings.

WAN-Side Source-Based Rate Limit

WAN-side SBRL uses Control Plane Policing (CoPP). CoPP specifies the WAN-side packet streams that are directed for SBRL. Both trusted and untrusted sites can be specified using CoPP. Using CoPP, you can specify unlimited trusted sites. Access control list (ACL) is used to specify the trusted sites.

WAN-side SBRL also supports the quarantine functionality. When a packet stream enters quarantine, all punts from the packet stream are dropped for the configured period.

Subscriber-Side Source-Based Rate Limit

All subscriber-side punts are processed by subscriber-side SBRL. Note that the CoPP processes all punted packets, but there is no dependency between CoPP and subscriber-side SBRL.



Note The default subscriber-side rate for cable-l3-mobility is 4 packets per second.

How to Configure Source-Based Rate Limit

This section contains the following:

Configuring WAN-Side Source-Based Rate Limit

You must enable WAN-side SBRL in two parts:

1. Configure Control Plane Policing (CoPP) to specify which packets are subject to SBRL.
2. Configure WAN-side SBRL to set the rate-limiting parameters for the specified punt-causes.

In the CoPP policy map, the special action **set qos-group 99** denotes that the packets matching a particular class are subject to WAN-side SBRL. This means that the QoS group 99 is globally reserved for SBRL, and must not be used in other policy-maps.

Packets matching a class without **set qos-group 99** bypass WAN-side SBRL. This means that CoPP is also used to specify trusted traffic streams that are not subject to WAN-side SBRL.

All punted packets are subject to CoPP. So, you must ensure that subscriber-side traffic does not match a trusted class.

WAN-side SBRL identifies traffic streams by hashing the punt cause, VRF index, and source IP address. This value is used as the index for rate-limiting. The router does not perform special processing for hash collisions, so hash-colliding streams are treated as if they are from the same stream.

By default, WAN-side SBRL is disabled.

Restrictions

- All the punted packets are subject to CoPP and punt-policing.

This section contains the following:

Configuring Control Plane Policing

Punted packets matching the trusted class bypass WAN-side SBRL. The rest of the WAN-side punts are sent to WAN-side SBRL.



Note The following example shows a simple trusted class.

Procedure

	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	access-list <i>access-list-number</i> permit <i>protocol</i> { any host { <i>address</i> <i>name</i> }} { any host { <i>address</i> <i>name</i> }} tos <i>tos</i> Example: Router (config)# access-list 130 permit ip 192.168.1.10 0.0.0.0 192.168.1.11 0.0.0.0 tos 4	Configures an access list for filtering frames by protocol type. Note Since all the punted packets are subject to CoPP, you must ensure that subscriber-side traffic does not match a trusted class.
Step 4	class-map <i>class-map-name</i> Example:	Creates a class-map and enters QoS class-map configuration mode.

	Command or Action	Purpose
	<code>Router(config)# class-map match-all sbrl_v4_trusted</code>	
Step 5	match access-group <i>access-list-index</i> Example: <code>Router(config-cmap)# match access-group 130</code>	Specifies access groups to apply to an identity policy. The range of is from 1 to 2799.
Step 6	exit Example: <code>Router(config-cmap)# exit</code>	Exits QoS class-map configuration mode and returns to global configuration mode.
Step 7	policy-map <i>policy-map-name</i> Example: <code>Router(config)# policy-map copp_policy</code>	Specifies a service policy and enters QoS policy-map configuration mode.
Step 8	class <i>class-map-name</i> Example: <code>Router(config)# class sbrl_v4_trusted</code>	Enters QoS policy-map class configuration mode.
Step 9	police rate <i>units</i> pps conform-action <i>action</i> exceed-action <i>action</i> Example: <code>Router(config-pmap-c)# police rate 1000 pps conform-action transmit exceed-action transmit</code>	Polices traffic destined for the control plane at a specified rate. Note The rate is irrelevant if both the configured actions are transmit .
Step 10	exit Example: <code>Router(config-pmap-c)# exit</code>	Exits policy-map class police configuration mode
Step 11	class class-default Example: <code>Router(config-pmap)# class class-default</code>	Specifies the action to take on the packets that do not match any other class in the policy map.
Step 12	set qos-group <i>99</i> Example: <code>Router(config-pmap-c)# set qos-group 99</code>	Enables WAN-side SBRL for the packets that match this class.
Step 13	exit Example: <code>Router(config-pmap-c)# exit</code>	Exits policy-map class configuration mode
Step 14	exit Example: <code>Router(config-pmap)# exit</code>	Exits policy-map configuration mode

	Command or Action	Purpose
Step 15	control-plane [host transit cef-exception] Example: Router(config)# control-plane	Associates or modifies attributes (such as a service policy) that are associated with the control plane of the router and enters control plane configuration mode.
Step 16	service-policy {input output} <i>policy-map-name</i> Example: Router(config-cp)# service-policy input copp_policy	Attaches a policy map to a control plane.
Step 17	end Example: Router(config-cp)# end	Exits control plane configuration mode and returns to privileged EXEC mode.

Enabling WAN-Side Source-Based Rate Limit

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password, if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	platform punt-sbri wan punt-cause <i>punt-cause rate-per-1-sec rate</i> Example: Router(config)# platform punt-sbri wan punt-cause 10 rate-per-1-sec 4	Configures WAN-side rate limit. <ul style="list-style-type: none"> • punt-cause <i>punt-cause</i>—Specifies the punt-cause value in number 1 to 107 or string. • rate-per-1-sec <i>rate</i>—Specifies the rate in packets per second. The range is from 1 to 256, specified in powers-of-2.

Configuring WAN-Side Quarantine

The WAN-side quarantine extends the WAN-side SBRL configuration. When a traffic stream enters quarantine, all punted packets in the stream are dropped for the configured period.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password, if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	platform punt-sbri wan punt-cause <i>punt-cause rate-per-1-sec rate</i> quarantine-time time burst-factor <i>burst-factor</i> Example: Router(config)# platform punt-sbri wan punt-cause 10 rate-per-1-sec 4 quarantine-time 10 burst-factor 500	Configures quarantine for the WAN-side packet stream. <ul style="list-style-type: none"> • punt-cause <i>punt-cause</i>—Specifies the punt-cause value in number 1 to 107 or string. • rate-per-1-sec <i>rate</i>—Specifies the rate limit in packets per second. The range is from 1 to 256, specified in powers-of-2. • quarantine-time <i>time</i>—Specifies the quarantine time, in minutes. The range is from 1 to 60. • burst-factor <i>burst-factor</i>—Specifies the burst-factor, in number of packets. The range is from 50 to 1000.

Example

When (*burst-factor x rate*) packets arrive at a rate faster than *rate*, the packet stream enters quarantine.

For example, during a DoS attack, when the following occurs:

- Punted packets from a WAN-side source arrive at 100 packets per second.
- WAN-side SBRL is configured with a rate of 4 packets per second, quarantine time of 10 minutes, and burst-factor of 500 packets.

The packet rate is significantly higher than the configured rate. Therefore, when 2000 (4 x 500) packets have arrived, the packet stream enters into quarantine. Quarantine is activated at 20 seconds (2000 packets per 100 packets per second), and all punted packets from the stream are dropped for 10 minutes. After 10 minutes, the quarantine is deactivated.

The quarantine calculations restart immediately. So, if the scanning attack is continuous, quarantine is reactivated after the next 20 seconds.

Configuring Subscriber-Side Source-Based Rate Limit

This section contains the following:

Configuring Subscriber-Cable Modem Source-Based Rate Limit

Subscriber-cable modem SBRL identifies traffic streams by using the slot, MAC domain, and Service ID (SID) associated with the packet (that is, *slot/MD/SID*). All punts from this *slot/MD/SID* are aggregated and rate-limited as configured.

Before you begin

Restrictions

- All the punted packets are subject to CoPP and punt-policing.
- Layer 3 mobility punts are not subject to subscriber-cable modem SBRL. Layer 3 mobility punts are subject to the subscriber-MAC address SBRL.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password, if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	platform punt-sbri subscriber rate rate Example: Router(config)# platform punt-sbri subscriber rate 4	Configures subscriber-cable modem rate in packets per second. The range is from 1 to 256, specified in powers-of-2.

Configuring Subscriber-MAC Address Source-Based Rate Limit

Subscriber-MAC address SBRL identifies traffic streams by hashing the punt cause and the source MAC address. The hash value is used as the index for rate-limiting. Hash-collision detection is performed so that all traffic streams are processed separately.

The default rate for cable-l3-mobility is 4 packets/second. There are no other default settings. Using the 'no' configuration returns the rate to the default value.

The rate is specified in packets-per-4-seconds, and is restricted to powers-of-2 between 1 and 256. This rate allows a packet/second rate in the range [0.25, 0.50, 1, 2, 4, 8, 16, 32, 64]. The "no-drop" keyword disables rate-limiting for the specified punt-cause.

There is an optional quarantine configuration. When a traffic stream enters quarantine, all punted packets in the stream are dropped for the configured period. A traffic stream enters quarantine when (burst-factor x rate)

packets arrive at a rate factor than *rate*. An example would be that of a faulty cable modem that continuously sends DHCPv6 solicits.

- DHCPv6 solicits from the faulty cable modem arrive at 100 packets/second, and are all punted.
- Subscriber-side SBRL is configured with a rate-per-4-sec of 8 (i.e. 2 packets-per-sec), quarantine time of 10 minutes, and burst-factor of 500 packets.

The traffic stream rate is higher than the configured rate. Therefore, when approximately 1000 (2 x 500) packets have arrived, the traffic stream enters quarantine. The quarantine happens after about 10 seconds (1000 packets at 100 packets per second), and all punted packets from the stream are dropped for 10 minutes. After 10 minutes, the quarantine is deactivated. The quarantine calculations restart immediately, so if the traffic stream remains continuous, quarantine is reactivated after the next 10 seconds.

Before you begin

Restrictions

- All punted packets are subject to CoPP and punt-policing.
- The ARP-filter handles the subscriber-side ARP packets. The ARP packets are not processed at the subscriber-side SBRL.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password, if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	platform punt-sbri subscriber punt-cause <i>punt-cause</i> rate-per-4-sec <i>rate</i> [quarantine-time <i>time</i> burst-factor <i>burst-factor</i>]	Configures subscriber-MAC address SBRL. <ul style="list-style-type: none"> • punt-cause <i>punt-cause</i> - Specifies the punt cause. • rate-per-4-sec <i>rate</i> - Specifies the rate in packets per 4-seconds. The range is from 1 to 256, specified in powers-of-2. • quarantine-time <i>time</i> - Specifies the quarantine time, in minutes. The range is from 1 to 60. • burst-factor <i>burst-factor</i> - Specifies the burst-factor, in number of packets. The range is from 50 to 1000.

Configuring Source-Based Rate Limit Ping-Bypass

Follow the steps below to configure source-based rate limit ping-bypass.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password, if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	platform punt-sbri ping-bypass Example: Router(config)# platform punt-sbri ping-bypass	Configures source-based rate limit ping-bypass.

Configuring Punt Policing

The punt policer aggregates all packets (both subscriber-side and WAN-side) with the specified punt cause, and rate-limits them according to the configured parameters.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password, if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	platform punt-policer <i>punt-cause punt-rate</i> [high] Example: Router(config)# platform punt-policer 1 10	Configures punt policing. <ul style="list-style-type: none"> • <i>punt-cause</i>—Punt cause. The range is from 1 to 107. • <i>punt-rate</i>—Rate limit in packets per second. The range is from 10 to 146484. • high—(Optional) Specifies that the punt policing is performed only for high priority traffic.

Verifying the Source-Based Rate Limit Configuration

- **show running-config | include punt-sbri**—Displays the SBRL configuration.

There is no specific command to display the SBRL configuration. It must be piped from the running-config. To see the default configurations, use **show running-config all**.

Following is a sample output of the command:

```
Router# show running-config | include punt-sbri

platform punt-sbri wan punt-cause for-us-data rate-per-1-sec 8
platform punt-sbri wan punt-cause glean-adj rate-per-1-sec 4 quarantine-time 10
burst-factor 1000
platform punt-sbri subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 8
platform punt-sbri subscriber punt-cause sv-match-unknown rate-per-4-sec 8 quarantine-time
  5 burst-factor 500

. . .
```

- **show access-lists** —Displays the access list information for verifying CoPP configuration.

Following is a sample output of the command:

```
Router# show access-lists

Extended IP access list 120
  10 permit ip any any dscp af31
  20 permit ip any any dscp cs2
  30 permit ip any any dscp af21
  40 permit ip 68.86.0.0 0.1.255.255 any
IPv6 access list TRUSTEDV6
  permit ipv6 2001:558::/32 any sequence 10
```

- **show policy-map *policy-map-name***—Displays the information for the policy map.

Following is a sample output of the command:

```
Router# show policy-map copp_policy

Policy Map copp_policy
Class sbri_trusted
  police rate 1000 pps
    conform-action transmit
    exceed-action transmit
Class class-default
  set qos-group 99
```

- **show policy-map control-plane**—Displays the control plane policy map information.

Following is a sample output of the command:

```
Router# show policy-map control-plane

Control Plane

Service-policy input: copp_policy

Class-map: sbri_trusted (match-any)
  0 packets, 0 bytes
```

```

5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group 120
Match: access-group name TRUSTEDV6
police:
  rate 1000 pps, burst 244 packets
  conformed 0 packets, 0 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    transmit
  conformed 0 pps, exceeded 0 pps

Class-map: class-default (match-any)
  28 packets, 4364 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
QoS Set
  qos-group 99
  Marker statistics: Disabled

```

- **show platform hardware qfp active infrastructure punt sbrl**—Displays the SBRL statistics.

Following is a sample output of the command:

```
Router# show platform hardware qfp active infrastructure punt sbrl
```

```
SBRL statistics
```

```
Subscriber MAC-addr
  drop-cnt  evict-cnt  quar  MAC-Address      ID  punt-cause
-----
          10000      10000      0  0010.88a3.0456  101  cable-13-mobility
```

```
WAN-IPv4
  drop-cnt  evict-cnt  quar  VRF  cause  IP-address
-----
  456788    456788    0     0    050   1.2.0.66
```

```
WAN-IPv6
  drop-cnt  evict-cnt  quar  VRF  cause  IP-address
-----
  129334    129334    1     0    011   3046:1829:fefb::ddd1
    965      965      0     0    011   2001:420:2c7f:fc01::3
```

```
. . .
```



Note The value of *quar* is either 0 or 1. The value 1 indicates that quarantine is activated. The *quar* value is updated only when a packet from the source is dropped. If a source enters quarantine, and then stops sending packets, the *quar* value remains 1. However, the *drop-cnt* does not increment.



Note The SBRL statistics algorithm stores the data for the worst offenders. Sources that drop only a few packets are displayed in the table initially, but may be overwritten if the *drop-cnt* does not increase continuously. The *evict-cnt* increases in tandem with *drop-cnt*, but begins to decrease when a source is no longer being actively rate-limited. When the *evict-cnt* drops below 10, the record may be overwritten.

- **show platform hardware qfp active infrastructure punt statistics type global-drop**—Displays the global punt policer statistics.

Following is a sample output of the command:

```
Router# show platform hardware qfp active infrastructure punt statistics type global-drop
```

```
Global Drop Statistics
```

```
Number of global drop counters = 22
```

Counter ID	Drop Counter Name	Packets
000	INVALID_COUNTER_SELECTED	0
001	INIT_PUNT_INVALID_PUNT_MODE	0
002	INIT_PUNT_INVALID_PUNT_CAUSE	0
003	INIT_PUNT_INVALID_INJECT_CAUSE	0
004	INIT_PUNT_MISSING_FEATURE_HDR_CALLBACK	0
005	INIT_PUNT_EXT_PATH_VECTOR_REQUIRED	0
006	INIT_PUNT_EXT_PATH_VECTOR_NOT_SUPPORTED	0
007	INIT_INJ_INVALID_INJECT_CAUSE	0
008	INIT_INJ_MISSING_FEATURE_HDR_CALLBACK	0
009	PUNT_INVALID_PUNT_CAUSE	0
010	PUNT_INVALID_COMMON_HDR_VERSION	0
011	PUNT_INVALID_PLATFORM_HDR_VERSION	0
012	PUNT_PATH_NOT_INITIALIZED	0
013	PUNT_GPM_ALLOC_FAILURE	0
014	PUNT_TRANSITION_FAILURE	0
015	PUNT_DELAYED_PUNT_PKT_SB_NOT_IN_USE	0
016	PUNT_CAUSE_GLOBAL_POLICER	0
017	INJ_INVALID_INJECT_CAUSE	0
018	INJ_INVALID_COMMON_HDR_VERSION	0
019	INJ_INVALID_PLATFORM_HDR_VERSION	0
020	INJ_INVALID_PAL_HDR_FORMAT	0
021	PUNT_GPM_TX_LEN_EXCEED	0

- **show platform hardware qfp active infrastructure punt summary [threshold threshold-value]**—Displays the punt path rate-limiting summary.

Following is a sample output of the command:

```
Router# show platform hardware qfp active infrastructure punt summary
```

```
Punt Path Rate-Limiting summary statistics
```

Subscriber-side						
ID	punt cause	CPP punt	CoPP	ARPFilt/SBRL	per-cause	global
017	IPv6 Bad hop limit	22	0	0	0	0
050	IPv6 packet	13	0	0	0	0
080	CM not online	335	0	0	0	0

Verifying the Source-Based Rate Limit Configuration

```
WAN-side
```

ID	punt cause	CPP punt	CoPP	SBRL	per-cause	global
017	IPv6 Bad hop limit	471	0	0	0	0
018	IPV6 Hop-by-hop Options	29901	0	0	1430	0
024	Glean adjacency	111	0	0	0	0
025	Mcast PIM signaling	19	0	0	0	0
050	IPv6 packet	11	0	0	0	0

- **show platform software punt-policer**—Displays the punt policer configuration and statistics.

Following is a sample output of the command:

```
Router# show platform software punt-policer
```

```
Per Punt-Cause Policer Configuration and Packet Counters
```

Punt Cause	Description	Configured (pps)		Conform Packets		Dropped Packets	
		Normal	High	Normal	High	Normal	High
2	IPv4 Options	4000	3000	0	0	0	0
3	Layer2 control and legacy	40000	10000	16038	0	0	0
4	PPP Control	2000	1000	0	0	0	0
5	CLNS IS-IS Control	2000	1000	0	0	0	0
6	HDLc keepalives	2000	1000	0	0	0	0
7	ARP request or response	2000	1000	0	49165	0	0
8	Reverse ARP request or re...	2000	1000	0	0	0	0
9	Frame-relay LMI Control	2000	1000	0	0	0	0
10	Incomplete adjacency	2000	1000	0	0	0	0
11	For-us data	40000	5000	279977	0	0	0
12	Mcast Directly Connected ...	2000	1000	0	0	0	0

- **show platform hardware qfp active infrastructure punt policer summary**—Displays the punt policer summary.

Following is a sample output of the command:

```
Router# show platform hardware qfp active infrastructure punt policer summary
```

```
QFP Punt Policer Config Summary
```

Policer Handle	Rate (pps)	PeakRate (pps)	ConformBurst (pps)	ExceedBurst (pps)	Scaling Factor
001	300000	0	2288	2288	0
002	4000	0	4000	0	0
003	3000	0	3000	0	0
004	40000	0	40000	0	0
005	10000	0	10000	0	0
006	2000	0	2000	0	0
007	1000	0	1000	0	0
008	2000	0	2000	0	0
009	1000	0	1000	0	0
010	2000	0	2000	0	0
011	1000	0	1000	0	0
012	2000	0	2000	0	0
013	1000	0	1000	0	0
014	2000	0	2000	0	0

Configuration Example for Source-Based Rate Limit

Example: WAN-Side SBRL Configuration

```
access-list 120 permit ip any any dscp af31
access-list 120 permit ip any any dscp cs2
access-list 120 permit ip any any dscp af21
access-list 120 permit ip 192.168.1.10 0.1.255.255 any

ipv6 access-list TRUSTEDV6
  permit ipv6 any any dscp af31
  permit ipv6 any any dscp cs2
  permit ipv6 any any dscp af21
  permit ipv6 2001:558::/32 any

class-map match-all sbrl_trusted_v4
  match access-group 120

class-map match-all sbrl_trusted_v6
  match access-group name TRUSTEDV6

policy-map copp_policy
  ! IPv4 trusted:
  !   Specified rate is irrelevant.
  !   No special action; these packets bypass WAN-side SBRL.
  class sbrl_trusted_v4
    police rate 1000 pps conform transmit exceed transmit
  ! IPv6 trusted:
  !   Specified rate is irrelevant.
  !   No special action; these packets bypass WAN-side SBRL.
  class sbrl_trusted_v6
    police rate 1000 pps conform transmit exceed transmit

  ! add other classes here, if necessary

  ! Special action to activate WAN-side SBRL for this class.
  class class-default
    set qos-group 99

control-plane
  service-policy input copp_policy

platform punt-sbri wan punt-cause for-us-data rate-per-1-sec 4
platform punt-sbri wan punt-cause glean-adj rate-per-1-sec 4 quarantine-time 10 burst-factor
1000
```

Example: Subscriber-Side SBRL Configuration

```
platform punt-sbri subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 8
platform punt-sbri subscriber punt-cause sv-match-unknown rate-per-4-sec 8 quarantine-time
5 burst-factor 500
```

Conversion of Divert Rate Limit Configuration on the Cisco uBR10012 Router to SBRL Configuration on the Cisco cBR Series Routers

Divert Rate Limit Configuration on the Cisco uBR10012 Router

The following is a sample Divert Rate Limit (DRL) configuration on the Cisco uBR10012 router:

```

service divert-rate-limit ip fib_rp_glean rate 4 limit 4
service divert-rate-limit ip fib_rp_dest rate 4 limit 4
service divert-rate-limit ip fib_rp_punt rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_dest rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_punt rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_glean rate 4 limit 4
service divert-rate-limit ipv6 icmpv6 rate 4 limit 4

service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x68 mask 0xFF
service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x40 mask 0xFF
service divert-rate-limit trusted-site 68.86.0.0 255.254.0.0 tos 0x0 mask 0x0
service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x48 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x40 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x48 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x68 mask 0xFF
service divert-rate-limit trusted-site-ipv6 2001:558::/32 traffic-class 0x0 mask 0x0

interface Cabledx/y/z
  cable divert-rate-limit rate 4 limit 30

```

In Cisco IOS Release 12.2(33)SCH2, the **divert-rate-limit max-rate wan** command was introduced on the Cisco uBR10012 router. This configuration limits the aggregate rate of diverted packets on the WAN-side, on a per-divert-code basis. The following is the recommended best-practice configuration for the **divert-rate-limit max-rate wan** command:

```

service divert-rate-limit max-rate wan fib_rp_glean rate 5000
service divert-rate-limit max-rate wan fib_rp_punt rate 5000
service divert-rate-limit max-rate wan fib_rp_dest rate 40000

service divert-rate-limit max-rate wan ipv6_fib_glean rate 5000
service divert-rate-limit max-rate wan ipv6_fib_punt rate 5000
service divert-rate-limit max-rate wan ipv6_fib_dest rate 40000

```

SBRL Configuration on the Cisco cBR Series Routers

The DRL functionality is called as Source-Based Rate Limit (SBRL) on the Cisco cBR Series Routers. The punt-path has three layers of protection:

- [CoPP, on page 17](#)
- [SBRL, on page 17](#)
- [Punt Policer, on page 18](#)

CoPP

CoPP is used to specify the trusted sites and activate WAN-side SBRL. However, since CoPP applies to all punted packets, you must ensure that cable-side punts do not match the trusted sites.

The following is a sample CoPP configuration, which is equivalent to the configuration on the Cisco uBR10012 router:

```
access-list 120 permit ip any any dscp af31
access-list 120 permit ip any any dscp cs2
access-list 120 permit ip any any dscp af21
access-list 120 permit ip 68.86.0.0 0.1.255.255 any

ipv6 access-list TRUSTEDV6
  permit ipv6 any any dscp af31
  permit ipv6 any any dscp cs2
  permit ipv6 any any dscp af21
  permit ipv6 2001:558::/32 any

class-map match-all sbrl_trusted_v4
  match access-group 120

class-map match-all sbrl_trusted_v6
  match access-group name TRUSTEDV6

policy-map copp_policy
  class sbrl_trusted_v4
    police rate 1000 pps conform transmit exceed transmit
  class sbrl_trusted_v6
    police rate 1000 pps conform transmit exceed transmit
  class class-default
    set qos-group 99

control-plane
  service-policy input copp_policy
```



-
- Note**
- The **set qos-group 99** command activates SBRL for the specified class.
 - The police rate for **sbrl_trusted_vx** is irrelevant, as both actions are set to **transmit**.
 - You can add other trusted sites, as necessary.
-

SBRL

The following subscriber-side SBRL configuration is recommended. This configuration covers the expected subscriber-side punt-causes.

```
platform punt-sbri subscriber punt-cause for-us-data rate-per-4-sec 32
platform punt-sbri subscriber punt-cause for-us-ctrl rate-per-4-sec 8
platform punt-sbri subscriber punt-cause sv-match-unknown rate-per-4-sec 4
platform punt-sbri subscriber punt-cause cable-pre-reg rate-per-4-sec 8
platform punt-sbri subscriber punt-cause cable-dhcp rate-per-4-sec 8
platform punt-sbri subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 8
platform punt-sbri subscriber punt-cause cbl-dhcpv6-req rate-per-4-sec 8
```

For WAN-side SBRL, the Cisco cBR Series routers do not have separate IPv4 and IPv6 configurations as the punt causes are shared between IPv4 and IPv6. The *limit* cannot be configured as the hardware policer is used. Therefore, we recommend that you configure a higher *rate* initially. In the following sample configuration, *glean-adj* and *for-us-data* correspond to **x_rp_glean** and **x_rp_dest**, respectively on the Cisco uBR 10012 router.

```
platform punt-sbri wan punt-cause for-us-data rate 8
platform punt-sbri wan punt-cause glean-adj rate 8
```



Note

- The *fib-punt* punt cause is used in the Cisco uBR10012 router for packets destined to the management Ethernet. This punt cause is not used on the Cisco cBR Series routers.
- The Cisco cBR Series routers do not have an equivalent punt cause for ICMPV6. In the Cisco uBR10012 routers, ICMPv6 packets must be processed by the Route Processor to generate the checksum. In the Cisco cBR Series routers, ICMPv6 is processed in the control-plane. However, ICMPv6 punts can be identified and rate-limited (in aggregate) using CoPP.

Punt Policer

The punt policer operates on all punt causes and is fully configurable. The punt policer is not divided into WAN-side and subscriber-side. All packets with a given punt cause are aggregated and rate-limited as configured.

Following are the default settings (best-practice configuration) for the punt policer on the Cisco cBR Series routers:

punt-cause	LO	HI
CPP_PUNT_CAUSE_GLEAN_ADJ	2000	5000
CPP_PUNT_CAUSE_FOR_US	40000	5000



Note

- The equivalent punt cause for *fib-glean* (on the Cisco uBR10012 router) is *GLEAN_ADJ/HI* on the Cisco cBR Series routers.
- The equivalent punt cause for *fib-dest* (on the Cisco uBR10012 router) is *FOR_US/LO* on the Cisco cBR Series routers.

Additional References

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>	http://www.cisco.com/support

Feature Information for Source-Based Rate Limit

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.



Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for Source-Based Rate Limit

Feature Name	Releases	Feature Information
Source-based rate limit	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.

