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.

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.

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

- 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 3
- 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 Examples for Source-Based Rate Limit, on page 15
- Default SBRL Configuration, on page 18
- Conversion of SBRL Subscriber-side Configuration from 16.8.x to 16.9.x, on page 18
- Conversion of Divert Rate Limit Configuration on the Cisco uBR10012 Router to SBRL Configuration on the Cisco cBR Series Routers, on page 19
- Additional References, on page 22
- Feature Information for Source-Based Rate Limit, on page 22

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	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • 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 • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Note Do not use DPICs (8X10G and 2x100G) to forward IP traffic, as it may cause buffer exhaustion, leading to line card reload.

The only allowed traffic on a DPICs DEPI, UEPI, and GCP traffic from the Cisco cBR-8 router to Remote PHY devices. Other traffic such as DHCP, SSH, and UTSC should flow via another router, since DPICs cannot be used for normal routing.

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.

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.

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** *access-list-number* **permit** *protocol* {**any** | **host** {*address* | *name*}} {**any** | **host** {*address* | *name*}} **tos** *tos*	Configures an access list for filtering frames by protocol type.

	Command or Action	Purpose
	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`	**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** *class-map-name* **Example:** `Router(config)# class-map match-all sbrl_v4_trusted`	Creates a class-map and enters QoS class-map configuration mode.
Step 5	**match access-group** *access-list-index* **Example:** `Router(config-cmap)# match access-group 130`	Specifies access groups to apply to an identity policy. The range of is from 1 to 2799.
Step 6	**exit** **Example:** `Router(config-cmap)# exit`	Exits QoS class-map configuration mode and returns to global configuration mode.
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map copp_policy`	Specifies a service policy and enters QoS policy-map configuration mode.
Step 8	**class** *class-map-name* **Example:** `Router(config)# class sbrl_v4_trusted`	Enters QoS policy-map class configuration mode.
Step 9	**police rate** *units* **pps conform-action** *action* **exceed-action** *action* **Example:** `Router(config-pmap-c)# police rate 1000 pps conform-action transmit exceed-action transmit`	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:** `Router(config-pmap-c)# exit`	Exits policy-map class police configuration mode
Step 11	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Specifies the action to take on the packets that do not match any other class in the policy map.
Step 12	**set qos-group 99** **Example:** `Router(config-pmap-c)# set qos-group 99`	Enables WAN-side SBRL for the packets that match this class.
Step 13	**exit** **Example:**	Exits policy-map class configuration mode

	Command or Action	Purpose
	`Router(config-pmap-c)# exit`	
Step 14	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode
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**} *policy-map-name* **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. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**platform punt-sbrl wan punt-cause** *punt-cause* **rate-per-1-sec** *rate* **Example:** `Router(config)# platform punt-sbrl wan punt-cause 10 rate-per-1-sec 4`	Configures WAN-side rate limit. • **punt-cause** *punt-cause*—Specifies the punt-cause value in number 1 to 107 or string. • **rate-per-1-sec** *rate*—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. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**platform punt-sbrl wan punt-cause** *punt-cause* **rate-per-1-sec** *rate* **quarantine-time** *time* **burst-factor** *burst-factor* **Example:** `Router(config)# platform punt-sbrl wan punt-cause 10 rate-per-1-sec 4 quarantine-time 10 burst-factor 500`	Configures quarantine for the WAN-side packet stream. • **punt-cause** *punt-cause*—Specifies the punt-cause value in number 1 to 107 or string. • **rate-per-1-sec** *rate*—Specifies the rate limit in packets per second. The range is from 1 to 256, specified in powers-of-2. • **quarantine-time** *time*—Specifies the quarantine time, in minutes. The range is from 1 to 60. • **burst-factor** *burst-factor*—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 are 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

Restrictions

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

- The ARP-filter handles the subscriber-side ARP packets. ARP packets are not processed by subscriber-side SBRL.
- The maximum rate is 255. Due to this, the configured rate of 256 from 16.8.X will not transfer properly. A new command must be entered to transfer the configuration.

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.

Default settings for subscriber-side SBRL are listed in this topic. Using the 'no' configuration returns the rate to the default value.

Rate-limiting is performed using a 2-color token-bucket algorithm. The rate is specified in packets-per-4-seconds, in the range [1, 255]. This translates to a packets-per-second rate in the range [0.25, ~64]. The optional bucket-size is specified in packets, in the range [1, 255]. If not specified, then bucket-size is set equal to rate.

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 faster 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.

1. **enable**

   ```
   Router> enable
   ```

   Enables privileged EXEC mode. Enter your password, if prompted.

2. **configure terminal**

   ```
   Router# configure terminal
   ```

   Enters global configuration mode.

3. **platform punt-sbrl subscriber punt-cause***punt-cause***rate-per-4-sec** *rate* [**bucket-size***bucket-size*] [**quarantine-time***time***burst-factor***burst-factor*]

   Configures subscriber-MAC address SBRL.

   - **punt-cause** *punt-cause* - Specifies the punt cause.
   - **rate-per-4-sec** *rate* - Specifies the rate in packets per 4-seconds. The range is from 1 to 255.
   - **bucket-size***bucket-size* – Specifies the bucket-size in packets. The range is from 1 to 255. If bucket-size is not entered, the bucket-size is set equal to the rate.

- **quarantine-time** *time*– Specifies the quarantine time, in minutes. The range is from 1 to 60.
- **burst-factor** *burst-factor*– 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. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**platform punt-sbrl ping-bypass** **Example:** `Router(config)# platform punt-sbrl ping-bypass`	Configures source-based rate limit ping-bypass.

Configuring SNMP RX Queuing

Table 2: Feature History

Feature Name	Release Information	Feature Description
SNMP RX queuing	Cisco IOS XE Bengaluru 17.6.1a	This feature introduces a control plane policing queue to shape incoming SNMP traffic in Cisco cBR-8 routers. It reduces the need for SNMP poller to retransmit the polling request in case the request is dropped when SNMP traffic overloads the queue.

Spike in SNMP traffic leads to drops in punt-path-rate-limiting (PPRL). Cisco IOS XE Bengaluru 17.6.1a release introduces a control plane policing queue to shape incoming SNMP traffic. It reduces the need for SNMP poller to retransmit the polling request in case the request is dropped when SNMP traffic overloads the queue.

This feature is disabled by default. Use the following command to configure this feature:

cable rxq snmp rate *packets-per-second* **qlimit** *packets* [**avg-pkt-size** *bytes*]

For example:

```
Router(config)#cable rxq snmp rate 1024 qlimit 8192 avg-pkt-size 1500
Router(config)#end
```

The SNMP packet rate range is 64–1024 packet/second. The queue limit range is 64–8192 packets. The average packet size range is 95–1500 bytes, default size is 128 bytes.

Note The RXQ rate must be smaller than the punt-policer rate, so that RXQ handles the rate-limiting of SNMP packets.

When you update the RXQ parameters, the existing queue must be empty. It results in delay before the new queue parameters take effect.

To verify the SNMP RX queuing configuration, use the **show** command as shown in the following examples:

```
Router#show platform hardware qfp active feature docsis rxq idx 1
Idx  Uidb          Qid           Rate(Kbps)  Qlmt(Byte)
1 0x0003ed92    0x0000b3a0    12288       12288000

Router#show plat hard qfp active infra bqs queue output default interface-string RXQ0
Interface: RXQ0 QFP: 0.0 if_h: 4718 Num Queues/Schedules: 1
  Queue specifics:
    Index 0 (Queue ID:0xb3a0, Name: )
    Software Control Info:
      (cache) queue id: 0x0000b3a0, wred: 0x52783200, qlimit (bytes): 12288000
      parent_sid: 0x29e23, debug_name:
      sw_flags: 0x48000011, sw_state: 0x00000801, port_uidb: 257426
      orig_min  : 0                   ,      min: 1228800
      min_qos   : 0                   , min_dflt: 0
      orig_max  : 0                   ,      max: 0
      max_qos   : 0                   , max_dflt: 0
      share     : 1
      plevel    : 0, priority: 65535
      defer_obj_refcnt: 0, cp_ppe_addr: 0x00000000
    Statistics:
      tail drops  (bytes): 115203800           ,          (packets): 525349
      total enqs  (bytes): 208955400           ,          (packets): 1131326
      queue_depth (bytes): 0
      licensed throughput oversubscription drops:
                  (bytes): 0                   ,          (packets): 0
```

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. • Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**platform punt-policer** {**cable-snmp** | *punt-cause* }*punt-rate* [**high**] **Example:** `Router(config)# platform punt-policer 1 10`	Configures punt policing. • *punt-cause*—Specifies the punt cause value. • **cable-snmp**—This is the punt-cause assigned to SNMP packets destined to the CMTS. • *punt-rate*—Specifies the rate in packets/second. The range is from 10 to 300000. • **high**—(Optional) Specifies that the punt policing is performed only for high priority traffic.

Verifying the Source-Based Rate Limit Configuration

- **show cable dp sbrl config**—Displays the SBRL configuration, including default settings. This is equivalent to **show running-config all | include punt-sbrl**.

  Following is a sample output of the command:

```
Router# show cable dp sbrl config
platform punt-sbrl wan punt-cause for-us-data rate-per-1-sec 8
platform punt-sbrl wan punt-cause glean-adj rate-per-1-sec 4 quarantine-time 10
burst-factor 1000
platform punt-sbrl subscriber punt-cause for-us-data rate-per-4-sec 32 bucket-size 32
platform punt-sbrl subscriber punt-cause for-us-ctrl rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cable-l3-mobility rate-per-4-sec 16 bucket-size
 16
platform punt-sbrl subscriber punt-cause sv-match-unknown rate-per-4-sec 4 bucket-size
 4
platform punt-sbrl subscriber punt-cause cable-pre-reg rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 8 bucket-size
 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-req rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-sub rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv4-sub rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv4-disc-req rate-per-4-sec 8 bucket-size
 8
```

- **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 sbrl_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: sbrl_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-l3-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.

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-str         CPP-punt   CoPP   ARPfilt-SBRL   RXQ-ARPauto   punt-pol   global   to-RP
-------------------------------------------------------------------------------------------------
157  cable-snmp                49320      0          0          23154          0        0      26166
135  cbl-dhcpv4-disc-req          29      0          0              0          0        0          9
119  cbl-dhcpv6-req                2      0          0              0          0        0          2
118  cbl-dhcpv6-solicit           13      0          0              0          0        0         13
103  cable-pre-reg                 4      0          0              0          0        0          4
055  for-us-ctrl                  27      0          0              0          0        0         27
011  for-us-data                  10      0          0              0          0        0         10
010  incomplete-adj               22      0          0              0          0        0         22

WAN-side
ID   punt-cause-str         CPP-punt   CoPP   SBRL   RXQ   punt-pol   global   to-RP
-------------------------------------------------------------------------------------------
168  cable-snmp-rxq           26166       0      0     0       0        0          0
107  cable-dhcp                  44       0      0     0       0        0         44
056  for-us-internal-ctrl         1       0      0     0       0        0          1
055  for-us-ctrl                418       0      0     0       0        0        418
021  diag                       310       0      0     0       0        0        310
011  for-us-data                 69       0      0     0       0        0         69
010  incomplete-adj              23       0      0     0       0        0         23
007  arp                          1       0      0     0       0        0          1
003  unknown-encap              369       0      0     0       0        0        369
```

- **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                              Configured (pps) Conform Packets   Dropped Packets
Cause Description                 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  Rate     PeakRate   ConformBurst  ExceedBurst   Scaling
Handle   (pps)    (pps)      (pps)         (pps)         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 Examples for Source-Based Rate Limit

The following sample configurations are examples for Source-Based Rate Limit Configuration.

Example: Subscriber-Side SBRL Configuration

```
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 2 bucket-size 8
platform punt-sbrl subscriber punt-cause sv-match-unknown rate-per-4-sec 4 bucket-size 10
quarantine-time 5 burst-factor 500
```

WAN Side Source-Based Rate Limit

WAN-side SBRL is enabled through CoPP. CoPP is used to specify which WAN-side packet streams are directed to WAN-side SBRL, using the **set qos-group 99** command. This means that in cBR-8, **qos-group 99** is globally reserved for SBRL, and cannot be otherwise used.

In the examples below, WAN-side punts matchingthe trusted classes bypass WAN-side SBRL. WAN-side punts that end up in the **default-class** are sent to WAN-side SBRL.

Configuring Control Plane Policing for Releases Before Cisco IOS XE Cupertino 17.9.1w

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

Example 2: WAN-Side SBRL Configuration

The following example shows a simple CoPP configuration which sends traffic to WAN-side SBRL, and also demonstrates how trusted and untrusted traffic is specified. CoPP applies to all punted packets, so it is necessary to ensure that the trusted/untrusted configuration does not interfere with cable-side packets.

Note All ACLs used by CoPP should be configured to 'permit' packets, even for packet streams that are untrusted.

```
! trusted packets
access-list 120 permit ip 192.168.1.10 0.0.0.0 any tos 2

! untrusted packets
access-list 130 permit ip 192.168.1.10 0 0 0 0 any tos 4

class-map match-any SBRL_TRUSTED
  match access-group 120
```

```
class-map match-any SBRL_UNTRUSTED
  match access-group 130

policy-map COPP_POLICY
  class SBRL_TRUSTED
    ! the specified rate is irrelevant
    ! no special action, so these packets bypass SBRL
    police rate 1000 pps conform transmit exceed transmit

  class SBRL_UNTRUSTED
    ! the specified rate is irrelevant
    ! these packets are all dropped
    police rate 1000 pps conform drop exceed drop

  << other classes, if necessary >>

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

control-plane
  service-policy input COPP_POLICY
```

Configuring Control Plane Policing for Cisco IOS XE Cupertino 17.9.1w and Later

Starting with Cisco IOS XE Cupertino 17.9.1w, the **punt-path** is modified to set **qos-group** in context to **99** for **subscriber-side punts**, which is the qos-group that is reserved for SBRL.

This allows configuration of a class-map in CoPP to identify subscriber-side punts. Subscriber-side punts can effectively 'bypass' CoPP. The CoPP policy can then be simplified, because it does not interfere with subscriber-side punts. All subscriber-side punts are still subject to subscriber-side SBRL, so there is no security issue. The previous example is modified, and shown below:

```
! trusted packets
access-list 120 permit ip 192.168.1.10 0.0.0.0 any tos 2

! untrusted packets
access-list 130 permit ip 192.168.1.10 0 0 0 0 any tos 4

class-map match-any SBRL_TRUSTED
  match access-group 120

class-map match-any SBRL_UNTRUSTED
  match access-group 130

class-map match-any SUBSCRIBER_SIDE
  match qos-group 99

policy-map COPP_POLICY
  class SUBSCRIBER_SIDE
    ! the specified rate is irrelevant
    ! these packets go to subscriber-side SBRL
    police rate 1000 pps conform-action transmit exceed-action transmit

  class SBRL_TRUSTED
    ! the specified rate is irrelevant
    ! no special action, so these packets bypass SBRL
    police rate 1000 pps conform transmit exceed transmit

  class SBRL_UNTRUSTED
    ! the specified rate is irrelevant
    ! these packets are all dropped
    police rate 1000 pps conform drop exceed drop
```

```
  << other classes, if necessary >>

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

control-plane
  service-policy input COPP_POLICY
```

Default SBRL Configuration

Because of the dependency on CoPP, WAN-side SBRL is disabled by default. There is no default WAN-side SBRL configuration.

Subscriber-side SBRL has the following default settings:

```
platform punt-sbrl subscriber punt-cause for-us-data rate-per-4-sec 32 bucket-size 32
platform punt-sbrl subscriber punt-cause for-us-ctrl rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cable-l3-mobility rate-per-4-sec 16 bucket-size
16
platform punt-sbrl subscriber punt-cause sv-match-unknown rate-per-4-sec 4 bucket-size 4
platform punt-sbrl subscriber punt-cause cable-pre-reg rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-solicit rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-req rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv6-sub rate-per-4-sec 8 bucket-size 8
platform punt-sbrl subscriber punt-cause cbl-dhcpv4-disc-req rate-per-4-sec 8 bucket-size
8
platform punt-sbrl subscriber punt-cause cbl-dhcpv4-sub rate-per-4-sec 8 bucket-size 8
```

Conversion of SBRL Subscriber-side Configuration from 16.8.x to 16.9.x

In 16.9.x, several new punt-causes were added for DHCP packets on the subscriber-side. This means that the recommended configuration for 16.8.x does not match up with the default configuration in 16.9.x.

In 16.8.x, the cable-dhcp punt-cause is used by both subscriber-side and WAN-side DHCP punts. In 16.9.x, new punt-causes were added on the subscriber-side for DHCP packets, with the result that the cable-dhcp punt-cause is used ONLY for WAN-side DHCP punts. This means that configuring a rate for cable-dhcp on the subscriber-side is meaningless. The chart below shows the DHCP-related punt-causes for 16.8.x and 16.9.x. In 16.9.x, all the subscriber-side DHCP punt-causes have default SBRL settings.

Table 3: 16.8.x

punt-cause	Origin	Description
cbl-dhcpv6-solicit	sub	DHCPv6 solicit
cbl-dhcpv6-req	sub	DHCPv6 request
cable-dhcp	sub/WAN	all other DHCP packets

Table 4: 16.9.x

punt-cause	Origin	Description
cbl-dhcpv6-solicit	sub	DHCPv6 solicit
cbl-dhcpv6-req	sub	DHCPv6 request
cbl-dhcpv6-sub	sub	all other (sub-side) DHCPv6 packets
cbl-dhcpv4-disc-req	sub	DHCPv4 discover & request
cbl-dhcpv4-sub	sub	all other (sub-side) DHCPv4 packets
cable-dhcp	WAN	all (WAN-side) DHCP packets

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 Cablex/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 20
- SBRL, on page 21
- Punt Policer, on page 21

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

The recommended subscriber-side SBRL configuration is the default configuration. All expected subscriber-side punt-causes have default settings.

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-sbrl wan punt-cause for-us-data rate 8
platform punt-sbrl 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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	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 https://cfnng.cisco.com/ 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 5: 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 theCisco cBR Series Converged Broadband Routers.
Source-based rate limit	Cisco IOS XE Gibraltar 16.12.1z1	A new punt cause **cable-snmp** was added to rate-limit the SNMP packets destined to the CMTS.