送信元ベースのレート制限

送信元ベースのレート制限（SBRL）機能は、Cisco CMTS に向けられたサービス妨害（DoS）攻撃やハードウェア障害によって発生する可能性がある、フォワーディング プロセッサ（FP）上のパケットのルート プロセッサ（RP）インターフェイスへの輻輳を防止します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

• 送信元ベースのレート制限に関する機能情報，20 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *1*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

送信元ベースのレート制限の前提条件

- WAN 側 SBRL のコントロール プレーン ポリシング（CoPP）を設定する必要があります。

送信元ベースのレート制限の制限事項

- WAN-IP および加入者の MAC アドレスのエンティティはハッシュを使用して識別され、2 つ（またはそれ以上の）エンティティ間でハッシュ衝突が発生する可能性があります。
- Cisco cBR ルータはハッシュ衝突に対し特別な処理を実行しません。ハッシュ衝突が発生する送信元は、それらが同じ送信元であるかのように、レート制限されています。
- QOS グループ 99 は SBRL 用に予約されており、他のクラス マップには使用できません。

送信元ベースのレート制限に関する情報

送信元ベースのレート制限（SBRL）機能は、CPP のパント パスで動作します。SBRL は、パント パスまたは RP でオーバーロードになる可能性のあるパケット ストリームを識別してレート制限を実施します。

パントされたパケットは、FP - RP キュー経由で FP から RP に送信されます。サービス妨害（DoS）は次の状況で発生する可能性があります。

- FP - RP キューが輻輳している
- RP がパントされたパケットを十分高速に処理できない

いずれの状況でも、有効なパントされたパケットが適切に処理されません。このような状況は、DoS 攻撃または外部ハードウェア障害によって意図的に発生する可能性があります。

SBRL で特定されたパケット ストリームは、設定されたパラメータに従ってレート制限されます。FP - RP キューにパケットが到達する前に、CPP でレート制限が発生します。これによって RP が保護され、他の有効なパントされたパケットが RP に到達できます。

デフォルトでは、SBRL は Cisco cBR ルータで無効です。SBRL には、WAN 側と加入者側で別々の設定があります。

WAN 側送信元ベースのレート制限

WAN 側 SBRL は、コントロール プレーン ポリシング（CoPP）を使用します。CoPP は、SBRL 宛の WAN 側パケット ストリームを指定します。信頼済みサイトと非信頼サイトの両方を CoPP を使用して指定できます。CoPP を使用すると、信頼済みサイトを無制限に指定できます。信頼済みサイトを指定するには、アクセス コントロール リスト（ACL）を使用します。

WAN 側 SBRL は、隔離機能もサポートします。パケット ストリームが隔離に入ると、パケット ストリームのすべてのパントが設定した期間にわたってドロップされます。

加入者側送信元ベースのレート制限

加入者側 SBRL 設定はグローバルであり、各ケーブル インターフェイスで設定する必要はありません。Cisco cBR ルータは、レイヤ 3 モビリティの原因単位の加入者側設定もサポートします。

（注） レイヤ 3 モビリティのデフォルトの加入者側原因単位レートは 4 パケット/秒です。加入者側原因単位レートは変更できますが、無効にできません。

送信元ベースのレート制限の設定方法

この項の構成は、次のとおりです。

WAN 側送信元ベースのレート制限の設定

次の 2 つの設定で、WAN 側 SBRL をイネーブルにする必要があります。

1. どのパケットを SBRL の対象にするかを指定するために、コントロール プレーン ポリシング（CoPP）を設定します。
2. 指定したパント要因に対するレート制限パラメータを設定するために、WAN 側 SBRL を設定します。

CoPP ポリシー マップでの特殊なアクション **set qos-group 99** は、特定のクラスに一致するパケットが WAN 側 SBRL の対象であることを表します。これは、QoS グループ 99 が SBRL 用にグローバルに確保されており、他のポリシー マップには使用できないことを意味します。

set qos-group 99 を含まないクラスにマッチするパケットは、WAN 側 SBRL をバイパスします。これは、CoPP は、WAN 側 SBRL の対象とならない信頼済みトラフィック ストリームを指定するためにも使用できることを意味します。

すべてのパントされたパケットは CoPP の対象となります。したがって、加入者側のトラフィックが信頼済みクラスに一致しないことを確認する必要があります。

WAN 側 SBRL は、パント要因、VRF インデックス、および送信元 IP アドレスをハッシュすることにより、トラフィック ストリームを特定します。この値は、レート制限のインデックスとして使用されます。ルータはハッシュ衝突に対して特別な処理を実行しないため、ハッシュ衝突をしているストリームは同じストリームからのものとして処理されます。

デフォルトでは、WAN 側 SBRL はディセーブルになっています。

制限事項

- パントされたすべてのパケットは、CoPP とパント ポリシングの対象です。

この項の構成は、次のとおりです。

コントロール プレーン ポリシングの設定

信頼済みクラスと一致するパントされたパケットは、WAN 側の SBRL を回避します。WAN 側の残りのパントは、WAN 側の SBRL に送信されます。

（注） 次に、信頼済みクラスの簡単な例を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number***permit** *protocol* {**any** | **host** {*address* | *name*}} {**any** | **host** {*address* | *name*}} **tos** *tos* 例： `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`	プロトコル タイプを基準にフレームをフィルタリングするためのアクセス リストを設定します。 （注） すべてのパントされたパケットは CoPP の対象となるため、加入者側のトラフィックが信頼済みクラスと同じでないことを確認する必要があります。
ステップ 4	**class-map** *class-map-name* 例： `Router(config)# class-map match-all sbrl_v4_trusted`	クラスマップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 5	**match access-group** *access-list-index* 例： `Router(config-cmap)# match access-group 130`	アイデンティティ ポリシーを適用するアクセス グループを指定します。その範囲は 1 ～ 2799 です。
ステップ 6	**exit** 例： `Router(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**policy-map** *policy-map-name* 例： `Router(config)# policy-map copp_policy`	サービスポリシーを指定し、QoSポリシーマップ コンフィギュレーション モードを開始します。
ステップ 8	**class** *class-map-name* 例： `Router(config)# class sbrl_v4_trusted`	QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**police rate** *units***pps conform-action** *action* **exceed-action** *action* 例： `Router(config-pmap-c)# police rate 1000 pps conform-action transmit exceed-action transmit`	コントロール プレーン宛てのトラフィックを指定のレートでポリシングします。 （注） 設定したアクションを両方とも**送信**する場合は、レートは関係ありません。
ステップ 10	**exit** 例： `Router(config-pmap-c)# exit`	ポリシー マップ クラス ポリシング コンフィギュレーション モードを終了します。
ステップ 11	**class class-default** 例： `Router(config-pmap)# class class-default`	ポリシー マップ内の他のどのクラスとも一致しないパケットに実行するアクションを指定します。
ステップ 12	**set qos-group 99** 例： `Router(config-pmap-c)# set qos-group 99`	このクラスに一致するパケットの WAN 側の SBRL を有効にします。
ステップ 13	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 14	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 15	**control-plane** [**host** | **transit** | **cef-exception**] 例： `Router(config)# control-plane`	ルータのコントロール プレーンに属性（サービス ポリシーなど）を関連付けるか、関連付けられている属性を変更し、コントロール プレーン コンフィギュレーション モードを開始します。

ステップ 16	**service-policy** {**input** |**output**出力ポリシー マップ名前
	
	例：
	`Router(config-cp)#`
	`service-policy input copp_policy`
		ポリシー マップをコントロール プレーンに関連付けます。

ステップ 17	**end** 例： `Router(config-cp)# end`	コントロール プレーン コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

WAN 側の送信元ベースのレート制限の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**platform punt-sbrl wan punt-cause** *punt-cause* **rate** *rate* 例： `Router(config)# platform punt-sbrl wan punt-cause 10 rate 4`	WAN 側のレート制限を設定します。 • **punt-cause** *punt-cause*：パント要因を指定します。範囲は 1 ～ 107 です。 • **rate** *rate*：1 秒間のパケット数でレートを指定します。範囲は 2 の累乗で指定される 1 ～ 256 です。

WAN 側の隔離の設定

WAN 側の隔離により、WAN 側の SBRL 設定が拡張されます。トラフィック ストリームが隔離に入ると、ストリーム内のパントされたすべてのパケットが設定した期間にわたってドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**platform punt-sbrl wan punt-cause** *punt-cause* **rate** *rate* **quarantine-time** *time* **burst-factor** *burst-factor* 例： `Router(config)# platform punt-sbrl wan punt-cause 10 rate 4 quarantine-time 10 burst-factor 500`	WAN 側のパケット ストリームの隔離を設定します。 • **punt-cause** *punt-cause*：パント要因を指定します。範囲は 1 ～ 107 です。 • **rate** *rate*：レート制限を毎秒のパケット数単位で指定します。範囲は 2 の累乗で指定される 1 ～ 256 です。 • **quarantine-time** *time*：隔離時間（分単位）を指定します。指定できる範囲は 1 ～ 60 です。 • **burst-factor** *burst-factor*：バースト係数をパケット数単位で指定します。範囲は 50 ～ 1000 です。

パケット（*burst-factor* x *rate*）が *rate* よりも高速なレートで届く場合は、そのパケット ストリームは隔離されます。

たとえば、DoS 攻撃では次のようになります。

- WAN 側の送信元からパントされたパケットは、毎秒 100 パケットで到着します。
- WAN 側の SBRL は、毎秒 4 パケットのレート、隔離時間 10 分、バースト係数 500 パケットで設定されています。

パケット レートは、設定したレートよりもかなり高く設定されています。そのため、2000（4 x 500）パケットが到着したら、パケット ストリームが隔離されます。隔離は 20 秒間（毎秒 100 パケットごとに 2000 パケット）で有効になり、ストリームからパントされたパケットは 10 分間ドロップされます。10 分後、隔離は無効になります。

隔離の計算はすぐに再開します。したがって、スキャン攻撃が継続すると、次の20秒後には隔離が再び有効になります。

加入者側送信元ベースのレート制限の設定

この項の構成は、次のとおりです。

加入者ケーブル モデムの送信元ベースのレート制限の設定

加入者ケーブル モデムの SBRL では、パケットに関連するスロット、MAC ドメイン、サービス ID（つまり、*slot/MD/SID*）を使用して、トラフィック ストリームを特定します。この *slot/MD/SID* のすべてのパントは集約され、設定のとおりにレート制限されています。

はじめる前に

制限事項

- パントされたすべてのパケットは、CoPP とパント ポリシングの対象です。
- レイヤ 3 モビリティのパントは、加入者ケーブル モデムの SBRL の対象ではありません。レイヤ 3 モビリティのパントは、加入者 MAC アドレスの SBRL の対象です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**platform punt-sbrl subscriber rate** *rate* 例： `Router(config)# platform punt-sbrl subscriber rate 4`	毎秒のパケット数で加入者ケーブル モデム レートを設定します。範囲は 1 ～ 256 で、2 のべき乗で示します。

加入者 MAC アドレスの送信元ベースのレート制限の設定

加入者 MAC アドレス SBRL では、パント要因と送信元 MAC アドレスのハッシュ値でトラフィック ストリームを識別します。この値は、レート制限のインデックスとして使用されます。Cisco cBR ルータはハッシュ衝突に対し特別な処理を実行しません。そのため、ハッシュ衝突パケット ストリームは同じパケット ストリームからのようにレート制限されます。

レイヤ 3 モビリティ パントのデフォルトのレートは 4 パケット/秒です。

はじめる前に

制限事項

- パントされたすべてのパケットは、CoPP とパント ポリシングの対象です。
- 加入者 MAC アドレス SBRL は、加入者側のレイヤ 3 モビリティ パントにのみ適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**platform punt-sbrl subscriber punt-cause** *punt-cause* **rate** *rate* 例： `Router(config)# platform punt-sbrl subscriber punt-cause 99 rate 2`	加入者 MAC アドレス SBRL を設定します。 • **punt-cause** *punt-cause*：パント要因を指定します。レイヤ 3 モビリティのパント要因は 99 です。 • **rate** *rate*：レート制限を毎秒のパケット数単位で指定します。範囲は 2 の累乗で指定される 1 ～ 256 です。

送信元ベースのレート制限 ping バイパスの設定

送信元ベースのレート制限 ping バイパスを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**platform punt-sbrl ping-bypass** 例： `Router(config)# platform punt-sbrl ping-bypass`	送信元ベースのレート制限 ping バイパスを設定します。

パント ポリシングの設定

パント ポリサーが、指定したパント要因ですべてのパケット（加入者側と WAN 側の両方）を収集し、設定したパラメータに従ってパケットをレート制限します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**platform punt-policer** *punt-cause punt-rate* [**high**] 例： `Router(config)# platform punt-policer 1 10`	パント ポリシングを設定します。 • *punt-cause*：パント要因。範囲は 1 ～ 107 です。 • *punt-rate*：レート制限を毎秒のパケット数で設定します。範囲は 10 ～ 146484 です。

	コマンドまたはアクション	目的
		• **high**：（任意）パントのポリシングが優先順位の高いトラフィックに対してのみ実行されるように指定します。

送信元ベースのレート制限設定の確認

- **show running-config | include punt-sbrl**：SBRL 設定を表示します。

  次に、コマンドの出力例を示します。

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

platform punt-sbrl wan punt-cause 11 rate 8
platform punt-sbrl wan punt-cause 24 rate 4
platform punt-sbrl subscriber rate 8
```

- **show access-lists** ：CoPP 設定を確認するためのアクセス リスト情報を表示します。

  次に、コマンドの出力例を示します。

```
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*：ポリシー マップの情報を表示します。

  次に、コマンドの出力例を示します。

```
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**：コントロールプレーン ポリシーマップの情報を表示します。

  次に、コマンドの出力例を示します。

```
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**：SBRL 統計情報を表示します。

次に、コマンドの出力例を示します。

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

SBRL statistics

Subscriber CM
  drop-cnt  evict-cnt    SID  Interface
-------------------------------------------------
         1          1      5  Cable3/0/0
       982        982      5  Cable3/0/0

Subscriber MAC-addr
  nothing to report

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
```

（注） *quar* の値は 0 または 1 です。値が 1 の場合は、隔離が有効であることを示します。値 *quar* は、送信元からのパケットがドロップされた場合のみ更新されます。送信元が隔離され、パケットの送信が停止した場合、値 *quar* は 1 のままです。ただし、*drop-cnt* の値は増えません。

（注） SBRL統計アルゴリズムに最悪の攻撃者のデータが保存されます。いくつかのパケットのみがドロップされた送信元がまずテーブルに表示されますが、*drop-cnt* が増え続けないと上書きされる場合があります。*evict-cnt* は *drop-cnt* と連動して増えますが、送信元がアクティブにレート制限されなくなると減り始めます。*evict-cnt* が 10 未満になると、レコードが上書きされる場合があります。

- **show platform hardware qfp active infrastructure punt statistics type global-drop**：グローバル パント ポリサーの統計情報を表示します。

  次に、コマンドの出力例を示します。

```
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*]：パント パス レート制限の概要を表示します。

  次に、コマンドの出力例を示します。

```
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

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**：パント ポリサーの設定と統計情報を表示します。

  次に、コマンドの出力例を示します。

```
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**：パント ポリサーの概要を表示します。

  次に、コマンドの出力例を示します。

```
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
 . . .
```

送信元ベースのレート制限の設定例

例：WAN 側 SBRL の設定

```
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


! punt-cause 11 is FOR_US, punt-cause 24 is GLEAN_ADJ
platform punt-sbrl wan punt-cause 11 rate 4
platform punt-sbrl wan punt-cause 24 rate 4
```

例：加入者側の SBRL の設定

```
platform punt-sbrl subscriber rate 4
```

例：SBRL の設定

```
…
platform punt-sbrl wan punt-cause 11 rate 4
platform punt-sbrl wan punt-cause 18 rate 16 quarantine-time 10 burst-factor 500
platform punt-sbrl wan punt-cause 24 rate 4
platform punt-sbrl subscriber rate 4
…
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
…
policy-map copp_policy
class sbrl_trusted_v4
  police rate 1000 pps conform-action transmit  exceed-action transmit
 class sbrl_trusted_v6
  police rate 1000 pps conform-action transmit  exceed-action transmit
 class class-default
  set qos-group 99
…
control-plane
service-policy input copp_policy
…
```

Cisco uBR10012 ルータにおける転送レート制限の設定から Cisco cBR シリーズ ルータにおける SBRL 設定への変換

Cisco uBR10012 ルータにおける転送レート制限の設定

次に、Cisco uBR10012 ルータにおける転送レート制限（DRL）の設定例を示します。

```
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
```

Cisco IOS リリース 12.2(33)SCH2 では、**divert-rate-limit max-rate wan** コマンドが Cisco uBR10012 ルータに追加されました。この設定により、WAN 側の転送パケットの集約レートが転送コード単位で制限されます。 次に、**divert-rate-limit max-rate wan** コマンドで推奨されるベストプラクティスの設定を示します。

```
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
```

Cisco cBR シリーズ ルータにおける SBRL 設定

DRL 機能は、Cisco cBR シリーズ ルータでは送信元ベースのレート制限（SBRL）と呼ばれています。パント パスには 3 つの保護レイヤがあります。

- CoPP, （18 ページ）
- SBRL, （19 ページ）
- パント ポリサー, （19 ページ）

CoPP

CoPP は、信頼済みサイトの指定と WAN 側 SBRL の有効化に使用されます。ただし、CoPP はパントパケットすべてに適用されるため、ケーブル側のパントが信頼済みサイトと一致しないことを確認する必要があります。

次に、CoPP 設定の例を示します。これは、Cisco uBR10012 ルータでの設定と同じです。

```
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
```

（注）

- **set qos-group 99** コマンドを使用すると、指定したクラスの SBRL が有効化されます。
- 両方のアクションが **transmit** に設定されているため、**sbrl_trusted_v***x* のポリシー レートは無関係です。
- 必要に応じて、他の信頼済みサイトも追加できます。

SBRL

加入者側の SBRL 設定には、グローバル コンフィギュレーション モードの単一コマンドを使用します。ハードウェアのポリサーが使用されているため、制限は設定できません。そのため、最初に高いレートを設定することを推奨します。

Cisco cBR シリーズ ルータにおける WAN 側の SBRL では、パント要因が IPv4 と IPv6 の間で共有されるため、IPv4 と IPv6 の設定を分けられません。ハードウェアのポリサーが使用されているため、制限は設定できません。そのため、最初に高いレートを設定することを推奨します。次の設定例では、パント要因 24 は *Glean adjacency* を、パント要因 11 は *For-us data* を示しています。これらは、Cisco uBR10012 ルータの *x*_rp_glean と *x*_rp_dest にそれぞれ相当します。

```
platform punt-sbrl subscriber rate 16

platform punt-sbrl wan punt-cause 11 rate 8
platform punt-sbrl wan punt-cause 24 rate 8
```

（注）
- *fib-punt* パント要因は、管理イーサネット宛てのパケット用として Cisco uBR10012 ルータで使用されます。このパント要因は、Cisco cBR シリーズ ルータでは使用されません。
- Cisco cBR シリーズ ルータには、ICMPV6 のパント要因に相当するものがありません。Cisco uBR10012 ルータでは、ICMPv6 パケットをルート プロセッサで処理し、チェックサムを生成する必要があります。Cisco cBR シリーズ ルータでは、ICMPv6 をコントロール プレーンで処理します。ただし、CoPP を使用して、ICMPv6 パントを識別し、レート制限（アグリゲーション）することができます。

パント ポリサー

パント ポリサーは、すべてのパント要因に対して動作できるだけでなく、完全に設定可能です。また、WAN 側と加入者側で分けられてはいません。特定のパント要因を持つすべてのパケットが、設定通りに集約され、レート制限されます。

次に、Cisco cBR シリーズ ルータでのパント ポリサーのデフォルト設定（ベスト プラクティス設定）を示します。

```
punt-cause                      LO     HI

CPP_PUNT_CAUSE_GLEAN_ADJ        2000   5000
CPP_PUNT_CAUSE_FOR_US           40000  5000
```

（注）
- *fib-glean*（Cisco uBR10012 ルータ上）に相当するパント要因は、Cisco cBR シリーズ ルータでは *GLEAN_ADJ/HI* です。
- （Cisco uBR10012 ルータ上の）*fib-dest* に相当するパント要因は、Cisco cBR シリーズ ルータでは *FOR_US/LO* です。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

送信元ベースのレート制限に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *2*：送信元ベースのレート制限に関する機能情報

機能名	リリース	機能情報
送信元ベースのレート制限	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。