



Cisco NCS 560 シリーズルータ（IOS XR リリース 6.6.x）モジュ ラ QoS コンフィギュレーションガイド

初版：2019年5月31日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

パケット分類の概要 1

NCS 560 シリーズ ルータの制約事項 1

トラフィック クラスの要素 2

デフォルト トラフィック クラス 3

トラフィック クラスの作成 3

トラフィック ポリシーの要素 5

トラフィック ポリシーの作成 6

トラフィック ポリシーのインターフェイスへの適用 7

パケットのマーキング 9

出力方向での IP パケットの QoS 再マーキング 11

出力方向でのイーサネット パケットの QoS 再マーキング 11

バンドル トラフィック ポリシー 12

デュアル ポリシーマップを使用した QoS 出力マーキングとキューイング 12

制約事項 15

In-Place ポリシーの変更 17

モジュラ QoS サービス パケットの分類の参照 18

IP precedence によるパケットの CoS の指定 18

パケットの分類に使用する IP precedence ビット 18

IP precedence 値の設定 18

IP プレシデンス と IP DSCP マーキングの比較 19

QoS-group の使用とキューの選択 19

第 2 章

モジュラ QoS の輻輳回避 21

テール ドロップと FIFO キュー 21

テールドロップの設定	21
ランダム早期検出と TCP	23
ランダム早期検出の設定	23
Weighted Random Early Detection : 重み付けランダム早期検出	25
WRED の平均キュー サイズ	26
重み付けランダム早期検出の設定	26

第 3 章

輻輳管理の概要	29
Class-based Weighted Fair Queueing	29
残りの帯域幅	29
残存帯域幅の設定 : インスタンス 2	30
低遅延キューイングとストリクトプライオリティ キューイング	32
ストリクトプライオリティ キューイングによる低遅延キューイングの設定	32
トラフィック シェーピング	34
トラフィック シェーピングの設定	34
トラフィック ポリシング	36
認定バーストおよび超過バースト	37
シングルレート ポリサー	37
トラフィック ポリシングの設定 (シングルレート 2 カラー)	38
トラフィック ポリシングの設定 (シングルレート 3 カラー)	40
2 つのレートを使用したポリシング機能	42
トラフィック ポリシングの設定 (2 レート 3 カラー)	43
モジュラ QoS 輻輳管理のリファレンス	44
認定バースト	44
超過バースト	45
2 レート ポリサーの詳細	46

第 4 章

リンクバンドルの QoS	49
ロード バランシング	49
リンクバンドルでの QoS の設定	50

第 5 章	階層型モジュラ QoS の概要	55
	H-QoS 設定の制約事項	56
	階層型キューイングの設定	57



第 1 章

パケット分類の概要

パケットの分類には、特定のグループ（またはクラス）内のパケットを分類し、これにトラフィック記述子を割り当て、ネットワークで QoS 処理用にアクセスできるようにする処理が含まれます。トラフィック記述子には、パケットが受ける転送処理（Quality of Service）に関する情報が含まれます。パケット分類を使用すると、複数のプライオリティ レベルまたは CoS にネットワークトラフィックを区分できます。発信元が契約された条項に従うことに同意し、ネットワークが QoS の実行を約束します。トラフィック ポリサーとトラフィック シェーパーは、契約を順守するために、パケットのトラフィック記述子を使用します。

トラフィック ポリサーおよびトラフィック シェーパーは、IP precedence などのパケット分類機能を使用して、さまざまなタイプの QoS サービスに対して、ルータを通過するパケット（またはトラフィックフロー）を選択します。パケットを分類した後、他の QoS 機能を使用して、輻輳管理、帯域幅割り当て、および遅延限度などの適切なトラフィック処理ポリシーを、各トラフィック クラスに割り当てることができます。

モジュラ Quality of Service (QoS) コマンドラインインターフェイス (MQC) は、分類する必要があるトラフィックフローを定義するために使用します。このとき、各トラフィックフローをサービスクラス、またはクラスと呼びます。その後、トラフィック ポリシーを作成し、クラスに適用します。定義されたクラスに該当しないトラフィックはすべて、デフォルトクラスのカテゴリに分類されます。

- [NCS 560 シリーズ ルータの制約事項 \(1 ページ\)](#)
- [トラフィック クラスの要素 \(2 ページ\)](#)
- [トラフィック ポリシーの要素 \(5 ページ\)](#)
- [デュアル ポリシーマップを使用した QoS 出力マーキングとキューイング \(12 ページ\)](#)
- [制約事項 \(15 ページ\)](#)
- [In-Place ポリシーの変更 \(17 ページ\)](#)
- [モジュラ QoS サービス パケットの分類の参照 \(18 ページ\)](#)

NCS 560 シリーズ ルータの制約事項

- `hw-module profile qos ingress-model peering` コマンドはサポートされていません。
- 一致 ACL はサポートされていません。

トラフィック クラスの要素

トラフィック クラスの目的は、ルータのトラフィックを分類することです。 **class-map** コマンドを使用してトラフィック クラスを定義します。

トラフィック クラスには、3つの主要な要素が含まれています。

- 名前
- 一連の **match** コマンド：パケットを分類するためのさまざまな基準を指定します。
- これらの **match** コマンドを評価する方法の手順（トラフィック クラスに複数の **match** コマンドが存在する場合）

パケットは、**match** コマンドで指定された基準に合っているかどうかを判断するためにチェックされます。指定された基準に合っていれば、パケットはクラスのメンバーと見なされ、トラフィック ポリシーで設定された QoS 仕様に従って転送されます。一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。

次の表に、このルータでサポートされている一致タイプの詳細を示します。

サポートされている一致タイプ	最小、最大	エントリの最大数	一致 NOT のサポート	範囲のサポート	インターフェイスでサポートされる方向
IPv4 DSCP IPv6 DSCP DSCP	(0, 63)	64	あり	あり	入力
IPv4 Precedence IPv6 Precedence Precedence	(0, 7)	8	あり	なし	入力
MPLS Experimental Topmost	(0, 7)	8	あり	なし	入力
Access-group	N/A	8	なし	該当なし	入力
QoS-group	(1, 7)	7	なし	なし	出力
CoS	(0, 7)	8	なし	あり	入力
プロトコル	(0, 255)	1	あり	該当なし	入力



- (注) 出力キューの統計情報は、出力で対応する一致基準があるクラスにのみ表示されます。したがって、入力に **set qos-group x** を設定した場合、対応する **match qos-group x** を出力に設定して出力側で統計情報が表示されるようにする必要があります。また、[QoS-groupの使用とキューの選択 \(19 ページ\)](#) も参照してください。

デフォルトトラフィッククラス

未分類のトラフィック（トラフィッククラスで指定された一致条件を満たさないトラフィック）は、デフォルトトラフィッククラスに属するものとして扱われます。

ユーザがデフォルトクラスを設定しない場合でも、パケットはデフォルトクラスのメンバとして扱われます。ただし、デフォルトでは、デフォルトクラスにイネーブルな機能はありません。そのため、機能が設定されていないデフォルトクラスに属するパケットには QoS 機能は適用されません。この後、これらのパケットは、ファーストインファーストアウト（FIFO）キューに配置され、使用可能な下位リンクの帯域幅で決められたレートで転送されます。この FIFO キューは、テールドロップと呼ばれる輻輳回避技術で管理されます。

出力分類の場合、**qos-group** (1-7) での一致がサポートされています。**match qos-group 0** は設定できません。出力ポリシーの **class-default** は **qos-group 0** にマッピングします。

次に、デフォルトクラスにトラフィックポリシーを設定する例を示します。

```
configure
policy-map ingress_policy1
class class-default
  police rate percent 30
!
```

トラフィッククラスの作成

一致基準が含まれるトラフィッククラスを作成するには、**class-map** コマンドを使用してトラフィッククラス名を指定し、必要に応じて **match** コマンドをクラスマップコンフィギュレーションモードで使用します。

ガイドライン

- ユーザは、設定の単一行において一致タイプに対し複数の値を提供できます。つまり、最初の値が一致基準を満たさない場合は、一致ステートメントに示された次の値が分類のために検討されます。
- not** キーワードを **match** コマンドに使用すると、指定されていないフィールドの値に基づいて照合が実行されます。
- この設定作業で指定するすべての **match** コマンドの使用は任意ですが、1つのクラスに少なくとも1つの一致基準を設定する必要があります。

- **match-any** を指定した場合、トラフィック クラスで受信したトラフィックがトラフィック クラスの一部と分類されるには、一致基準の1つを満たす必要があります。これはデフォルトです。 **match-all** を指定した場合は、トラフィック がすべての一致基準を満たす必要があります。
- **match access-group** コマンドの場合は、IPv4 ヘッダーおよび IPv6 ヘッダーのパケット長または TTL (パケット 存続時間) フィールドに基づいた QoS 分類はサポートされません。
- **match access-group** コマンドの場合は、ACL リストがクラス マップ内で使用されると、ACL の拒否アクションは無視され、トラフィック は指定された ACL の一致パラメータに基づいて分類されます。
- **match qos-group**、**traffic-class**、および **discard-class** は出力方向でのみサポートされます。また、これらは出力方向でサポートされている唯一の一致基準です。
- 出力のデフォルト クラスは、暗黙的に **qos-group 0** に一致します。
- マルチキャストはルータ上のユニキャストとは異なるシステム パスを取得し、後でインターフェイスごとに 20:80 のマルチキャスト対ユニキャストの比率の出力を満たします。この比率は、トラフィック と同じ優先度レベルに維持されます。
- マルチキャスト トラフィック の出力 QoS はトラフィック クラス 0 ~ 5 は優先順位が低く、トラフィック クラス 6 ~ 7 は優先順位が高いものとして処理します。現在、ユーザはこれを設定できません。
- 出力シェーピングは、優先順位が高い (HP) トラフィック クラスでのマルチキャスト トラフィック には影響しません。ユニキャスト トラフィック にのみ、適用されます。
- 入力ポリシーでトラフィック クラスを設定しますが、対応するトラフィック クラス値の出力に一致クラスがない場合は、このクラスを持つ入力 of トラフィック は出力ポリシー マップのデフォルト クラスでは説明されません。
- トラフィック クラス 0 のみがデフォルト クラスに分類されます。入力に割り当てられていても、出力キューが割り当てられていないゼロ以外のトラフィック クラスは、デフォルト クラスにも、他のどのクラスにも分類されません。
- また、[QoS-group の使用とキューの選択 \(19 ページ\)](#) も参照してください。

設定例

トラフィック クラスの設定を完了するには、以下を完全に行う必要があります。

1. クラス マップの作成
2. パケットをその特定のクラスのメンバとして分類するための一致基準の指定
サポートされる一致タイプの一覧については、[トラフィック クラスの要素 \(2 ページ\)](#) を参照してください。

```
Router# configure
Router(config)# class-map match-any qos-1
```

```
Router(config-cmap)# match qos-group 1  
Router(config-cmap)# end-class-map  
Router(config-cmap)# commit
```

クラス マップ設定を確認するには、次のコマンドを使用します。

```
Router#show class-map qos-1  
1) ClassMap: qos-1    Type: qos  
   Referenced by 2 Policymaps
```

[実行コンフィギュレーション \(8 ページ\)](#) も参照してください。

[確認 \(9 ページ\)](#) も参照してください。

関連項目

- [トラフィック クラスの要素 \(2 ページ\)](#)
- [トラフィック ポリシーの要素 \(5 ページ\)](#)

関連コマンド

トラフィック ポリシーの要素

トラフィック ポリシーには、次の3つの要素が含まれています。

- 名前
- トラフィック クラス
- Quality of Service (QoS) ポリシー

トラフィック ポリシーにトラフィックを分類するのに使用するトラフィック クラスを選択した後で、ユーザはこの分類されたトラフィックに適用される QoS 機能を入力できます。

MQC では、必ずしも1つのトラフィック クラスだけを1つのトラフィック ポリシーに関連付ける必要はありません。

クラスをポリシーマップで設定する順序が重要です。クラスの一貫規則は、クラスをポリシーマップで指定した順序で TCAM にプログラミングされます。したがって、あるパケットが複数のクラスと一致する場合は、最初に一致したクラスだけが返され、対応するポリシーが適用されます。

ルータは、入力方向のポリシーマップごとに 32 のクラスを、出力方向のポリシーマップごとに 8 つのクラスをサポートしています。

次の表に、ルータでサポートされているクラスアクションを示します。

サポートされているアクションタイプ	インターフェイスでサポートされる方向
bandwidth-remaining	出力
mark	(パケットのマーキング (9 ページ) を参照)。
police	入力
priority	出力 (レベル 1~レベル 7)
shape	出力

WRED は、**default** オプションと **discard-class** オプションをサポートしています。discard-class に渡される値は 0 と 1 のみです。

トラフィック ポリシーの作成

トラフィック ポリシーの目的は、ユーザが指定したトラフィック クラスまたはクラスに分類されたトラフィックに関連付ける QoS 機能を設定することです。

トラフィック クラスを設定するには、[トラフィック クラスの作成 \(3 ページ\)](#) を参照してください。

policy-map コマンドを使用してトラフィック ポリシーを定義した後、インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用してこのポリシーを 1 つ以上のインターフェイスに付加し、これらのインターフェイスのトラフィック ポリシーを指定できます。デュアルポリシー サポートを使用すると、2 つのトラフィック ポリシーを使用できます (1 つはマーキング、もう 1 つは出力に付加されるキューイング)。[トラフィック ポリシーのインターフェイスへの適用 \(7 ページ\)](#) を参照してください。

設定例

トラフィック ポリシーの設定を完了するには、以下を完全に行う必要があります。

- 1 つまたは複数のインターフェイスに付加してサービス ポリシーを指定するためのポリシー マップの作成
- トラフィック クラスのトラフィック ポリシーへの関連付け
- クラス アクションの指定 ([トラフィック ポリシーの要素 \(5 ページ\)](#) を参照)

```
Router# configure
Router(config)# policy-map test-shape-1
Router(config-pmap)# class qos-1

/* Configure class-action ('shape' in this example).
Repeat as required, to specify other class-actions */
Router(config-pmap-c)# shape average percent 40
Router(config-pmap-c)# exit
```

```
/* Repeat class configuration as required, to specify other classes */  
  
Router(config-pmap) # end-policy-map  
Router(config) # commit
```

[実行コンフィギュレーション \(8 ページ\)](#) を参照してください。

[確認 \(9 ページ\)](#) を参照してください。

関連項目

- [トラフィック ポリシーの要素 \(5 ページ\)](#)
- [トラフィック クラスの要素 \(2 ページ\)](#)

関連コマンド

- [bandwidth](#)
- [bandwidth remaining](#)
- [class](#)
- [police](#)
- [policy-map](#)
- [priority](#)
- [queue-limit](#)
- [service-policy](#)
- [set discard-class](#)
- [set dscp](#)
- [set mpls experimental](#)
- [set precedence](#)
- [set qos-group](#)
- [shape](#)

トラフィック ポリシーのインターフェイスへの適用

トラフィック クラスおよびトラフィック ポリシーが作成された後、インターフェイスにトラフィック ポリシーを適用し、ポリシーの適用方向を指定する必要があります。



- (注) ポリシーマップをインターフェイスに適用すると、各クラスの転送速度のカウンタの精度が損なわれます。これは、転送速度のカウンタが指数関数的減衰フィルタに基づいて計算されるためです。

設定例

トラフィック ポリシーをインターフェイスに適用するには、以下を完了する必要があります。

1. トラフィック クラス、およびパケットをクラスに対応させる関連付けられたルールの作成（[トラフィック クラスの作成 \(3 ページ\)](#) を参照）
2. 1 つまたは複数のインターフェイスに適用してサービス ポリシーを指定するためのトラフィック ポリシーの作成（[トラフィック ポリシーの作成 \(6 ページ\)](#) を参照）
3. トラフィック クラスのトラフィック ポリシーへの関連付け
4. 入力または出力方向での、トラフィック ポリシーのインターフェイスへの適用

```
Router# configure
Router(config)#
Router(config-int)# service-policy output
Router(config-int)# commit
```

```
RP/0/RP0/CPU0:R1(config)# interface twentyFiveGigE 0/0/0/26.1
RP/0/RP0/CPU0:R1(config-if)# service-policy input cos
RP/0/RP0/CPU0:R1(config-if)# commit
```

実行コンフィギュレーション

```
RP/0/RP0/CPU0:R1# show run interface TwentyFiveGigE0/0/0/26.1
```

```
interface TwentyFiveGigE0/0/0/26.1 l2transport
encapsulation dot1q 25
service-policy input cos
!
```

```
RP/0/RP0/CPU0:R1# show run policy-map cos
```

```
policy-map cos
class cos1
police rate 3 mbps
!
!
class cos2
police rate 2 mbps
!
!
class cos3
police rate 3 mbps
!
!
class class-default
police rate 4 mbps
!
!
end-policy-map
!
```

```
RP/0/RP0/CPU0:R1#
```

確認

関連項目

- [トラフィック ポリシーの要素 \(5 ページ\)](#)
- [トラフィック クラスの要素 \(2 ページ\)](#)

関連コマンド

- [service-policy](#)

パケットのマーキング

パケットマーキング機能では、指定マーキングに基づいてパケットを区別する方法がユーザに提供されます。ルータは、出力パケット マーキングをサポートしています (discard-class で使用する場合のみ)。

また、ルータは L2 入力マーキングもサポートしています。

入力マーキングの場合：

入力トラフィック：入力 pop 操作では、カスタマー VLAN タグ (CoS、DEI) の再マーキングはサポートされていません。

出力トラフィック：入力「pop VLAN」は出力トラフィックの「push VLAN」に変換され、新たにプッシュされた VLAN タグで (CoS、DEI) マーキングがサポートされます。2つの VLAN タグが出力側のパケット ヘッダーにプッシュされる場合は、内部と外部の両方の VLAN タグがマークされます。次に例を示します。

1. rewrite ingress tag pop 1 symmetric
2. rewrite ingress tag pop 2 symmetric
3. rewrite ingress tag translate 2-to-1 dot1q/dot1ad <> symmetric

制限事項

出力マーキング ポリシーの統計情報とカウンタはルータ上では確認できません。

制限事項

出力マーキング ポリシーの統計情報とカウンタはルータ上では確認できません。

サポートされているパケット マーキング操作

次の表に、サポートされているパケット マーキング操作を示します。

サポートされているマーク タイプ	範囲	無条件マーキングのサポート	条件付きマーキングのサポート
set dscp	0 ~ 63	入力	なし

サポートされているマークタイプ	範囲	無条件マーキングのサポート	条件付きマーキングのサポート
set qos-group	0 ~ 7	入力	なし

クラスベースの無条件パケット マーキング

パケット マーキング機能により、次のようにネットワークを複数のプライオリティ レベルまたはサービス クラスに区切ることができます。

- QoS 無条件パケット マーキングを使用して、ネットワークに入るパケットの IP precedence または DSCP 値を設定します。ネットワーク内のルータは、新しくマーキングされた IP precedence 値を使用して、トラフィックの処理方法を決定できます。

入力方向で、IP Precedence または DSCP 値に基づいてトラフィックを照会した後、そのトラフィックを特定の discard-class に設定できます。それによって、輻輳回避技術である Weighted Random Early Detection (WRED; 重み付けランダム早期検出) は、discard-class 値を使用して、パケットがドロップされる可能性を判断します。

- QoS 無条件パケット マーキングを使用して、MPLS パケットを QoS グループに割り当てます。ルータは、QoS グループを使用して送信用のパケットのプライオリティを設定する方法を決定します。トラフィック クラス識別子を MPLS パケット上に設定するには、**set traffic-class** コマンドをポリシーマップクラス コンフィギュレーションモードで使用します。



(注) QoS グループ ID を設定しても、パケットを送信する優先順位が自動的に決まるわけではありません。最初に QoS グループを使用する出力ポリシーを設定する必要があります。

- CoS 無条件パケット マーキングを使用して、IEEE 802.1p/スイッチ間リンク (ISL) パケットのプライオリティ値を設定するパケットを割り当てます。ルータでは、CoS 値を使用して、パケットに転送のための優先順位を付ける方法を決定し、このマーキングを使用してレイヤ 2 からレイヤ 3 へのマッピングを行います。送信パケットのレイヤ 2 の CoS 値を設定するには、ポリシーマップ コンフィギュレーションモードで **set cos** コマンドを使用します。
- 802.1ad フレームの Drop Eligible Indicator (DEI) ビットに基づいてパケットをマークするには、QoS の無条件パケットマーキングを使用します。ドロップ適正インジケータ (DEI) 値を設定するには、**set dei** コマンドをポリシーマップクラス コンフィギュレーションモードで DEI 値を設定します。



(注) 特に明記されていないかぎり、レイヤ 3 物理インターフェイスのクラス単位の無条件パケット マーキングがバンドルインターフェイスに適用されます。

出力方向での IP パケットの QoS 再マーキング

ルータは出力方向におけるすべての IP パケットの IP DSCP ビットのゼロへのマーキングをサポートしています。この機能は、IP パケットの優先順位の再マーキングに役立ちます。これは主に IP over Ethernet over MPLS over GRE のようなシナリオで使用されます。この機能は、`class-default` 内に設定されている `set dscp 0` オプションがある入力ポリシーマップを使用して実行されます。

設定例

```
Router# configure
Router(config)# policy-map ingress-set-dscp-zero-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp 0
Router(config-pmap-c)# end-policy-map
Router(config-pmap)# commit
```

実行コンフィギュレーション

```
policy-map ingress-set-dscp-zero-policy
class class-default
  set dscp 0
!
end-policy-map
!
```

出力方向でのイーサネット パケットの QoS 再マーキング

ルータは、出力方向でのイーサネットパケットのレイヤ2マーキングをサポートしています。この機能を有効にするには、次の手順を実行する必要があります。

- 出力インターフェイスでのキューイングとマーキングのポリシー マップを設定します。
- 入力にトラフィッククラスを設定し、`match traffic-class` をキューイング用の出力で使用します。
- `set qos-group` コマンドが入力ポリシー内に設定されており、対応する `match qos-group` コマンドが出力マーキング ポリシー内に設定されていることを確認します。対応する QoS グループがない場合は、トラフィック障害が発生します。

入力「push VLAN」は、出力トラフィックの「pop VLAN」に変換されます。この場合、(CoS、DEI) 再マーキングは VLAN タグではサポートされません。次に例を示します。

1. `rewrite ingress tag push dot1q/dot1ad <> symmetric`
2. `rewrite ingress tag push dot1q/dot1ad <> second-dot1q <> symmetric`
3. `rewrite ingress tag translate 1-to-2 dot1q/dot1ad <> second-dot1q <> symmetric`



- (注) Cisco IOS XR ソフトウェア リリース 6.3.1 は、レイヤ 3 インターフェイス上での出力マーキングのポリシー マップをサポートしていません。

実行コンフィギュレーション

```
policy-map egress-marking
class qos1
set cos 1
!
class qos2
set cos 2
set dei 1
!
class qos3
set cos 3
!
class class-default
set cos 7
!
end-policy-map
!
```

バンドルトラフィックポリシー

ポリシーはバンドルにバインドできます。ポリシーがバンドルにバインドされている場合、各バンドルメンバ（ポート）で同じポリシーがプログラミングされます。たとえば、ポリサーまたはシェーパー レートがある場合、各ポートに同じレートが設定されます。トラフィックはロード バランシング アルゴリズムに基づいてメンバをバンドルするようスケジュールされます。

入力および出力トラフィックの両方がサポートされています。パーセントベースのポリシーと時間ベースのポリシーがサポートされています。



- (注) BVI インターフェイス上では、出力マーキングはサポートされていません。

詳細については、[リンク バンドルでの QoS の設定（50 ページ）](#) を参照してください。

デュアルポリシーマップを使用した QoS 出力マーキングとキューイング

QoS 出力マーキング/キューイングを実現するため、ルータはマーキングとキューイングに非依存ポリシーを使用して、出力上でデュアル ポリシー モデルを利用します。

出力マーキングは、qos-group/discard-class を設定することで、入力インターフェイス上にポリシーマップを適用して実現できます。次に、入力ポリシーマップで設定されている qos-group

を出力ポリシーマップと DP (drop-precedence または discard class) 値とともに使用することで、発信 L2 パケットの cos/dei を再マークします。同様に、出力キューイングは、トラフィッククラスを設定し、入力インターフェイスにポリシーマップを適用することで実現できます。次に、キューイングアクションを実行するために、出力ポリシーマップがトラフィッククラスを使用します。

利点

- この機能により、ユーザは DP (drop precedence) フィールドに基づいてマーキングを決定することができます。
- MPLS からレイヤ 2 へのトラフィック ストリームの場合、レイヤ 2 パケットは MPLS データパケット内にあります。したがって、データ伝送後はレイヤ 2 ヘッダーのマーキングは出力のみになる可能性があります。
- 出力書き換え動作の場合、VLAN タグが変更または追加されていると、cos または dei フィールドが出力マーキングでマークされることがあります。

QoS 出力マーキングとキューイングは、次の 3 つのステップにまとめることができます。

1. 入力ポリシーマップの設定：着信パケットを分類し、qos-group/discard-class またはトラフィッククラスを設定します。
2. 出力ポリシーマップの設定：
 - 出力マーキングポリシーの設定：
 - qos-group/discard-class で分類するためのクラスマップを作成します。
 - policy-map を作成し、L2 ヘッダーの cos/dei フィールドをマークします。
 - 出力キューイングポリシーの設定：
 - クラスマップを作成し、トラフィッククラスで分類します。
 - ポリシーマップを作成し、キューイングアクション（帯域幅、シェーピング、優先順位など）を実行します。
3. ポリシーをインターフェイスに付加します。



(注) QinQ トラフィックのマーキング時は、外側の dot1q ヘッダーのみが影響を受け、内側のヘッダーはそのまま残ります。ただし、新しい QinQ タグを追加した書き換え操作が少ない場合は、内側のヘッダーがマークされます。

例：入力ポリシーマップの設定：

```
/*Create class-map/*  
Router#config
```

```

Router(config)#class-map match-any cos2
Router(config-cmap)#match cos 2
Router(config-cmap)#commit
Router(config)#class-map match-any cos3
Router(config-cmap)#match cos 3
Router(config-cmap)#commit
Router(config)#class-map match-any cos4
Router(config-cmap)#match cos 4
Router(config-cmap)#commit

/*Create classification policies*/
Router#config
Router(config)#policy-map ingress-classification
Router(config-pmap)#class cos 2
Router(config-pmap-c)#set qos-group 1
Router(config-pmap-c)#set traffic-class 3
Router(config-pmap-c)#class cos3
Router(config-pmap-c)#set qos-group 2
Router(config-pmap-c)#set traffic-class 5
Router(config-pmap-c)#class cos4
Router(config-pmap-c)#set qos-group 3
Router(config-pmap-c)#set traffic-class 4
Router(config-pmap-c)#class class-default
Router(config-pmap-c)#set qos-group 7
Router(config-pmap-c)#set traffic-class 6
Router(config-pmap-c)#commit

```

例：出力ポリシーマップの設定：

```

*/Egress Marking Policy/*
Router#config
Router(config)#class-map match-any qos1
Router(config-cmap)#match qos-group 1
Router(config-cmap)#commit
Router(config)#class-map match-any qos2
Router(config-cmap)#match qos-group 2
Router(config-cmap)#commit
Router(config)#class-map match-any qos3
Router(config-cmap)#match qos-group 3
Router(config-cmap)#commit
Router#config
Router(config)#policy-map egress-marking
Router(config-pmap)#class qos1
Router(config-pmap-c)#set cos 1
Router(config-pmap-c)#class qos2
Router(config-pmap-c)#set cos 2
Router(config-pmap-c)#set dei 1
Router(config-pmap-c)#class qos3
Router(config-pmap-c)#set cos 3
Router(config-pmap-c)#class class-default
Router(config-pmap-c)#set cos 7
Router(config-pmap-c)#commit

*/Egress Queuing Policy/*
Router#config
Router(config)#class-map match-any tc3
Router(config-cmap)#match traffic-class 3
Router(config-cmap)#commit
Router(config)#class-map match-any tc4
Router(config-cmap)#match traffic-class 3
Router(config-cmap)#commit
Router(config)#class-map match-any tc5
Router(config-cmap)#match traffic-class 3

```

```
Router (config-cmap) #commit
Router#config
Router (config) #policy-map egress-queuing
Route (config-pmap) #class tc3
Router (config-pmap-c) #shape average 2 mbps
Router (config-pmap-c) #class tc4
Router (config-pmap-c) #shape average 5 mbps
Router (config-pmap-c) #class tc5
Router (config-pmap-c) #shape average 7 mbps
Router (config-pmap-c) #class class-default
Router (config-pmap-c) #commit
```

例：インターフェイスへのポリシーの付加

```
Router#config
Router (config) #interface tenGigE 0/0/1/0/0
Router (config-if) #service-policy input ingress-classification
Router (config-if) #service-policy output egress-marking
Router (config-if) #service-policy output egress-queuing
Router (config-if) #commit
```

制約事項

- マーキング ポリシーの統計情報はサポートされていません。つまり、show policy-map interface コマンドは出力を表示しません。
- キューイング ポリシーが適用されている場合にのみ、統計情報の出力が表示されます。
- 出力マーキング ポリシーは、qos-group/discard-class でのみ分類できます。
- 出力キューイング ポリシーはトラフィッククラスでのみ分類できます。
- 出力マーキング ポリシーがマークできるのは、L2 ヘッダーの cos/dei フィールドのみです。

制約事項

入力 QoS スケール制限については、次の表を参照してください。

表 1: 入力 QoS のスケール制限

	クラスマップ サイズ	入力 QoS が適用されるインターフェイスの最大数	
		コアあたり	NPU あたり
	4	872	1744
	8	436	872
	16	218	436
	32	109	218



(注) ルータのコアは単一であるため、コアあたりのスケールが適用されます。

その他の制約事項は次のとおりです。

- 入力サービス ポリシーに **set traffic class** ステートメントを明示的に設定した場合、対応する **match traffic class** をトラフィックの出力に設定して正しく一致するようにし、**show policy-map interface <> output** コマンド内で統計情報を説明する必要があります。入力トラフィックを出力の **class-default** に一致させるには、トラフィック クラスを入力上で 0 に設定する必要があります。
- 入力サービス ポリシーで **set traffic class** を設定し、出力に対応する **match traffic class** がない場合、トラフィックは **class default** には移動せず、そのトラフィック フローの統計情報は **show policy-map interface <> output** コマンド内に表示されません。
- 入力に **set traffic class** ステートメントがない場合、トラフィックは出力の **default-class** に到達します。
- 入力サービスポリシーに **set discard-class** ステートメントを設定した場合、対応する **match discard-class** をトラフィックの出力に設定して正しく一致するようにし、**show policy-map interface <> output** コマンド内で統計情報を説明する必要があります。
- 入力サービスポリシーに **set discard-class** を設定し、出力に対応する **match discard-class** がない場合、トラフィックは **class-default** には到達せず、このトラフィック フローの統計情報は **show policy-map interface <> output** コマンド内に表示されません。
- システムは、ピアリング モードではクラスマップ サイズをサポートしていません。

BVI 上での QoS の制約事項

- BVI 上の入力 QoS ポリシーはポリサーをサポートしません。
- システムは、BVI 上の出力 QoS ポリシーをサポートしません。
- BVI と同じブリッジ ドメインに含まれている L2 インターフェイス上に L3 入力 QoS ポリシーを適用すると、パケットがその BVI MAC アドレス宛である場合は分類が動作しない可能性があります。
- QoS ポリシーが BVI に付加されている場合、ポリシーは、同じブリッジドメインに含まれている L2 インターフェイスによって継承されます。そのため、他のポリシーは L2 インターフェイスに適用できません。同様に、QoS ポリシーが L2 インターフェイスのいずれかに付加されている場合は、同じブリッジドメインに含まれている BVI に QoS ポリシーを適用できません。

In-Place ポリシーの変更

In-Place ポリシーの変更機能では、QoS ポリシーが 1 つ以上のインターフェイスに付加されている場合でも QoS ポリシーを変更できます。変更されたポリシーは、新しいポリシーをインターフェイスにバインドするときに同じチェックを受けます。ポリシー変更が成功した場合、変更されたポリシーは、ポリシーが付加されているすべてのインターフェイスに対して有効になります。ただし、ポリシーの変更がいずれかのインターフェイスで失敗した場合には、すべてのインターフェイスに対して変更前のポリシーが有効になるように、自動ロールバックが開始されます。

また、ポリシー マップに使用するクラス マップを変更することもできます。クラス マップに対して行った変更は、ポリシーが付加されているすべてのインターフェイスに反映されます。



- (注)
- インターフェイスに付加されているポリシーの QoS 統計情報は、ポリシーを変更すると失われます (0 にリセット)。
 - インターフェイスに付加されている QoS ポリシーを変更したとき、変更されたポリシーを使用するインターフェイスでは、短期間、有効なポリシーがない場合が生じる可能性があります。
 - システムは、マーキング ポリシーの `show policy-map` 統計情報をサポートしていません。
 - ACL のインプレース変更では、ポリシーマップ統計情報カウンターはリセットされません。



- (注)
- L3 インターフェイスに適用される QoS EXP 出力マーキングの場合、NPU ごとの固有のポリシーマップは 3 つに制限されます。ポリシーマップの上限に達したときに、異なるインターフェイス間で共有されるポリシーマップを変更しようとする、エラーが発生する可能性があります。
 - L2 インターフェイスに適用される QoS 出力マーキング (CoS、DEI) の場合、NPU ごとの固有のポリシーマップは 13 に制限されます。ポリシーマップの上限に達したときに、異なるインターフェイス間で共有されているポリシーマップを変更しようとする、エラーが発生する可能性があります。

確認

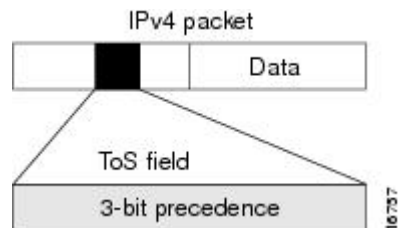
In-Place ポリシーの変更時に回復不可能なエラーが発生した場合は、ポリシーは対象のインターフェイスに対して矛盾した状態になります。コンフィギュレーションセッションのブロックが解除されるまで、新たな設定を行うことはできません。インターフェイスからポリシーを削除し、変更されたポリシーを確認し、それに応じて再適用することを推奨します。

モジュラ QoS サービス パケットの分類の参照

IP precedence によるパケットの CoS の指定

IP precedence を使用すると、パケットの CoS を指定できます。着信トラフィックで precedence レベルを設定し、そのレベルを QoS キューイング機能と組み合わせて使用することで、差別化サービスを作成できます。そうすることで、後続の各ネットワーク要素は、判断されたポリシーに基づいてサービスを提供できます。IP precedence は通常、ネットワークまたは管理ドメインの端にできるだけ近いところに配置されます。これによって、他のコアまたはバックボーンにおいて、優先順位に基づいて QoS を設定できます。

図 1: IPv4 パケットのタイプオブサービス フィールド



この目的には、IPv4 ヘッダーのタイプオブサービス (ToS) フィールドにある3つの precedence ビットを使用できます。ToS ビットを使用して、最大8つのサービスクラスを定義できます。その後、ネットワーク全体で設定された他の機能によって、これらのビットを使用して、ToS の付与に関するパケットの処理方法を決定します。これらの他の QoS 機能では、輻輳管理戦略や帯域幅の割り当てなど適切なトラフィック処理ポリシーを割り当てることができます。たとえば、LLQ などのキューイング機能は、パケットの IP precedence 設定を使用して、トラフィックに優先順位を付けることができます。

パケットの分類に使用する IP precedence ビット

IP ヘッダーの ToS フィールドにある3つの IP precedence ビットを使用して、各パケットの CoS 割り当てを指定します。最大8個のクラスにトラフィックを分類した後、ポリシーマップを作成して、各クラスの輻輳処理、帯域幅割り当てといったネットワーク ポリシーを定義できます。

各 precedence は名前に対応します。IP precedence ビットの設定6と7は、ルーティングアップデートなどのネットワーク制御情報用に予約されています。これらの名前はRFC 791 で定義されています。

IP precedence 値の設定

デフォルトでは、ルータは IP precedence 値を変更しません。これによって、ヘッダーの precedence 値セットが維持され、すべての内部ネットワーク デバイスが IP precedence の設定に基づいてサービスを提供できるようになります。このポリシーは、ネットワークのエッジでネットワークトラフィックをさまざまなタイプのサービスにソートすること、またこれらの

サービスタイプをネットワークコアで設定することを指定する標準的な方法に従っています。その後、ネットワークのコアにあるルータは、precedence ビットを使用して、送信順やパケットドロップの可能性などを決定できるようになります。

ネットワークに入ってくるトラフィックには外部デバイスで設定された precedence が設定されている可能性があるため、ネットワークに入るすべてのトラフィックの precedence をリセットすることを推奨します。IP precedence の設定を制御することによって、すでに IP precedence を設定したユーザが、自身のすべてのパケットに高い優先度設定を設定して、自身のトラフィックに対してより高いサービスを得ることを禁止します。

クラスベースの無条件パケットマーキング、および LLQ 機能では、IP precedence ビットを使用できます。

IP プレシデンス と IP DSCP マーキングの比較

ネットワークでパケットをマークする必要があり、すべてのデバイスで IP DSCP マーキングがサポートされている場合は、IP DSCP マーキングの方が無条件パケットマーキングのオプションが多いため、IP DSCP マーキングを使用してください。IP DSCP によるマーキングが好ましくない場合、またはネットワークにあるデバイスで IP DSCP 値がサポートされているかどうか不明な場合は、パケットのマーキングに IP precedence 値を使用してください。IP precedence 値は、おそらくネットワーク内のすべてのデバイスでサポートされています。

最大 8 種類の IP precedence マーキングと、64 種類の IP DSCP マーキングを設定できます。

QoS-group の使用とキューの選択

ルータは、各出力インターフェイスで最大 8 つの CoSQ をサポートしています。範囲は 0 ~ 7 で、0 はデフォルトの CoSQ です。qos-group 値は、CoSQ と最終的には仮想出力キュー (VOQ) を選択するために使用されます。

入力ポリシーマップで、CoSQ 0 以外の特定の CoSQ にトラフィッククラスを指定するには、クラスマップに `set qos-group x` コマンド (x は CoSQ 値) を明示的に設定する必要があります。

出力ポリシーマップで、対応する `match qos-group x` が設定されたクラスマップを使用すると、トラフィッククラスに QoS アクションをさらに適用できます。

次に例を示します。

```
policy-map test-ingress
class precl
set traffic-class 1
then, class-map tcl
match traffic-class 1
then,
policy-map test-egress
class tcl
shape average percent 70
```




第 2 章

モジュラ QoS の輻輳回避

輻輳回避技術では、トラフィックフローをモニタすることにより、共通ネットワークのボトルネックでの輻輳を予測し、回避します。発生した後に輻輳を制御する輻輳管理技術に対し、回避技術は輻輳が発生する前に実行されます。

輻輳の回避は、パケットのドロップにより行われます。ルータは、次の QoS 輻輳回避技術をサポートしています。

- [テールドロップと FIFO キュー \(21 ページ\)](#)
- [ランダム早期検出と TCP \(23 ページ\)](#)
- [Weighted Random Early Detection : 重み付けランダム早期検出 \(25 ページ\)](#)
- [テールドロップと FIFO キュー \(21 ページ\)](#)
- [ランダム早期検出と TCP \(23 ページ\)](#)
- [Weighted Random Early Detection : 重み付けランダム早期検出 \(25 ページ\)](#)

テール ドロップと FIFO キュー

テールドロップは、出力キューが満杯のときに、輻輳が削除されるまでパケットをドロップする輻輳回避技術です。テールドロップでは、すべてのトラフィックフローを平等に扱い、サービスクラス間で区別しません。テールドロップは、ファーストインファーストアウト (FIFO) キューに入り、下位リンク帯域幅によって決定したレートで転送された未分類のパケットを管理します。

テール ドロップの設定

クラスの一貫基準を満たすパケットは、サービスを提供されるまで、クラス用に予約されたキューに蓄積されます。**queue-limit** コマンドを使用して、クラスの最大しきい値を定義します。最大しきい値に達すると、クラス キューへの待機パケットがテールドロップ (パケットドロップ) します。

制約事項

- **queue-limit** コマンドを設定する場合は、デフォルトクラスを除き、**priority**、**shape average**、**bandwidth**、または **bandwidth remaining** のうちのいずれかのコマンドを設定する必要があります。

設定例

テールドロップの設定を実行するには、以下を完全に行う必要があります。

1. 1つ以上のインターフェイスに付加できるポリシーマップを作成（または変更）し、サービスポリシーを指定します。
2. トラフィッククラスのトラフィックポリシーへの関連付け
3. ポリシーマップに設定されているクラスポリシーにキューが保持できる最大限度の指定
4. ポリシーマップに属するトラフィックのクラスへの優先順位の指定
5. （任意）ポリシーマップに属するクラスに割り当てた帯域幅の指定、またはさまざまなクラスに残りの帯域幅を割り当てる方法の指定
6. 出力インターフェイスのサービスポリシーとして使用するためのその出力インターフェイスへのポリシーマップの付加

```
Router# configure
Router(config)# policy-map test-qlimit-1
Router(config-pmap)# class qos-1
Router(config-pmap-c)# queue-limit 100 us
Router(config-pmap-c)# priority level 7
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# interface HundredGigE 0/6/0/18
Router(config-if)# service-policy output test-qlimit-1
Router(config-if)# commit
```

実行コンフィギュレーション

```
policy-map test-qlimit-1
  class qos-1
    queue-limit 100 us
    priority level 7
  !
  class class-default
  !
end-policy-map
!
```

確認

```
Router# show qos int hundredGigE 0/6/0/18 output
```

```

NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000220 -- output policy
NPU Id:                               3
Total number of classes:                2
Interface Bandwidth:                    100000000 kbps
VOQ Base:                               11176
VOQ Stats Handle:                       0x88550ea0
Accounting Type:                        Layer1 (Include Layer 1 encapsulation and above)
-----
Level1 Class (HP7)                      = qos-1
Egressq Queue ID                        = 11177 (HP7 queue)
TailDrop Threshold                      = 1253376 bytes / 100 us (100 us)
WRED not configured for this class

Level1 Class                             = class-default
Egressq Queue ID                        = 11176 (Default LP queue)
Queue Max. BW.                          = 101803495 kbps (default)
Queue Min. BW.                          = 0 kbps (default)
Inverse Weight / Weight                  = 1 (BWR not configured)
TailDrop Threshold                      = 1253376 bytes / 10 ms (default)
WRED not configured for this class

```

関連項目

- [テールドロップと FIFO キュー \(21 ページ\)](#)

関連コマンド

- [queue-limit](#)

ランダム早期検出と TCP

ランダム早期検出 (RED) の輻輳回避技術は、TCP の輻輳制御メカニズムを利用しています。高輻輳期間の前にランダムにパケットをドロップすることにより、RED はパケットの送信元に、その伝送レートを低下させるよう指示します。パケット送信元が TCP を使用している場合、送信元はすべてのパケットが宛先に届くようになるまで伝送レートを下げます。これは輻輳が解消されたことを示します。TCP にパケットの送信速度を下げさせる手段として RED を使用できます。TCP は停止するだけでなく、素早く再起動して、ネットワークがサポート可能なレートに伝送レートを対応させます。

RED は時間の損失を分散させて、トラフィックのバーストを吸収しながら通常の低いキューの深さを維持します。インターフェイスでイネーブルにすると、RED は、設定時に選択したレートで輻輳が発生した場合にパケットのドロップを開始します。

ランダム早期検出の設定

ランダム早期検出 (RED) を有効にするには、**random-detect** コマンドと **default** キーワードを使用する必要があります。

ガイドライン

`class-default` を含む任意のクラスで **random-detect default** コマンドを設定する場合は、コマンド **shape average**、**bandwidth**、および **bandwidth remaining** を設定する必要があります。

設定例

ランダム早期検出の設定を実行するには、以下を完全に行う必要があります。

- 1つ以上のインターフェイスに付加できるポリシー マップを作成（または変更）し、サービス ポリシーを指定します。
- トラフィック クラスのトラフィック ポリシーへの関連付け
- デフォルトの最小しきい値および最大しきい値を使用した RED の有効化
- （任意）ポリシーマップに属するクラスに割り当てた帯域幅の指定、またはさまざまなクラスに残りの帯域幅を割り当てる方法の指定
- （任意）指定したビット レートまたは使用可能な帯域幅のパーセンテージに従ったトラフィックのシェーピング
- 出力インターフェイスのサービス ポリシーとして使用するためのその出力インターフェイスへのポリシー マップの付加

```
Router# configure
Router(config)# policy-map test-wred-2
Router(config-pmap)# class qos-1
Router(config-pmap-c)# random-detect default
Router(config-pmap-c)# shape average percent 10
Router(config-pmap-c)# end-policy-map
Router(config)# commit
Router(config)# interface HundredGigE 0/6/0/18
Router(config-if)# service-policy output test-wred-2
Router(config-if)# commit
```

実行コンフィギュレーション

```
policy-map test-wred-2
  class qos-1
    random-detect default
    shape average percent 10
  !
  class class-default
  !
end-policy-map
!

interface HundredGigE 0/6/0/18
  service-policy output test-wred-2
!
```

確認

```
Router# show qos int hundredGigE 0/6/0/18 output
```

```
NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000220 -- output policy
NPU Id: 3
Total number of classes: 2
Interface Bandwidth: 100000000 kbps
VOQ Base: 11176
VOQ Stats Handle: 0x88550ea0
Accounting Type: Layer1 (Include Layer 1 encapsulation and above)
-----
Level1 Class = qos-1
Egressq Queue ID = 11177 (LP queue)
Queue Max. BW. = 10082461 kbps (10 %)
Queue Min. BW. = 0 kbps (default)
Inverse Weight / Weight = 1 (BWR not configured)
Guaranteed service rate = 10000000 kbps
TailDrop Threshold = 12517376 bytes / 10 ms (default)

Default RED profile
WRED Min. Threshold = 12517376 bytes (10 ms)
WRED Max. Threshold = 12517376 bytes (10 ms)

Level1 Class = class-default
Egressq Queue ID = 11176 (Default LP queue)
Queue Max. BW. = 101803495 kbps (default)
Queue Min. BW. = 0 kbps (default)
Inverse Weight / Weight = 1 (BWR not configured)
Guaranteed service rate = 50000000 kbps
TailDrop Threshold = 62652416 bytes / 10 ms (default)
WRED not configured for this class
```

関連項目

- [ランダム早期検出と TCP \(23 ページ\)](#)

関連コマンド

- [random-detect](#)

Weighted Random Early Detection : 重み付けランダム早期検出

重み付けランダム初期検知 (WRED) は、discard-class のような指定された任意の条件に基づいて選択的にパケットをドロップします。WREDは、この一致基準を使用して、異なるタイプのトラフィックの処理方法を決定します。

WRED は **random-detect** コマンドとさまざまな discard-class 値を使用して設定できます。値には、そのフィールドにおいて有効な値の範囲またはリストを指定できます。また、最小キューしきい値および最大キューしきい値を使用して、ドロップするポイントを決定できます。WRED

最大しきい値がキュー制限の近くにあることを確認します。最大しきい値に達すると、パケットはドロップされ始めます。

パケットが着信すると、次の処理が行われます。

- 平均キュー サイズが計算されます。
- 平均キュー サイズが最小キュー しきい値よりも小さい場合、着信パケットはキューイングされます。
- 平均キュー サイズがそのトラフィック タイプの最小キュー しきい値と、インターフェイスの最大しきい値の間の場合、そのトラフィック タイプのパケット ドロップ確率に応じて、パケットはドロップされるか、キューイングされます。
- 平均キュー サイズが最大しきい値を超える場合、パケットはドロップします。

WRED の平均キュー サイズ

ルータで、WRED 計算で使用するパラメータが自動的に定義されます。平均キュー サイズは、キューの前の平均と現在のサイズを基にしています。式は次のようになります。

$$\text{average} = (\text{old_average} * (1 - 2^{-x})) + (\text{current_queue_size} * 2^{-x})$$

ここで、 x は指数加重係数です。

x を高い値にすると、前回の平均が重要視されます。係数を大きくすると、キューの長さの最大値と最小値が滑らかになります。平均キュー サイズは、素早い変化はしにくく、サイズの急激な変化を回避します。WRED 処理で、パケットのドロップの開始が遅くなりますが、実際のキュー サイズが最低しきい値を下回った時点でも、パケットのドロップが続く場合があります。ゆっくりと平均が推移するため、トラフィックの一時的なバーストが緩和されます。



- (注)
- 指数加重係数 x は固定されており、ユーザが設定することはできません。
 - x の値が高すぎる場合、WRED は輻輳に反応しません。パケットは、WRED が無効のときのように送信またはドロップします。
 - x の値が低すぎると、WRED は一時的なトラフィック バーストに過剰反応し、不必要にトラフィックをドロップします。

x の値が低い場合、平均キュー サイズは現在のキュー サイズ付近を追跡します。結果、平均はトラフィック レベルの変化とともに上下します。この場合、WRED 処理は、長いキューに素早く応答します。キューが最低しきい値を下回ると、パケットのドロップ処理が停止します。

重み付けランダム早期検出の設定

この設定タスクは、RED に **random-detect** コマンドを設定しないことを除き、RED の場合と同様です。

制約事項

- **priority** コマンドを使用して設定したクラスでは **random-detect** コマンドを使用できません。これは、プライオリティキューイング (PQ) に設定されているクラスでは WRED が設定できないからです。
- **random-detect** コマンドを設定する場合は、**shape average**、**bandwidth**、**bandwidth remaining** のいずれかのコマンドを設定する必要があります。

設定例

ランダム早期検出の設定を実行するには、以下を完全に行う必要があります。

1. 1つ以上のインターフェイスに付加できるポリシー マップを作成（または変更）し、サービス ポリシーを指定します。
2. トラフィック クラスのトラフィック ポリシーへの関連付け
3. 一致条件 (discard-class) の指定による WRED の有効化
4. (任意) ポリシーマップに属するクラスに割り当てた帯域幅の指定、またはさまざまなクラスに残りの帯域幅を割り当てる方法の指定
5. (任意) 指定したビット レートまたは使用可能な帯域幅のパーセンテージに従ったトラフィックのシェーピング
6. (任意) キュー制限の変更による各キューで使用可能なバッファ量の微調整
7. 出力インターフェイスのサービスポリシーとして使用するためのその出力インターフェイスへのポリシー マップの付加

```
Router# configure
Router(config)# policy-map test-wred-1
Router(config-pmap)# class qos-1
Router(config-pmap-c)# random-detect default
Router(config-pmap-c)# random-detect 10 ms 500 ms
Router(config-pmap-c)# shape average percent 10
Router(config-pmap-c)# commit

Router(config)# interface HundredGigE 0/6/0/18
Router(config-if)# service-policy output policy1
Router(config-if)# commit
```

実行コンフィギュレーション

```
policy-map test-wred-1
  class qos-1
    random-detect default
    random-detect 10 ms 500 ms
    shape average percent 10
  !
class class-default
!
end-policy-map
```

```

!
interface HundredGigE 0/6/0/18
  service-policy output test-wred-1
!

```

確認

```
Router# show qos int hundredGigE 0/6/0/18 output
```

```

NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000220 -- output policy
NPU Id:                               3
Total number of classes:               2
Interface Bandwidth:                   100000000 kbps
VOQ Base:                               11176
VOQ Stats Handle:                       0x88550ea0
Accounting Type:                         Layer1 (Include Layer 1 encapsulation and above)
-----
Level1 Class                           = qos-1
Egressq Queue ID                       = 11177 (LP queue)
Queue Max. BW.                          = 10082461 kbps (10 %)
Queue Min. BW.                          = 0 kbps (default)
Inverse Weight / Weight                 = 1 (BWR not configured)
Guaranteed service rate                 = 10000000 kbps
TailDrop Threshold                      = 1073741824 bytes / 858 ms (default)

Default RED profile
WRED Min. Threshold                     = 12517376 bytes (10 ms)
WRED Max. Threshold                     = 629145600 bytes (500 ms)

Level1 Class                           = class-default
Egressq Queue ID                       = 11176 (Default LP queue)
Queue Max. BW.                          = 101803495 kbps (default)
Queue Min. BW.                          = 0 kbps (default)
Inverse Weight / Weight                 = 1 (BWR not configured)
Guaranteed service rate                 = 50000000 kbps
TailDrop Threshold                      = 62652416 bytes / 10 ms (default)
WRED not configured for this class

```

関連項目

- [Weighted Random Early Detection : 重み付けランダム早期検出 \(25 ページ\)](#)
- [ランダム早期検出の設定 \(23 ページ\)](#)

関連コマンド

- [random-detect](#)



第 3 章

輻輳管理の概要

輻輳管理機能では、パケットに割り当てられた優先順位に基づいて、トラフィックフロー（またはパケット）がインターフェイスに送信される順番を決定することにより、輻輳を制御できます。輻輳管理は、キューを作成し、そのキューにパケットの分類に基づいてパケットを割り当て、キューにあるパケットの送信をスケジューリングする必要があります。

サポートされているトラフィック調整メカニズムのタイプは、次のとおりです。

- [Class-based Weighted Fair Queueing \(29 ページ\)](#)
- [低遅延キューイングとストリクトプライオリティキューイング \(32 ページ\)](#)
- [トラフィックシェーピング \(34 ページ\)](#)
- [トラフィックポリシング \(36 ページ\)](#)
- [Class-based Weighted Fair Queueing \(29 ページ\)](#)
- [残存帯域幅の設定：インスタンス 2 \(30 ページ\)](#)
- [低遅延キューイングとストリクトプライオリティキューイング \(32 ページ\)](#)
- [トラフィックシェーピング \(34 ページ\)](#)
- [トラフィックポリシング \(36 ページ\)](#)
- [モジュラ QoS 輻輳管理のリファレンス \(44 ページ\)](#)

Class-based Weighted Fair Queueing

Class-based Weighted Fair Queueing (CBWFQ) を使用すると、顧客の一致基準に基づいて、トラフィッククラスを定義できます。CBWFQ を使用して、トラフィッククラスを定義し、保証された最小帯域幅量をそのクラスに割り当てることができます。また、CBWFQ により、遅延に影響されやすいトラフィックのストリクトプライオリティキューが可能になります。

残りの帯域幅

CBWFQ アルゴリズムは、クラスに割り当てられた残存帯域幅の値から各クラスの重みを取得します。**bandwidth remaining** オプションでは、CBWFQ に対するクラスの重みを指定します。プライオリティキューが処理された後、残存帯域幅は帯域幅余剰比率 (BWRR) またはパーセ

ントに応じて分散されます。このコマンドをいずれのクラスにも設定しない場合、BWRR のデフォルト値が 1 と見なされます。**bandwidth remaining percent** の場合、残存帯域幅は 100 パーセントになるように他のクラスに均等に分散されます。

制約事項

- **bandwidth remaining** コマンドは、出力ポリシーに対してのみサポートされます。

残存帯域幅の設定：インスタンス 2

サポートされているプラットフォーム：Cisco NCS 5500、Cisco NCS 540、および Cisco NCS 560 シリーズルータ

この手順で最小帯域幅とルータ上の残存帯域幅を設定します。



- (注) **bandwidth**、**bandwidth remaining**、**shaping**、**queue-limit**、および **wred** コマンドは同じクラス内で一緒に設定することができます。ただし、**priority** はこれらのコマンドと一緒に設定できません (**priority** コマンドは **shape** および **queue-limit** と一緒に設定できます)。

設定例

最小帯域幅および残存帯域幅の設定を実行するには、以下を完全に行う必要があります。

1. 1 つ以上のインターフェイスに付加できるポリシー マップの作成または変更
2. ポリシーを作成または変更する必要があるトラフィック クラスの指定
3. クラスへの最小帯域幅および残存帯域幅の割り当て
4. 出力インターフェイスへのポリシー マップの適用

```
Router# configure
Router(config)# policy-map test-bw-bw-rem
Router(config-pmap)# class qos-6
Router(config-pmap-c)# bandwidth percent 60
Router(config-pmap-c)# bandwidth remaining percent 60
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface HundredGigE 0/6/0/18
Router(config-if)# service-policy output test-bw-bw-rem
Router(config-if)# commit
```

実行コンフィギュレーション

```
policy-map test-bw-bw-rem
  class qos-6
    bandwidth percent 60
```

```

    bandwidth remaining percent 60
    !
    class qos-5
      bandwidth percent 20
      bandwidth remaining percent 40
    !
    class class-default
    !
  end-policy-map
!

interface HundredGigE0/6/0/18
  service-policy input 100g-s1-1
  service-policy output test-bw-bw-rem
!

```

確認

Router# **show qos interface HundredGigE 0/6/0/18 output**

```

NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000220 -- output policy
NPU Id:                               3
Total number of classes:               3
Interface Bandwidth:                   100000000 kbps
VOQ Base:                              11176
VOQ Stats Handle:                      0x88550ea0
Accounting Type:                       Layer1 (Include Layer 1 encapsulation and above)
-----
Level1 Class                           = qos-6
Egressq Queue ID                       = 11182 (LP queue)
Queue Max. BW.                         = 100824615 kbps (default)
Queue Min. BW.                         = 60494769 kbps (60 %)
Inverse Weight / Weight                 = 2 (60%)
Guaranteed service rate                 = 71881188 kbps
TailDrop Threshold                     = 90177536 bytes / 10 ms (default)
WRED not configured for this class

Level1 Class                           = qos-5
Egressq Queue ID                       = 11181 (LP queue)
Queue Max. BW.                         = 100824615 kbps (default)
Queue Min. BW.                         = 20164923 kbps (20 %)
Inverse Weight / Weight                 = 3 (40%)
Guaranteed service rate                 = 27920792 kbps
TailDrop Threshold                     = 35127296 bytes / 10 ms (default)
WRED not configured for this class

Level1 Class                           = class-default
Egressq Queue ID                       = 11176 (Default LP queue)
Queue Max. BW.                         = 101803495 kbps (default)
Queue Min. BW.                         = 0 kbps (default)
Inverse Weight / Weight                 = 120 (BWR not configured)
Guaranteed service rate                 = 198019 kbps
TailDrop Threshold                     = 247808 bytes / 10 ms (default)
WRED not configured for this class

```

関連項目

- [残りの帯域幅 \(29 ページ\)](#)

関連コマンド

- [bandwidth remaining](#)

低遅延キューイングとストリクトプライオリティキューイング

低遅延キューイング (LLQ) 機能は、ストリクトプライオリティキューイング (PQ) を CBWFQ スケジューリングメカニズムにします。ストリクトプライオリティモードのプライオリティキューイング (PQ) は、場合によっては他のすべてのトラフィックを犠牲にして、1つのタイプのトラフィックが送信されることを確保します。PQ では、低プライオリティキューは悪影響を受けることがあり、最悪の場合、帯域幅の一部が使用可能な場合や、クリティカルなトラフィックの伝送レートが高い場合に、そのパケットが送信できなくなります。完全 PQ では、音声などの遅延に影響されやすいデータを、他のキューのパケットをキューから取り出す前にキューから取り出して送信できます。

ストリクトプライオリティキューイングによる低遅延キューイングの設定

ストリクトプライオリティキューイング (PQ) による低遅延キューイング (LLQ) を設定することで、音声などの遅延に影響されやすいデータを、他のキューのパケットをキューから取り出す前にキューから取り出して送信できます。

ガイドライン

- プライオリティレベル 1～7のみがサポートされています。プライオリティ 1 が最も高く、7 が最も低くなります。ただし、デフォルトの CoSQ 0 がすべての中でプライオリティが最も低くなります。
- 出力ポリシングはサポートされません。したがって、ストリクトプライオリティキューイングの場合、他のキューが提供されない可能性があります。
- `shape average` コマンドと `queue-limit` コマンドは `priority` とともに設定できます。

設定例

ストリクトプライオリティキューイングによる LLQ を完了するには、以下を完全に行う必要があります。

1. 1つ以上のインターフェイスに付加できるポリシーマップの作成または変更
2. ポリシーを作成または変更する必要があるトラフィッククラスの指定
3. トラフィッククラスへの優先度の指定
4. (オプション) 特定のビットレートへのトラフィックのシェーピング

5. 出力インターフェイスへのポリシー マップの適用

```
Router# configure
Router(config)# policy-map test-priority-1
Router(config-pmap)# class qos1
Router(config-pmap-c)# priority level 7
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface HundredGigE 0/6/0/18
Router(config-if)# service-policy output test-priority-1
Router(config-if)# no shutdown
Router(config-if)# commit
```

実行コンフィギュレーション

```
policy-map test-priority-1
  class qos-1
    priority level 7
  !
  class qos-2
    priority level 6
  !
  class class-default
  !
end-policy-map
!

interface HundredGigE0/6/0/18
  service-policy input 100g-s1-1
  service-policy output test-priority-1
!
```

確認

```
Router# show qos int hundredGigE 0/6/0/18 output
```

NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000220 -- output policy

```
NPU Id: 3
Total number of classes: 3
Interface Bandwidth: 100000000 kbps
VOQ Base: 11176
VOQ Stats Handle: 0x88550ea0
Accounting Type: Layer1 (Include Layer 1 encapsulation and above)
-----
Level1 Class (HP7) = qos-1
Egressq Queue ID = 11177 (HP7 queue)
TailDrop Threshold = 125304832 bytes / 10 ms (default)
WRED not configured for this class

Level1 Class (HP6) = qos-2
Egressq Queue ID = 11178 (HP6 queue)
TailDrop Threshold = 125304832 bytes / 10 ms (default)
WRED not configured for this class

Level1 Class = class-default
Egressq Queue ID = 11176 (Default LP queue)
```

```

Queue Max. BW.                = 101803495 kbps (default)
Queue Min. BW.                = 0 kbps (default)
Inverse Weight / Weight       = 1 (BWR not configured)
TailDrop Threshold            = 1253376 bytes / 10 ms (default)
WRED not configured for this class

```

関連コマンド

- [priority](#)

トラフィックシェーピング

トラフィックシェーピングでは、インターフェイスから出力されるトラフィックフローを制御して、リモートターゲットインターフェイスの速度に合わせてトラフィックフローを伝送することにより、指定されているポリシーにトラフィックを適合させることができます。ダウンストリーム要件を満たすように、特定のプロファイルに適合するトラフィックをシェーピングできるため、データレートが一致しないトポロジで発生するボトルネックが排除されます。



(注) トラフィックシェーピングは、出力方向でのみサポートされています。

トラフィックシェーピングの設定

発信インターフェイス上で実行されるトラフィックシェーピングは、レイヤ1レベルで実行され、レート計算にレイヤ1ヘッダーが含まれます。

ガイドライン

- 出力トラフィックシェーピングのみがサポートされます。
- 出力ポリシーの8つの qos-group クラス (class-default を含む) をすべて設定する必要があります。
- **shape average** コマンドは **priority** コマンドとともに設定できます。

設定例

トラフィックシェーピングの設定を完了するには、以下を完全に行う必要があります。

1. 1つ以上のインターフェイスに付加できるポリシーマップの作成または変更
2. ポリシーを作成または変更する必要があるトラフィッククラスの指定
3. 特定のビットレートへのトラフィックのシェーピング
4. 出力インターフェイスへのポリシーマップの適用


```

Router# configure
Router(config)# policy-map egress_policy1
Router(config-pmap)# class c5
Router(config-pmap-c)# shape average percent 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface HundredGigE 0/1/0/0
Router(config-if)# service-policy output egress_policy1
Router(config-if)# commit

```

実行コンフィギュレーション

```

policy-map egress_policy1
  class c5
    shape average percent 40
  !
  class class-default
  !
end-policy-map
!

interface HundredGigE0/6/0/18
  service-policy input 100g-s1-1
  service-policy output egress_policy1
!

```

確認

```

Router# show qos interface hundredGigE 0/6/0/18 output

NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000220 -- output policy
NPU Id: 3
Total number of classes: 2
Interface Bandwidth: 100000000 kbps
VOQ Base: 11176
VOQ Stats Handle: 0x88550ea0
Accounting Type: Layer1 (Include Layer 1 encapsulation and above)
-----
Level1 Class = c5
Egressq Queue ID = 11177 (LP queue)
Queue Max. BW. = 40329846 kbps (40 %)
Queue Min. BW. = 0 kbps (default)
Inverse Weight / Weight = 1 (BWR not configured)
Guaranteed service rate = 40000000 kbps
TailDrop Threshold = 50069504 bytes / 10 ms (default)
WRED not configured for this class

Level1 Class = class-default
Egressq Queue ID = 11176 (Default LP queue)
Queue Max. BW. = 101803495 kbps (default)
Queue Min. BW. = 0 kbps (default)
Inverse Weight / Weight = 1 (BWR not configured)
Guaranteed service rate = 50000000 kbps
TailDrop Threshold = 62652416 bytes / 10 ms (default)
WRED not configured for this class

```

関連項目

- [輻輳管理の概要 \(29 ページ\)](#)

関連コマンド

- `shape average`

トラフィック ポリシング

トラフィック ポリシングでは、インターフェイスで送受信されるトラフィックの最大レートを制限したり、ネットワークを複数のプライオリティレベルまたはサービスクラス (CoS) に区切ることができます。トラフィック ポリシングは、トークンバケットアルゴリズムを通じてトラフィックの最大レートを管理します。トークンバケットアルゴリズムでは、ユーザが設定した値を使用して、特定の瞬間にインターフェイス上で許可されるトラフィックの最大レートを決定します。トークンバケットアルゴリズムは、(トラフィック ポリシングでトラフィック ポリシーが設定された場所により) インターフェイスを出入りするすべてのトラフィックによって影響を受け、複数の大きなパケットが同じトラフィック ストリームで送信される場合に、ネットワーク帯域幅の管理に役立ちます。デフォルトでは、設定された帯域幅の値でインターフェイスから送信されるトラフィックに適用されるレイヤ 2 のカプセル化が考慮されません。

トラフィック ポリシングでは、認定情報レート (CIR) のバーストサイズ (Bc) を設定することにより、一定量の帯域幅管理も行えます。[認定バーストおよび超過バースト \(37 ページ\)](#) を参照してください。

ルータは、次のトラフィック ポリシング モードをサポートしています。

- カラーブラインドモードのシングルレート 2 カラー (SR2C)。[シングルレート ポリサー \(37 ページ\)](#) を参照してください。
- カラーブラインドモードのシングルレート 3 カラー (SR3C)。
- カラーブラインドモードの 2 レート 3 カラー (2R3C)。[2 つのレートを使用したポリシング機能 \(42 ページ\)](#) を参照してください。

制約事項

- トラフィック ポリシングは入力方向でのみサポートされ、カラーブラインドモードのみがサポートされています。
- ポリサー マーキングはサポートされていません。
- ポリサーは、コアレベルのインターフェイスに設定され、「show qos int <>」が NPU レベルで表示されます。

バンドル メンバーが同じ NPU に属していてもコア (NPU コア) が異なるバンドル インターフェイスに設定されているポリサーの場合、各メンバーはコアレベルのポリサー 設

定までトラフィックを送信しますが、「show qos int <>」は NPU レベルのポリサー出力を表示します。

例：

2つの 10GE メンバー（同じ NPU ではあっても、core0 のインターフェイスが 1 つ、core1 のインターフェイスが 1 つ）を持つバンドルインターフェイスの場合、バンドルインターフェイスに適用される 2R3C ポリサー（確認レートが 1G、超過レートが 1G、合計で 2G のポリサー レート）が「show qos int <>」出力に表示されます。

core0 のインターフェイス：確認レート 500 Mbps、超過レート 500 Mbps

core1 のインターフェイス：確認レート 500 Mbps、超過レート 500 Mbps

2つのインターフェイスのうちの1つのトラフィックについては、ポリシングされたレートが 1 Gbps になります。2つのインターフェイス上のトラフィックの場合、ポリシングされたレートは 2 Gbps になります。

認定バーストおよび超過バースト

トラフィックシェーパとは異なり、トラフィックポリサーは超過パケットをバッファせず、後で送信します。代わりに、ポリサーはバッファリングせずに「送信または送信なし」のポリシーを実行します。ポリシングは、通常のバースト値または認定バースト (bc) 値および超過バースト値 (be) を使用して、ルータが設定された設定情報レート (CIR) に到達できるようにします。ポリシングは、設定したバースト値に基づいて、パケットが CIR に適合しているか、または CIR を超過しているかを決定します。バーストパラメータは、ルータの一般的なバッファリングルールに基づいており、ラウンドトリップ時間のビットレートと同じになるようにバッファリングを設定して、輻輳期間中におけるすべての接続の、未処理の TCP ウィンドウに対応することが推奨されます。輻輳期間中には、超過バーストパラメータを適切に設定することにより、ポリサーによるパケットのドロップを抑えることができます。

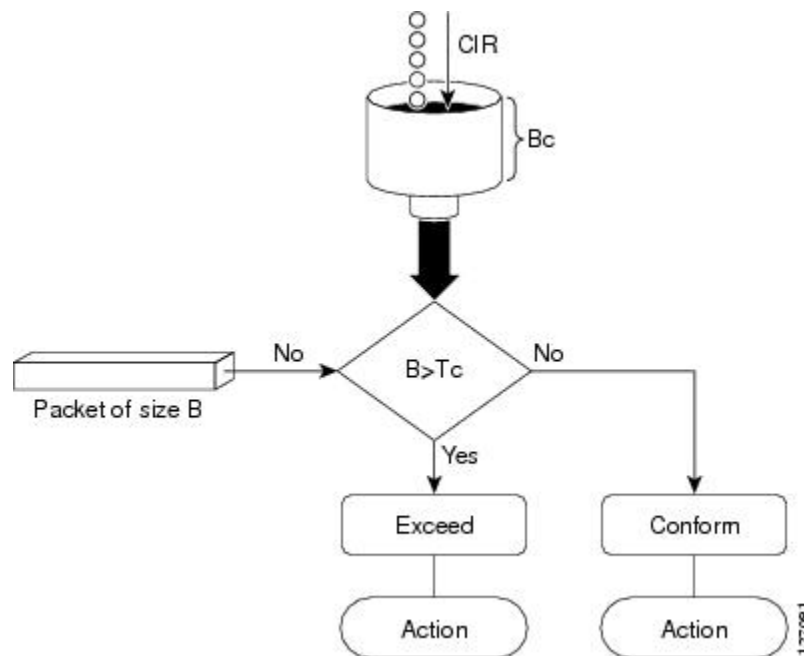
詳細については、[認定バースト \(44 ページ\)](#) および [超過バースト \(45 ページ\)](#) を参照してください。

シングルレート ポリサー

シングルレート 2 カラー ポリサー

シングルレート 2 カラー (SR2C) ポリサーでは、各パケットに対する 2 つのアクション (conform アクションおよび exceed アクション) を実行する単一のトークンバケットを使用できます。

図 2: シングルレート 2 カラー ポリサーのワークフロー



設定情報レート (CIR) の値に基づいて、トークンバケットは更新時間間隔で更新されます。Tc トークンバケットには Bc 値まで含めることができ、この値には、特定のバイト数または期間を指定できます。サイズ B のパケットが Tc トークンバケットを超える場合、パケットは CIR 値を超え、デフォルトのアクションが実行されます。サイズ B のパケットが Tc トークンバケット未満の場合、パケットは適合し、デフォルトの異なるアクションが実行されます。

シングルレート 3 カラー ポリサー

シングルレート 3 カラー (SR3C) ポリサーでは、各パケットに対する 3 つのアクション (conform アクション、exceed アクション、および violate アクション) を実行する単一のトークンバケットを使用できます。パケットは、CIR 値と 2 つの関連するバースト サイズ (認定バースト サイズ (CBS) と超過バースト サイズ (EBS)) に基づいてマーキングされます。パケットが CBS を超過しない場合、適合パケットとしてマークされます。パケットが CBS を超過するが EBS を超過しない場合、そのパケットは超過したものとしてマークされます。EBS も超過すると、違反パケットとしてマークされます。

トラフィック ポリシングの設定 (シングルレート 2 カラー)

トラフィック ポリシングは、多くの場合、ネットワークに出入りするトラフィックのレートを制限するためにネットワークのエッジのインターフェイスで設定されます。シングルレート 2 カラー ポリサーのデフォルトの適合アクションでパケットが送信され、デフォルト超過アクションでパケットがドロップされます。ユーザはこれらのデフォルトのアクションを変更できません。

設定例

トラフィック ポリシング設定を実行するには、以下を完全に行う必要があります。

1. 1つ以上のインターフェイスに付加できるポリシー マップの作成または変更
2. ポリシーを作成または変更する必要があるトラフィック クラスの指定
3. (任意) マーキングアクションの指定
4. トラフィックに対するポリシー レートの指定
5. 入力インターフェイスへのポリシー マップの適用

```
Router# configure
Router(config)# policy-map test-police-1
Router(config-pmap)# class ipv6-6
Router(config-pmap-c)# set dscp cs2 (optional)
Router(config-pmap-c)# set qos-group 7 (optional)
Router(config-pmap-c)# police rate percent 20 burst 10000 bytes
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface HundredGigE 0/6/0/18
Router(config-if)# service-policy input test-police-1
Router(config-if)# commit
```

実行コンフィギュレーション

```
class-map match-any ipv6-6
 match precedence 3
 end-class-map
!

policy-map test-police-1
 class ipv6-6
  set dscp cs2
  set qos-group 7
  police rate percent 20 burst 10000 bytes
 !
!
 class class-default
 !
 end-policy-map
!

interface HundredGigE0/6/0/18
 service-policy input test-police-1
 service-policy output test-priority-1
!
```

確認

```
Router# show qos interface hundredGigE 0/6/0/18 input

NOTE:- Configured values are displayed within parentheses
```

トラフィック ポリシングの設定 (シングルレート 3 カラー)

```

Interface HundredGigE0/6/0/18 ifh 0x3000220 -- input policy
NPU Id:                               3
Total number of classes:               2
Interface Bandwidth:                   100000000 kbps
Accounting Type:                       Layer1 (Include Layer 1 encapsulation and above)
-----
Levell Class                           =   ipv6-6
New dscp                                =   16
New qos group                           =   7

Policer Bucket ID                      =   0x102a0
Policer Stats Handle                   =   0x8a8090c0
Policer committed rate                  =   19980000 kbps (20 %)
Policer conform burst                   =   9856 bytes (10000 bytes)

Levell Class                           =   class-default

Default Policer Bucket ID               =   0x102a1
Default Policer Stats Handle            =   0x8a808e78
Policer not configured for this class

```

関連項目

- [トラフィック ポリシング \(36 ページ\)](#)

関連コマンド

- [police rate](#)

トラフィック ポリシングの設定 (シングルレート 3 カラー)

シングルレート 3 カラーポリサーのデフォルトの適合アクションと超過アクションでパケットが送信され、デフォルトの違反アクションでパケットがドロップされます。ユーザはこれらのデフォルトのアクションを変更できません。

設定例

トラフィック ポリシング設定を実行するには、以下を完全に行う必要があります。

1. 1 つ以上のインターフェイスに付加できるポリシー マップの作成または変更
2. ポリシーを作成または変更する必要があるトラフィック クラスの指定
3. (任意) マーキング アクションの指定
4. トラフィックのポリシー レートとピークバースト値の設定
5. 入力インターフェイスへのポリシー マップの適用

```

Router# configure
Router(config)# policy-map test-police-1R3C
Router(config-pmap)# class ipv4-5
Router(config-pmap-c)# set qos-group 2 (optional)
Router(config-pmap-c)# police rate percent 20 burst 100000 bytes peak-burst 190000 bytes
Router(config-pmap-c-police)# exit

```

```

Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface HundredGigE 0/6/0/18
Router(config-if)# service-policy input test-police-1R3C
Router(config-if)# commit

```

実行コンフィギュレーション

```

class-map match-any ipv4-5
  match precedence 3
end-class-map
!

policy-map test-police-1R3C
  class ipv4-5
    set qos-group 7
    police rate percent 20 burst 100000 bytes peak-burst 190000 bytes
  !
  class class-default
  !
end-policy-map
!

interface HundredGigE0/6/0/18
  service-policy input test-police-1R3C
  service-policy output test-priority-1
!

```

確認

```

Router# show qos interface hundredGigE 0/6/0/18 input

NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000220 -- input policy
NPU Id: 3
Total number of classes: 2
Interface Bandwidth: 100000000 kbps
Accounting Type: Layer1 (Include Layer 1 encapsulation and above)
-----
Level1 Class = ipv4-5
New qos group = 2

Policer Bucket ID = 0x102a1
Policer Stats Handle = 0x8a8090c0
Policer committed rate = 19980000 kbps (20 %)
Policer conform burst = 99584 bytes (100000 bytes)
Policer exceed burst = 188672 bytes (190000 bytes)

Level1 Class = class-default

Default Policer Bucket ID = 0x102a1
Default Policer Stats Handle = 0x8a808e78
Policer not configured for this class

```

関連項目

- [トラフィック ポリシング \(36 ページ\)](#)

関連コマンド

- [police rate](#)

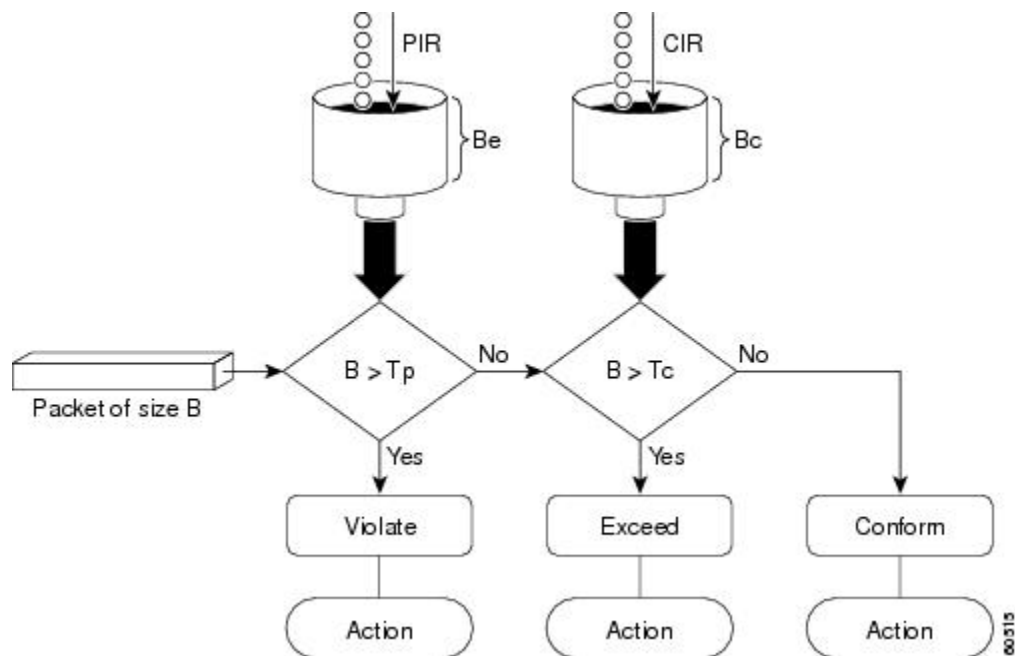
2つのレートを使用したポリシング機能

2 レート ポリサーは、2つのトークン バケット（認定トークン バケットおよび最大トークン バケット）を使用してトラフィックの最大レートを管理します。デュアルトークンバケット アルゴリズムは、ユーザが設定した値を使用して、特定の時点においてキューで許可されるトラフィックの最大レートを決定します。これにより、2レートポリサーは、2つの独立したレート（認定情報レート（CIR）および最大情報レート（PIR））でトラフィックを測定できます。

デュアルトークンバケットアルゴリズムでは、各パケットに対する3つのアクション（conform アクション、exceed アクション、および任意のviolate アクション）を使用できます。2レートポリサーを設定した状態でキューに入るトラフィックは、これらのカテゴリのいずれかに配置されます。アクションは、カテゴリごとに事前に決定されます。デフォルトのconformおよびexceedアクションはパケットを送信するようになっており、デフォルトのviolateアクションはパケットをドロップするようになっています。

次の図に、2レートポリサーを使用してパケットをマーキングする方法、および対応するアクションをパケットに割り当てる方法を示します。

図 3: パケットのマーキングとアクションの割り当て : 2レート ポリサー



また、2レートポリサーの詳細（46 ページ）も参照してください。

ルータは 2 レート 3 カラー (2R3C) ポリサーをサポートしています。

トラフィック ポリシングの設定 (2 レート 3 カラー)

2 レート 3 カラー (2R3C) ポリサーのデフォルトの適合アクションと超過アクションでパケットが送信され、デフォルトの違反アクションでパケットがドロップされます。ユーザはこれらのデフォルトのアクションを変更できません。

設定例

2 レート 3 カラー トラフィック ポリシングの設定を実行するには、以下を完全に行う必要があります。

1. 1 つ以上のインターフェイスに付加できるポリシー マップの作成または変更
2. ポリシーを作成または変更する必要があるトラフィック クラスの指定
3. パケット マーキングの指定
4. 2 レート トラフィック ポリシングの設定
5. 入力インターフェイスへのポリシー マップの適用

```
Router# configure
Router(config)# policy-map policy1
Router(config-pmap)# class ipv4-7
Router(config-pmap-c)# set qos-group 4
Router(config-pmap-c)# police rate percent 20 burst 100000 bytes peak-rate percent 50
peak-burst 200000 bytes
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface HundredGigE 0/6/0/18
Router(config-if)# service-policy input policy1
Router(config-if)# commit
```

実行コンフィギュレーション

```
policy-map policy1
  class ipv4-7
    set qos-group 4
    police rate percent 20 burst 100000 bytes peak-rate percent 50 peak-burst 200000 bytes
  !
!

interface HundredGigE 0/6/0/18
  service-policy input policy1
!
```

確認

```
Router# show policy-map interface HundredGigE 0/6/0/18
```

```

NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000220 -- input policy
NPU Id:                               3
Total number of classes:               8
Interface Bandwidth:                   100000000 kbps
Accounting Type:                       Layer1 (Include Layer 1 encapsulation and above)
-----
Levell Class                           =   ipv4-4
- - -
- - -
Levell Class                           =   ipv4-7
New qos group                          =   4

Policer Bucket ID                      =   0x102a3
Policer Stats Handle                   =   0x8a8089e8
Policer committed rate                  =   19980000 kbps (20 %)
Policer peak rate                      =   49860000 kbps (50 %)
Policer conform burst                  =   99584 bytes (100000 bytes)
Policer exceed burst                   =   199168 bytes (200000 bytes)

Levell Class                           =   class-default

Policer Bucket ID                      =   0x102a7
Policer Stats Handle                   =   0x8a7c8510
Policer committed rate                  =   29880000 kbps (30 %)
Policer conform burst                   =   4194304 bytes (default)

```

関連項目

- [2つのレートを使用したポリシング機能 \(42 ページ\)](#)

関連コマンド

- [police rate](#)

モジュラ QoS 輻輳管理のリファレンス

認定バースト

police コマンドの認定バースト (bc) パラメータでは、トラフィックを測定するためにルータが使用する 1 番目の適合 (緑色) トークンバケットが実装されます。bc パラメータにより、このトークンバケットのサイズが設定されます。最初は、トークンバケットは一杯の状態で、トークンカウントは認定バーストサイズ (CBS) と同じです。その後、メーターは、認定情報レート (CIR) によって示された秒単位の回数だけトークンカウントを更新します。

次に、メーターが適合トークンバケットを使用してパケットを送信する仕組みについて説明します。

- パケットが着信したときに、適合トークンバケットに十分なトークンがある場合、メーターはパケットを緑色でマーキングし、パケットのバイト数だけ適合トークンカウントをデクリメントします。

- 適合トークンバケットの使用可能なトークンが不十分な場合は、メーターにより、トラフィックフローは必要なトークンを借りてパケットを送信できます。メーターはパケットのバイト数の超過トークンバケットをチェックします。超過トークンバケットに使用可能な十分な数のトークンがある場合、メーターはパケットをマーキングします。

緑色：適合トークンカウントを最小値の0に達するまでデクリメントします。

黄色：超過トークンバケットから必要な残りのトークンを借り、最小値の0に達するまで、借りたトークン数だけ超過トークンカウントをデクリメントします。

- 使用可能なトークンの数が不十分な場合、メーターはパケットを赤色としてマーキングし、適合トークンカウントまたは超過トークンカウントをデクリメントしません。



(注) メーターが特定のカラーでパケットをマーキングするときには、そのカラーのトークンがパケット全体に対応するのに十分な数である必要があります。したがって、緑色のパケットの量が、認定情報レート (CIR) および認定バーストサイズ (CBS) よりも少なくなることはありません。特定のカラーのトークンは、そのカラーのパケットに対して常に使用されます。

超過バースト

`police` コマンドの超過バースト (`be`) パラメータでは、トラフィックを測定するためにルータが使用する2番目の超過 (黄色) トークンバケットが実装されます。最初は、超過トークンバケットは一杯の状態、トークンカウントは超過バーストサイズ (EBS) と同じです。その後、メーターは、認定情報レート (CIR) によって示された秒単位の回数だけトークンカウントを更新します。

次に、メーターが超過トークンバケットを使用してパケットを送信する仕組みについて説明します。

- 最初のトークンバケット (適合バケット) が認定バーストサイズ (CBS) を満たしている場合は、メーターにより、トラフィックフローは必要なトークンを超過トークンバケットから借りることができます。メーターはパケットを黄色としてマーキングしてから、パケットのバイト数だけ超過トークンバケットをデクリメントします。
- 借りるために必要なトークンが超過トークンバケットにない場合、メーターはパケットを赤色としてマーキングし、適合トークンバケットまたは超過トークンバケットをデクリメントしません。代わりに、メーターは `police` コマンドで設定した `exceed` アクションを実行します (たとえば、ポリサーがパケットをドロップするなど)。

2 レートポリサーの詳細

認定トークンバケットは、オーバーフローする前には認定バースト (bc) のサイズまでのバイト数を保持できます。次に説明するように、このトークンバケットは、CIR に適合しているか、または CIR を超過しているかを判断するトークンを保持しています。

- 一定時間での平均バイト数により認定トークンバケットがオーバーフローしない場合、トラフィックストリームは適合しています。この場合、トークンバケットアルゴリズムはトラフィックストリームを緑色でマーキングします。
- トラフィックストリームにより認定トークンバケットが最大トークンバケットにオーバーフローした場合、トラフィックストリームは超過しています。この場合、トークンバケットアルゴリズムはトラフィックストリームを黄色でマーキングします。トラフィックがポリシングレートを超過している間は、最大トークンバケットが満たされた状態になります。

最大トークンバケットは、オーバーフローする前にはピークバーストサイズ (be) までのバイト数を保持できます。このトークンバケットは、パケットが PIR に違反しているかを判断するトークンを保持しています。トラフィックストリームにより最大トークンバケットがオーバーフローした場合、トラフィックストリームは違反しています。この場合、トークンバケットアルゴリズムはトラフィックストリームを赤色でマーキングします。

たとえば、250 kbps のレートでデータストリームが 2 レートポリサーに着信した場合に、CIR が 100 kbps、PIR が 200 kbps の場合、ポリサーはパケットを次のようにマーキングします。

- 100 kbps はレートに適合
- 100 kbps はレートを超過
- 50 kbps はレートに違反

ルータは認定トークンバケットと最大トークンバケットの両方のトークンを次のように更新します。

- ルータは、パケットがインターフェイスに着信するたびに認定トークンバケットを CIR 値で更新します。認定トークンバケットには、認定バースト (bc) 値まで含めることができます。
- ルータは、パケットがインターフェイスに着信するたびに最大トークンバケットを PIR 値で更新します。最大トークンバケットには、ピークバースト (be) 値まで含めることができます。
- 着信パケットが CIR に適合した場合、ルータはパケットに対して適合アクションを実行し、そのパケットのバイト数だけ認定トークンバケットと最大トークンバケットの両方をデクリメントします。
- 着信パケットが CIR を超過した場合、ルータはパケットに対して confirm アクションを実行し、そのパケットのバイト数だけ認定トークンバケットをデクリメントし、パケットのオーバーフローバイト数だけ最大トークンバケットをデクリメントします。

- 着信パケットがPIRを超過した場合、ルータはパケットに対して違反アクションを実行しますが、最大トークンパケットをデクリメントしません。

[2つのレートを使用したポリシング機能 \(42 ページ\)](#) を参照してください。



第 4 章

リンクバンドルの QoS

バンドルは、1つ以上のポートグループを集約し、1つのリンクとして扱うようにしたものです。ルータは、イーサネットインターフェイスと VLAN インターフェイス（バンドルサブインターフェイス）のバンドルをサポートしています。物理インターフェイスで現在サポートされているすべての QoS 機能は、すべてのリンクバンドルインターフェイスでもサポートされています。バンドルメンバーへの QoS の適用はサポートされていません。

リンクバンドルの制約事項

- イーサネットリンクのバンドリングのみがサポートされています。
- バンドルインターフェイスには、物理インターフェイスのみを含めることができます。
- 1つのバンドル内のすべてのリンクは、802.3ad (LACP) または EtherChannel (非 LACP) のいずれかを実行するように設定する必要があります。1つのバンドル内の混合リンクはサポートされません。
- イーサネットリンクバンドルでは MAC アカウンティングはサポートされていません。
- 各リンクバンドルでサポートされるリンクの最大数は 64 です。
- サポートされるリンクバンドルの最大数は 128 です。
- [ロードバランシング \(49 ページ\)](#)
- [リンクバンドルでの QoS の設定 \(50 ページ\)](#)

ロードバランシング

ロードバランシング機能は、ルータのレイヤ3ルーティング情報に基づいて、複数のリンクにトラフィックを分散する転送メカニズムです。ルータがバンドル内のリンクの1つを介してパケットを配信できる場合、ルータでサポートされるのは宛先別のロードバランシングのみです。宛先別ロードバランシングがイネーブルの場合、使用可能なリンクが複数ある場合でも、特定の送信元/宛先のペア間のすべてのパケットが同じリンクを通過します。つまり、宛先別ロードバランシングでは特定の送信元/宛先のペアに対するパケットが順々に着信するようになります。

リンクバンドルのレイヤ3ロードバランシング

リンクバンドルのレイヤ3ロードバランシングは、パケットのIPv4送信元および宛先アドレスに基づいて、イーサネットフローポイント（EFP）で実行されます。レイヤ3サービス固有のロードバランシングが設定されている場合、すべての出力バンドルはIPv4送信元および宛先アドレスに基づいてロードバランシングされます。パケットにIPv4アドレスがない場合は、デフォルトのロードバランシング（パケットヘッダーのMAC SA/DAに基づく）が使用されます。

リンクバンドルでのQoSの設定

QoSは、個々のインターフェイスに設定する方法と同じ方法でリンクバンドルに設定されます。

ガイドライン

- QoSポリシーがバンドルに適用される場合（入力または出力方向）、ポリシーはそれぞれのメンバインターフェイスに適用されます。シェーパーまたは帯域幅の値の計算に使用する参照帯域幅は、物理メンバインターフェイスの帯域幅に従って適用されます。
- QoSポリシーがバンドルインターフェイスに適用されない場合、入力および出力両方のトラフィックがリンクメンバポートごとにデフォルトキューを使用します。
- バンドルポリシーマップで指定されたシェーピングレートは、すべてのバンドルメンバを集約したものではありません。バンドルに適用されたシェーピングレートは、リンクのロードバランシングによって異なります。たとえば10 Mbpsのシェーピングレートのポリシーマップが2つのメンバリンクを持つバンドルに適用され、トラフィックが常に同じメンバリンクにロードバランシングされると、全体で10 Mbpsのレートがバンドルに適用されます。ただし、トラフィックが2つのリンクの間で均等にロードバランシングされている場合、バンドルの全体的なシェーピングレートは20 Mbpsになります。
- メンバがバンドルから削除されると、分離したリンクに属している統計情報が失われるので、全体のバンドル統計情報が変わります。
- バンドルに適用されているQoSポリシーはそのすべてのメンバリンクに継承され、シェーパー/帯域幅の計算に使用した参照帯域幅はバンドル全体ではなく、物理メンバインターフェイスの帯域幅に従って適用されます。

設定例

リンクバンドルでQoS設定を完了するには、以下を完全に行う必要があります。

1. クラスマップの作成
2. ポリシーマップの作成とそれぞれのクラスマップの指定
3. トラフィックに対するアクションタイプの指定

ステップ 1、2 および 3 の詳細については、[トラフィック ポリシーのインターフェイスへの適用 \(7 ページ\)](#) を参照してください。

4. リンクバンドルの作成
5. リンクバンドルへのトラフィックポリシーの適用

```
/* Configure Ether-Bundle and apply traffic policy */
Router(config)# interface Bundle-Ether 12000
Router(config-if)# mtu 9100
Router(config-if)# service-policy input ingress
Router(config-if)# service-policy output egress
Router(config-if)# ipv4 address 100.12.0.0 255.255.255.254
Router(config-if)# bundle maximum-active links 64
Router(config-if)# commit
```

実行コンフィギュレーション

次の例では、トラフィックポリシーがどのようにイーサネットリンクバンドルに適用されるかを示します。ポリシーは、イーサネットリンクバンドルのメンバであるすべてのインターフェイスに適用されます。

```
/* Policy-map */

policy-map ingress
  class inet4-classifier-af1
    set qos-group 1
  !
  class inet4-classifier-af2
    set qos-group 2
  !
  class inet4-classifier-af3
    set qos-group 3
  !
  class inet4-classifier-af4
    set qos-group 4
  !
  class inet4-classifier-bel
    set qos-group 5
  !
  class inet4-classifier-nc1
    set qos-group 6
  !
  class class-default
  !
end-policy-map
!

/* Ether Bundle */
interface Bundle-Ether12000
  mtu 9100
  service-policy input ingress
  service-policy output egress
  ipv4 address 100.12.0.0 255.255.255.254
  load-interval 30
  flow ipv4 monitor FMM-V4 sampler SM ingress
  flow ipv6 monitor FMM-V6 sampler SM ingress
  flow mpls monitor FMM-MPLS sampler SM ingress
```

```

ipv4 access-group IPV4ACL_101 ingress
ipv6 access-group IPV6ACL_101 ingress
!

```

確認

- バンドルのステータスがUPであることを確認します。

```

router# show bundle bundle-ether 1200
Wed Dec 16 19:55:49.974 PST

```

```

Bundle-Ether12000

```

```

Status: Up
Local links <active/standby/configured>: 35 / 0 / 35
Local bandwidth <effective/available>: 3500000000 (3500000000) kbps
MAC address (source): ea3b.745f.c4b0 (Chassis pool)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 64
Wait while timer: 2000 ms
Load balancing: Default
LACP: Operational
  Flap suppression timer: Off
  Cisco extensions: Disabled
  Non-revertive: Disabled
mLACP: Not configured
IPv4 BFD: Not configured

```

Port	Device	State	Port ID	B/W, kbps
Hu0/4/0/0	Local	Active	0x8000, 0x0009	100000000
Link is Active				
Hu0/4/0/1	Local	Active	0x8000, 0x000a	100000000
Link is Active				

Hu0/4/0/35	Local	Active	0x8000, 0x002b	100000000
Link is Active				

- バンドルの統計情報を確認します。

```

router# show policy-map interface bundle-ether 12000

```

```

Bundle-Ether12000 input: ingress

```

```

Class inet4-classifier-af1
  Classification statistics
    Matched : 4647401962/21236124455654 26403040
    Transmitted : 4647401962/21236124455654 26403040
    Total Dropped : 0/0 0
Class inet4-classifier-af2
  Classification statistics
    Matched : 4502980177/20576584333939 25571493
    Transmitted : 4502980177/20576584333939 25571493
    Total Dropped : 0/0 0
Class inet4-classifier-af3
  Classification statistics
    Matched : 4647404125/21236213667880 26389086
    Transmitted : 4647404125/21236213667880 26389086
    Total Dropped : 0/0 0

```

```

Class inet4-classifier-af4
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :      9291188840/42456120548683      52771168
  Transmitted                    :      9291188840/42456120548683      52771168
  Total Dropped                  :                      0/0                      0
Class inet4-classifier-bel
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :      4647413429/21235847852686      26393414
  Transmitted                    :      4647413429/21235847852686      26393414
  Total Dropped                  :                      0/0                      0
Class inet4-classifier-ncl
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :      9294887621/42473100149807      52778258
  Transmitted                    :      9294887621/42473100149807      52778258
  Total Dropped                  :                      0/0                      0

Class class-default
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :                      0/0                      0
  Transmitted                    :                      0/0                      0
  Total Dropped                  :                      0/0                      0

Bundle-Ether12000 output: egress

Class c1
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :      16665494532/75878118942463      8760591
  Transmitted                    :      16655834643/75834136022017      8760591
  Total Dropped                  :           9659889/43982920446          0
  Queueing statistics
  Queue ID                       : None (Bundle)
  Taildropped(packets/bytes)     :      9659889/43982920446
Class c2
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :      16665421959/75877849543188      8718687
  Transmitted                    :      16665421959/75877849543188      8718687
  Total Dropped                  :                      0/0                      0
  Queueing statistics
  Queue ID                       : None (Bundle)
  Taildropped(packets/bytes)     :      0/0
Class c3
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :      16665247833/75877509455458      8703470
  Transmitted                    :      16665187414/75877234624197      8703470
  Total Dropped                  :           60419/274831261          0
  Queueing statistics
  Queue ID                       : None (Bundle)
  Taildropped(packets/bytes)     :      60419/274831261
Class c4
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :      33330896131/151755393012945      17470745
  Transmitted                    :      33330745421/151754709368565      17470745
  Total Dropped                  :           150710/683644380          0
  Queueing statistics
  Queue ID                       : None (Bundle)
  Taildropped(packets/bytes)     :      150710/683644380
Class c5
  Classification statistics      (packets/bytes)      (rate - kbps)
  Matched                       :      16878910340/76849791869834      8833394
  Transmitted                    :      16878849464/76849514633309      8833394
  Total Dropped                  :           60876/277236525          0
  Queueing statistics
  Queue ID                       : None (Bundle)
  Taildropped(packets/bytes)     :      60876/277236525

```

```

Class c6
  Classification statistics          (packets/bytes)      (rate - kbps)
  Matched                          : 33330898844/151756094112925  17456785
  Transmitted                       : 33330752668/151755427708382  17456785
  Total Dropped                     : 146176/666404543              0
  Queueing statistics
  Queue ID                          : None (Bundle)
  Taildropped(packets/bytes)        : 146176/666404543
Class c7
  Classification statistics          (packets/bytes)      (rate - kbps)
  Matched                          : 244106/79922040              74
  Transmitted                       : 244106/79922040              74
  Total Dropped                     : 0/0                          0
  Queueing statistics
  Queue ID                          : None (Bundle)
  Taildropped(packets/bytes)        : 0/0
Class class-default
  Classification statistics          (packets/bytes)      (rate - kbps)
  Matched                          : 267075066180/1215993441123215  139917482
  Transmitted                       : 267075066180/1215993441123215  139917482
  Total Dropped                     : 0/0                          0
  Queueing statistics
  Queue ID                          : None (Bundle)
  Taildropped(packets/bytes)        : 0/0

```

関連項目

- [リンクバンドルの QoS \(49 ページ\)](#)

関連コマンド

- bundle maximu-active links
- interface Bundle-Ether



第 5 章

階層型モジュラ QoS の概要

階層型 QoS (H-QoS) では、トラフィック管理をより細かい粒度で実行する、複数のポリシーレベルで QoS 動作を指定できます。

H-QoS は入れ子構造のトラフィック ポリシーを使用してルータ インターフェイスに適用されます。最初のレベルのトラフィック ポリシーは親トラフィック ポリシーで、メイン インターフェイス レベルまたはサブインターフェイス レベルでのトラフィックの制御に使用されます。2 番目のレベルのトラフィック ポリシーは子トラフィック ポリシーで、特定のトラフィック ストリームまたはクラスを介した追加制御に使用されます。子トラフィック ポリシーは前もって定義したトラフィック ポリシーであり、**service-policy** コマンドを使用して親トラフィック ポリシー内で参照されます。

2 レベル H-QoS は、すべてのラインカード上の入力方向と出力方向の両方で、物理またはバンドルのメイン インターフェイスとサブインターフェイス上でサポートされています。

3 レベル階層型 QoS (H QoS) は、クラス/サービス、グループ/イーサネットフロー ポイント (EFP)、およびポート レベルの SLA の適用を可能にします。サブインターフェイスに通常の 2 レベルの出力 H QoS ポリシーを適用して、子および親レベルでクラスおよび EFP Sla を実現できます。さらに、メイン インターフェイスにポート シェーパ ポリシーを適用して、1 + 2 の H-QoS モデルまたは 3 レベル H-QoS モデルで集約されたポート レベル SLA を実現できます。

重要な点として、リリース 6.6.25 (3 レベル H-QoS 機能が導入された) 前は、メイン インターフェイスでクラスデフォルトシェーパを適用すると、メイン インターフェイスを通過するトラフィックのみに適用されていたことに注意してください。3 レベル H-QoS を使用すると、メイン インターフェイスに適用されるクラスデフォルトシェーパはポートシェーパと見なされ、その物理ポートから発信されるすべてのトラフィックに適用されます。3 レベル H-QoS の利点は、サブインターフェイス上の親シェーパがオーバーサブスクライブできることです。これにより、第 3 レベルで集約ポートシェーパのベスト エフォート共有が可能になります。

- [H-QoS 設定の制約事項 \(56 ページ\)](#)
- [階層型キューイングの設定 \(57 ページ\)](#)

H-QoS 設定の制約事項

次に、H-QoS 設定時に適用される制約事項を示します。

1. 親トラフィック ポリシーのみが **class-default** タイプのトラフィック クラスをサポートしています。
2. 親トラフィック ポリシーは、クラス アクション **shape** のみをサポートしており、他のキューイング アクションは設定できません。
3. ルータでの設定時に、子トラフィック ポリシー内でプライオリティクラスにトラフィック シェーパを必ず使用してください。
4. 子ポリシーの総帯域幅は、親ポリシーのトラフィック シェーパ未満にする必要があります。
5. 輻輳回避と管理のため、親トラフィック ポリシー内のトラフィック シェーパでキュー制限とドロッププライオリティを計算します。
6. PBTS 機能は、H-QoS プロファイルが有効になっているときは動作しません。これは、TCAM の制限によるものです。
7. 適用されている QoS ポリシーがなくても、システムがサポートするバンドルサブインターフェイスは最大 896 のみです。これは、バンドルサブインターフェイスの HQoS プロファイルモードでの内部 LAG_ID リソース消費によるもので、QoS ポリシーが適用されていても、適用されていなくても同じです。
8. 7つの優先度レベルがサポートされているデフォルトモードとは異なり、HQoS プロファイルモードでサポートされる優先度レベルは最大 4 つのみです。また、以前は非 H-QoS プロファイルモードで 7つのレベルのプライオリティが使用されていましたが、物理およびバンドルのメインインターフェイスのポリシーにもこの制約が適用されます。
9. 同じポリシーマップでの帯域幅と残存帯域幅の設定は同時にサポートされません。また、クラスに帯域幅 (CIR) がある場合、他のクラスにも帯域幅設定のみが必要です。クラスマップに残存帯域幅のパーセンテージ率 (EIR) がある場合、他のクラスにも残存帯域幅設定のみが必要です。シェーピングは、任意のクラスに適用されます。
10. プライオリティクラスには、シェーピング設定を使用してレート制限を設定する必要があります。効果的なシェーパ値は、優先帯域幅予約として取得します。すべてのサブインターフェイスとメインインターフェイスにわたる優先帯域幅予約の合計は、ネットワーク インターフェイス (NIF) ポート速度を超過してはなりません。これは、ネットワーク インターフェイスポート全体にわたる優先度が高いトラフィックによるオーバーサブスクリプションを防ぐためです。

非プライオリティクラスと親のシェーピングのレートはオーバーサブスクライブの状態でもかまいません。

11. 帯域幅または残存帯域幅の比率 (BRR) の粒度は、非HQoS モードの 1:4096 と比べると 1:64 となります。そのため、使用した値に基づく帯域幅のパフォーマンスに精度差があることが考えられます。

次に、3 レベル H-QoS 設定時に適用される制約事項を示します。

- EFP 親レベルでの帯域幅アクションはサポートされていません。すべての EFP/サブインターフェイス ポリシーではポートシェーパを正当に共有できます。
- 3 レベル H-QoS は、入力ポリシーまたは出力マーキング ポリシーには適用されません。
- メイン インターフェイスで **clear qos counters** を実行すると、メイン インターフェイス ポリシーの統計情報のみがクリアされます。すべてのサブインターフェイスの統計情報をクリアするには「all」オプションを使用します。または、サブインターフェイス ポリシーの統計情報を個別にクリアします。
- メイン インターフェイス ポリシーの統計情報にはサブインターフェイスの packets/byte counters は反映されませんが、ポートシェーパは特定の物理インターフェイスのすべての論理ポートに適用されます。サブインターフェイス ポリシーマップの統計情報には、送信済みおよびドロップされた packets/byte counters の post-queueing の適用が反映されます。

階層型キューイングの設定

H-QoS を設定する前に、H-QoS プロファイルをルータ上で有効にする必要があります。H-QoS プロファイルを有効にした後に、次の設定に示すように、ルータをリロードする必要があります。

```
Router# configure
Router(config)# hw-module profile qos hqos-enable
Router(config)# commit
Router# reload
```

階層化キューイングの設定に含まれているステップは次のとおりです。

1. クラスマップを設定します。
2. 前のステップで設定したクラスマップを使用して子トラフィック ポリシーを設定します。
3. 親トラフィック ポリシーを設定して、そのポリシー内に子トラフィック ポリシーを追加します。



- (注) デフォルトのクラスマップサイズ (32) プロファイルが RSP4 で使用されている場合、サブインターフェイスでサポートされているポリシーマップのスケールは、RSP3 でサポートされているスケールと比較すると小さくなります。RSP4 でサブインターフェイス ポリシーマップのスケールを大きくするには、**hw-module profile qos max-classmap-size** を使用してポリシーマップごとに 4 つのクラスマップを設定します。

親トラフィックポリシーはH-QoSポリシーであり、物理またはバンドルのメインインターフェイスおよびサブインターフェイスに適用できます。

設定例

クラスマップの設定は次のとおりです。

```
Router# configure
Router(config)# class-map match-any tc2
Router(config-cmap)# match traffic-class 1
Router(config-cmap)# end-class-map
Router(config)# commit
```

子トラフィック ポリシーの設定は次のとおりです。

```
Router# configure
Router(config)# policy-map child
Router(config-pmap)# class tc2
Router(config-pmap-c)# shape average percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 1
Router(config-pmap)# end-policy-map
Router(config)# commit
```

親トラフィック ポリシーの設定は次のとおりです。

```
Router# configure
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# service-policy child
Router(config-pmap-c)# shape average percent 50
Router(config-pmap)# end-policy-map
Router(config)# commit
```

実行コンフィギュレーション

```
/* Configuration of a Class-map */
class-map match-any tc2
  match traffic-class 1
end-class-map
!
/* Configuration of a Child Traffic Policy */
policy-map child
  class tc2
    shape average percent 20
  !
```



```

class class-default
  shape average percent 1
!
end-policy-map
!
/* Configuration of a Parent Traffic Policy */
policy-map parent
  class class-default
    service-policy child
    shape average percent 50
  !
end-policy-map
!

```

メインインターフェイスでの親トラフィック ポリシーの適用

```

Router# configure
Router(config)# Interface TenGigE 0/0/0/10
Router(config-int)# service-policy output parent
Router(config-int)# commit

```

サブインターフェイスでの親トラフィック ポリシーの適用

```

Router# configure
Router(config)# Interface TenGigE 0/0/0/10.1
Router(config-int)# service-policy output parent
Router(config-int)# commit

```

確認

show qos interface interface-name output コマンドを使用して、H-QoS トラフィック ポリシーがインターフェイスに正しく適用されているかどうかを確認します。次の例では、**Level1 Class** が親トラフィック ポリシーに関連付けられているクラスマップに関する情報を提供し、**Level2 Class** が子トラフィック ポリシーに関連付けられているクラスマップに関する情報を提供します。

```
RP/0/RP0/CPU0:ios#show qos interface ten0/0/0/10 output
```

```

NOTE:- Configured values are displayed within parentheses
Interface TenGigE0/0/0/10 ifh 0x1e0 -- output policy
NPU Id: 0
Total number of classes: 3
Interface Bandwidth: 10000000 kbps
VOQ Base: 1136
Accounting Type: Layer1 (Include Layer 1 encapsulation and above)
-----

```

```

Level1 Class = class-default
Queue Max. BW. = no max (50 %)
Queue Min. BW. = 0 kbps (default)
Inverse Weight / Weight = 0 / (BWR not configured)
Level2 Class = tc2
Egressq Queue ID = 1138 (LP queue)
Queue Max. BW. = 1020015 kbps (20 %)
Queue Min. BW. = 0 kbps (default)
Inverse Weight / Weight = 1 / (BWR not configured)
Guaranteed service rate = 1000000 kbps
TailDrop Threshold = 1253376 bytes / 10 ms (default)
WRED not configured for this class

```

```

Level2 Class                = class-default
Egressq Queue ID           = 1136 (Default LP queue)
Queue Max. BW.             = 50625 kbps (1 %)
Queue Min. BW.             = 0 kbps (default)
Inverse Weight / Weight    = 1 / (BWR not configured)
Guaranteed service rate    = 50000 kbps
TailDrop Threshold         = 62720 bytes / 10 ms (default)
WRED not configured for this class

```

親および子のトラフィック ポリシーの異なるトラフィック クラスに一致したパケットの統計情報は、**show policy-map interface interface-name output** コマンドを使用して表示できます。また、このコマンドは、それぞれのトラフィック クラスに一致したパケットに指定したアクションが適用されたときに送信またはドロップされるパケットの数も表示します。

```
Router# show policy-map interface ten0/0/0/10 output
```

```

TenGigE0/0/0/10 output: parent
Class class-default
  Classification statistics          (packets/bytes)    (rate - kbps)
  Matched                          : 2313578823/296138089344  8494665
  Transmitted                       : 232805738/29799134464    854465
  Total Dropped                     : 2080773085/266338954880   7640200
Policy child Class tc2
  Classification statistics          (packets/bytes)    (rate - kbps)
  Matched                          : 2313578823/296138089344  8494665
  Transmitted                       : 232805738/29799134464    854465
  Total Dropped                     : 2080773085/266338954880   7640200
Queueing statistics
  Queue ID                          : 1138
  Taildropped(packets/bytes)        : 2080773085/266338954880
Policy child Class class-default
  Classification statistics          (packets/bytes)    (rate - kbps)
  Matched                          : 0/0 0
  Transmitted                       : 0/0 0
  Total Dropped                     : 0/0 0
Queueing statistics
  Queue ID                          : 1136
  Taildropped(packets/bytes)        : 0/0

```

階層型ポリシーを使用する場合、親ポリシーの統計情報を保存するための独立したハードウェアカウンタのセットはありません。代わりに、親ポリシーの統計情報は、同じポリシーマップにあるすべての子ポリシーの合計として、ソフトウェアで処理されます。

CoS 値が 1 および 2 の 2 つのトラフィックのストリームがそれぞれ 3.5 Gbps の速度で送信される次の例で、これを示します。

```

/*Hierarchical Policy Map Configuration*/
=====
Router# show running-config policy-map Hingress
policy-map Hingress
  class class-default
    service-policy ingress
    police rate 5 gbps peak-rate 9 gbps
  !
!
end-policy-map
!
/*Ingress Policy Map Configuration*/
=====
Router#show running-config policy-map ingress

```

```

policy-map ingress
  class cos1
    set traffic-class 1
    police rate 5 gbps
  !
  !
  class cos2
    set traffic-class 2
    police rate 5 gbps
  !
  !
  class class-default
  !
end-policy-map
!
/*Policy Map applied at TenGigE0/0/0/6.100 Interface*/
=====
Router#show policy-map interface tenGigE 0/0/0/6.100 input

TenGigE0/0/0/6.100 input: Hingress

Class class-default
  Classification statistics          (packets/bytes)      (rate - kbps)
  Matched                          :      856717937/109659895936      6683676
  Transmitted                       :      856717937/109659895936      6683676
  Total Dropped                     :                   0/0              0
  Policing statistics              (packets/bytes)      (rate - kbps)
  Policed(conform)                 :      856717937/109659895936      6683674
  Policed(exceed)                   :                   0/0              0
  Policed(violate)                  :                   0/0              0
  Policed and dropped               :                   0/0

Policy ingress Class cos1
  Classification statistics          (packets/bytes)      (rate - kbps)
  Matched                          :      437826303/56041766784      3341838
  Transmitted                       :      437826303/56041766784      3341838
  Total Dropped                     :                   0/0              0
  Policing statistics              (packets/bytes)      (rate - kbps)
  Policed(conform)                 :      437826303/56041766784      3341838
  Policed(exceed)                   :                   0/0              0
  Policed(violate)                  :                   0/0              0
  Policed and dropped               :                   0/0
  Policed and dropped(parent policer) : 0/0

Policy ingress Class cos2
  Classification statistics          (packets/bytes)      (rate - kbps)
  Matched                          :      418891634/53618129152      3341838
  Transmitted                       :      418891634/53618129152      3341838
  Total Dropped                     :                   0/0              0
  Policing statistics              (packets/bytes)      (rate - kbps)
  Policed(conform)                 :      418891634/53618129152      3341838
  Policed(exceed)                   :                   0/0              0
  Policed(violate)                  :                   0/0              0
  Policed and dropped               :                   0/0
  Policed and dropped(parent policer) : 0/0

Policy ingress Class class-default
  Classification statistics          (packets/bytes)      (rate - kbps)
  Matched                          :                   0/0              0
  Transmitted                       :                   0/0              0
  Total Dropped                     :                   0/0              0
Policy Bag Stats time: 0
Policy Bag Stats time: 0

```

3 レベル H-QoS の設定例

3 レベル H-QoS を設定するには、次の手順を実行します。

1. ポートシェーパまたは EFP グループシェーパを設定します。
2. EFP 親シェーパとクラスまたはサービスレベルのアクションを使用して 2 レベル H-QoS ポリシーを設定します。
3. メイン インターフェイスでポートシェーパまたは EFP グループシェーパを有効にしてルートポリシーにします。
4. 各 EFP インスタンスで 2 レベル H-QoS ポリシーを有効にします。これにより、サービス、EFP、EFP グループまたはポート SLA の 3 レベル階層が実現します。

次に、3 レベル H-QoS の設定例を示します。

```

policy-map port_shaper
  class class-default
    shape average 6 gbps
  !
end-policy-map
!

policy-map efp_policy
  class class-default
    service-policy efp_policy_child
    shape average 4 gbps
  !
end-policy-map

!

policy-map efp_policy_child
  class tc1
    shape average 50 mbps
    priority level 1
  !
  class tc2
    bandwidth percent 50
  !
  class tc3
    bandwidth percent 30
  !
  class class-default
  !
end-policy-map
!

interface TenGigE0/5/0/4
  service-policy output port_shaper
!

interface TenGigE0/5/0/4.1
  service-policy output efp_policy
  encapsulation dot1q 11
!

interface TenGigE0/5/0/4.2
  service-policy output efp_policy
  encapsulation dot1q 12
!

```

確認

XREEXEC モードで **show policy-map interface** コマンドを実行して、各サブインターフェイス/EFP ポリシーのパケット/バイトカウントとレートポストポートシェーパの適用を表示します。

