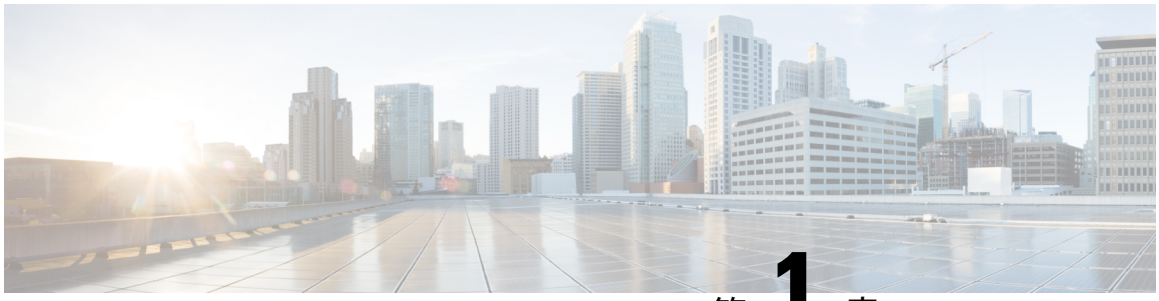
Cisco NCS 560 シリーズ ルータ（Cisco IOS XR リリース 7.0.x）モジュラ QoS コンフィギュレーション ガイド

初版：2019 年 8 月 30 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/

目 次



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、分類する必要の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

- **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		入力
MPLS Experimental Topmost	（0、7）	8	あり		入力
Access-group	該当なし		なし	該当なし	入力
QoS-group	（1、7）	7	なし	なし	出力
				あり	入力
プロトコル			あり	該当なし	入力

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。

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。
- 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の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。

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
```

「実行コンフィギュレーション （7 ページ）」も参照してください。

「確認 （7 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 （4 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。クラスの一致規則は、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	（「パケットマーキング （7 ページ）」を参照）。
police	入力
priority	出力（レベル 1）
shape	出力

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 （6 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. 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
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. クラスアクションの指定（「トラフィックポリシーの要素 （4 ページ）」を参照）

「実行コンフィギュレーション （7 ページ）」を参照してください。

「確認 （7 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 （4 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

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。

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 （5 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 （4 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

パケットマーキング

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。出力の**discard-class**の一致（設定されている場合）は、マーキングポリシーにのみ使用できます。

また、ルータは L2 入力マーキングもサポートしています。

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 cos	0 ～ 7	入力	なし
set dei	0 ～ 1	入力	なし
set discard-class	0 ～ 3	入力	なし
set dscp	0 ～ 63	入力	なし
set mpls experimental topmost	0 ～ 7	入力	なし
set precedence	0 ～ 7	入力	なし
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合した後、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重み付けランダム早期検出（WRED）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。

（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。

出力方向での L3 フローにおけるイーサネットパケットの QoS L2 再マーキング

ルータは、出力方向でのレイヤ3フローにおける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。

- ピアリングモードを有効にします。これを行うには、**hw-module profile qos ingress-model peering** コマンドを使用します。hw-module設定を機能させるには、ルータをリロードする必要があります。詳細については、『Modular QoS Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers』を参照してください。
- 出力インターフェイスでのマーキングのポリシーマップを設定します。
- **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。

制約事項とその他の重要なポイント

出力方向でのレイヤ 3 フローにおけるイーサネットパケットのレイヤ 2 マーキングを設定する前に、次のポイントを確認しておいてください。

- **set discard-class** は、ピアリングモードを使用した入力ポリシーではサポートされていません。
- 出力マーキングの統計情報は使用できません。
- レイヤ 2（802.1p）出力マーキングは、IP から IP、IP から MPLS、および MPLS から IP へのトラフィックのレイヤ 3 フローでサポートされています。
- 出力方向でのレイヤ 3 フローにおけるイーサネットパケットのレイヤ 2 マーキングは、ピアリングモードでのみサポートされます。

実行コンフィギュレーション

入力ポリシー：

最初に、入力で qos-group を設定する必要があります。

```
class-map match-any Class0
 match mpls experimental topmost 0
 match precedence routine
 match dscp 0-7
 end-class-map
class-map match-any Class1
 match mpls experimental topmost 1
 match precedence priority
 match dscp 8-15
 end-class-map
class-map match-any Class2
 match mpls experimental topmost 2
 match precedence immediate
 match dscp 16-23
 end-class-map
class-map match-any Class3
 match mpls experimental topmost 3
 match precedence flash
 match dscp 24-31
 end-class-map
class-map match-any Class4
 match mpls experimental topmost 4
 match precedence flash-override
 match dscp 32-39
 end-class-map
class-map match-any Class5
 match mpls experimental topmost 5
 match precedence critical
 match dscp 40-47
 end-class-map
class-map match-any Class6
 match mpls experimental topmost 6
 match precedence internet
 match dscp 48-55
 end-class-map
class-map match-any Class7
 match mpls experimental topmost 7
 match precedence network
```

```
 match dscp 56-63
 end-class-map
!

policy-map ncs_input
 class Class7
  set traffic-class 7
  set mpls experimental imposition 7
  set qos-group 7
!
 class Class6
  set traffic-class 6
  set mpls experimental imposition 6
  set qos-group 6
!
 class Class5
  set traffic-class 5
  set mpls experimental imposition 5
  set qos-group 5
!
 class Class4
  set traffic-class 4
  set mpls experimental imposition 4
  set qos-group 4
 !
 class Class3
  set traffic-class 4
  set mpls experimental imposition 3
  set qos-group 3
 !
 class Class2
  set traffic-class 2
  set mpls experimental imposition 2
  set qos-group 2
 !
 class Class1
  set traffic-class 2
  set mpls experimental imposition 1
  set qos-group 1
 !
 class Class0
  set traffic-class 0
  set mpls experimental imposition 0
  set qos-group 0
 !
 end-policy-map
!
```

出力ポリシー：

出力で、次のコマンドを実行してパケットをマークします。

```
class-map match-any qos7
match qos-group 7
 end-class-map
!
class-map match-any qos6
match qos-group 6
 end-class-map
!
class-map match-any qos5
match qos-group 5
 end-class-map
!
class-map match-any qos4
```

```
match qos-group 4
 end-class-map
!
class-map match-any qos3
match qos-group 3
 end-class-map
!
class-map match-any qos2
 match qos-group 2
 end-class-map
!
class-map match-any qos1
match qos-group 1
 end-class-map
!

policy-map ncs_output
 class qos7
  set cos 7
  set dei 1
!
 class qos6
  set cos 6
  set dei 1
!
 class qos5
  set cos 5
  set dei 1
!
 class qos4
  set cos 4
  set dei 1
!
 class qos3
  set cos 3
  set dei 1
!
 class qos2
  set cos 2
  set dei 1

!
 class qos1
  set cos 1
  set dei 1
!
 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、絶対レートベースのポリシー、および時間ベースのポリシーがサポートされています。

詳細については、「リンク バンドルでの QoS の設定 （52 ページ）」を参照してください。

入力ショートパイプ

QoS トラフィックが MPLS ネットワークから送出されると、最後から 2 番目の入力ラベルスイッチルータ（LSR）で MPLS ラベルスタックが削除され、IPv4 または IPv6 パケットが転送されます。このディスポジションプロセスは MPLS EXP ビット（EXP またはパイプモード）によって実行され、パケットは Differentiated Services Code Point（DSCP; DiffServ コードポイント）または precedence 値でマークされます（DSCP または precedence ベースの分類とも呼ばれます）。

通常、QoS トラフィックは、パケットに MPLS ラベルがない場合にのみ、DSCP および precedence ベースの分類をサポートします。ただし、入力ショートパイプ機能を使用すると、IPv4 または IPv6 ヘッダーのタイプオブサービス（ToS）フィールドを使用して、1 つの MPLS ラベルを含むパケットを分類できます。この分類方法は、入力ショートパイプと呼ばれます。この方法で IP パケットを分類するには、次の手順を実行する必要があります。

1. 子クラスマップを作成します。
2. 子クラスマップで ToS 値を指定します。
3. 子クラスマップを親クラスマップに付加します。
4. 親クラスマップを含むポリシーマップを作成します。
5. トラフィッククラスや QoS グループなどの入力アクションを設定します。

入力ショートパイプ機能を使用すると、トラフィックパケットの可視性が向上します。さらに、この機能により、IPv4 または IPv6 ネットワークに着信する MPLS パケットの分類の制限もなくなります。

制約事項とその他の重要なポイント

入力ショートパイプ機能を設定する前に、次のポイントを確認しておいてください。

- この機能は、トラフィックパケットに 1 つの MPLS ヘッダーがある場合にのみ動作します。複数の MPLS ヘッダーがある場合、入力ショートパイプ機能は動作しません。たとえば、ディスポジション時に 2 つのラベルがある明示的ヌルの場合、この機能は動作しません。
- 入力分類は、MPLS EXP ビット（EXP またはパイプモード）分類または DSCP および precedence（ショートパイプ）分類のいずれかを使用して実行できます。分類方法が混在しないようにしてください。混在していると、不明な動作が発生し、分類がまったく機能しない可能性があります。
- この機能は、L3VPN でのみサポートされており、L2VPN ではサポートされていません。
- この機能は、通常の IPv4 および IPv6 トラフィックでは動作しますが、MPLS を介した IPv6 VPN プロバイダーエッジ（6VPE）では動作しません。

- 親クラスマップに追加できる子クラスマップは 1 つだけです。
- この機能は、同じ親クラスマップのショートパイプおよびレガシー DSCP 分類の呼び出しをサポートします。
- 子クラスマップには、match precedence コマンドと match dscp コマンドのみを含めることができます。
- この機能はピアリングモードではサポートされません。

入力ショートパイプの設定

ここでは、入力ショートパイプ機能の設定例と、同じ親クラスにあるラベル付きパケットとラベルなしパケットの分類を設定する別の例について詳しく説明します。

IPv4 または IPv6 ヘッダーのタイプオブサービス（ToS）フィールドを使用して、1 つの MPLS ラベルを含むパケットを分類する設定例（入力ショートパイプ方式）：

```
class-map match-any in_pipe
 match mpls disposition class-map child_pipe
end-class-map
!
class-map match-any child_pipe
 match precedence 1
match dscp ipv4 af11
 end-class-map
!
class-map match-any ingress-business-high
match dscp af21, af22
end

class-map match-any ingress-business-low
match dscp af11, af12
end

policy-map ingress-classifier
class in_pipe
set traffic-class 5
class ingress-business-high
set traffic-class 4
class ingress-business-low
set traffic-class 2
class class-default
set traffic-class 0
!
```

次の設定例のように、同じ親クラスにあるラベル付きパケットとラベルなしパケットの両方の分類を設定できます。この例では、MPLS ラベル付きパケットの場合は、子クラスで設定された DSCP が分類されますが、ラベルなしパケットの場合は、**match dscp <value>** ステートメントで設定された DSCP および ToS が分類されます。

```
class-map match-any in_pipe
match mpls disposition class-map child_pipe  (labeled case)
match dscp af11 (non-labeled case)
end-class-map
!
class-map match-any child_pipe
match precedence 1
```

```
match dscp ipv4 af11
end-class-map
!
class-map match-any ingress-business-high
match dscp af21, af22
end

class-map match-any ingress-business-low
match dscp af11, af12
end

policy-map ingress-classifier
class in_pipe
set traffic-class 5
class ingress-business-high
set traffic-class 4
class ingress-business-low
set traffic-class 2
class class-default
set traffic-class 0
!
```

関連コマンド

- match mpls disposition class-map

選択的出力ポリシーベースのキューマッピング

選択的出力ポリシーベースのキューマッピングを使用すると、出力時にさまざまな順列でトラフィッククラス（TC）マップを組み合わせることができます。

（注） モジュラ型シャーシはこの機能をサポートしていません。

出力 TC（トラフィッククラス）マッピングを導入する主な目的は、1 つのポリシーを使用して入力のトラフィックを分類し、トラフィッククラスを割り当てることによって、分類されたトラフィックをキューに配置することです。出力では、TC のさまざまなグループ化をサポートできます。

各顧客が申し込んださまざまなサービスレベル契約（SLA）に基づいて、一部の TC をリアルタイム（RT）トラフィックのプライオリティキューにグループ化し、その他の TC を保証帯域幅（BW）トラフィックにグループ化し、残りをベストエフォート（BE）型トラフィック配信にグループ化することができます。

3 人の顧客が次の要件に基づいてこれらのサービスを購入した場合の例を考えてみましょう。

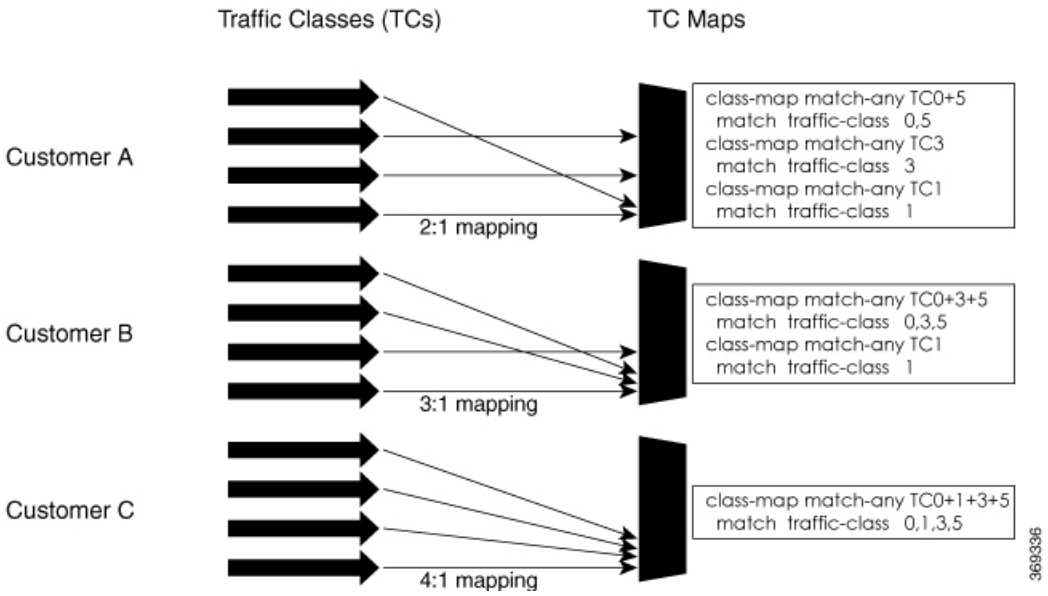
- 顧客 A：RT トラフィック、予約 BW トラフィック、および BE 型トラフィック配信が必要です。
- 顧客 B：予約 BW トラフィックおよび BE 型トラフィック配信が必要です。
- 顧客 C：BE 型トラフィック配信のみが必要です。

選択的出力ポリシーベースのキューマッピングを使用して、次のように3つのプロファイルを作成できます。

- 顧客A：プライオリティキューRTトラフィック（TC1）、保証BWトラフィック（TC3）、ベストエフォート型トラフィック（TC0、TC5）
- 顧客B：保証BWトラフィック（TC1）、ベストエフォート型トラフィック（TC0、TC3、TC5）
- 顧客C：ベストエフォート型トラフィック（TC0、TC1、TC3、TC5）

出力TCマッピングを使用して、プロバイダーとのSLAに基づいて顧客ごとに使用できる3種類のプロファイルを作成できます。

図 *1*：選択的出力ポリシーベースのキューマッピングを使用した *SLA* に基づく顧客プロファイルの作成



制約事項とその他の重要なポイント

選択的出力ポリシーベースのキューマッピング機能を設定する前に、次のポイントを確認しておいてください。

- 1 つの PM（ポリシーマップ）には、1 つの TC（トラフィッククラス）マッピングクラスのみを設定できます。
- マッピングされたクラスで使用した TC を、同じ PM にあるマッピングされていないクラスで使用することはできません。
- プラットフォームごとに最大 3 つの一意の TC マッピング PM またはプロファイルを設定できます。
- すべての TC マッピングクラスで、範囲値に **traffic-class 0** を含める必要があります。

- TC マッピングの範囲は 0 ～ 5 です。
- TC マッピングクラスが PM に存在する場合、クラスデフォルトはダミークラスになります。つまり、クラスデフォルトの統計情報と QoS 値は適用されません。
- TC マッピングクラスにはすべてのクラスデフォルトの制限が適用されます。たとえば、TC マッピングクラスで **priority** コマンドを設定することはできません。

（注） TC マッピング PM またはプロファイルは、TC マッピングクラスを含む PM です。

TC マッピングクラスの例：

match traffic-class 0 1 2 3

TC のマッピングされていないクラスの例：

match traffic-class 1

選択的出力ポリシーベースのキューマッピングの設定

ここでは、選択的出力ポリシーベースのキューマッピング機能の設定例と、この機能の動作を示すための使用例について詳しく説明します。

設定例

```
policy-map tc_pmap
class tc1
  shape average percent 10
 !
 class tc035
  shape average percent 1
 !
 class class-default
!
 end-policy-map
!
 class-map match-any tc035
match traffic-class 0 3 5
 end-class-map
!
```

確認

show qos interface コマンドと **show policy-map interface** コマンドを実行します。

ポリシーマップ内に TC マッピングクラスが存在する場合、クラスデフォルトの値は計算されません。

show qos interface bundle-Ether 44 の出力例

```
NOTE:- Configured values are displayed within parentheses
NPU Id:                        0
Total number of classes:       3
Interface Bandwidth:           100000000 kbps
Policy Name:                   tc_pmap
```

```
Accounting Type:              Layer1 (Include Layer 1 encapsulation and above)
------------------------------------------------------------------------------
Level1 Class                                =   tc1

Level1 Class                                =   tc035

Level1 Class                                =   class-default

Interface HundredGigE0/0/0/30 Ifh 0xf000208 (Member) -- output policy
NPU Id:                       0
Total number of classes:      3
Interface Bandwidth:          100000000 kbps
Policy Name:                  tc_pmap
VOQ Base:                     1264
Accounting Type:              Layer1 (Include Layer 1 encapsulation and above)
------------------------------------------------------------------------------
Level1 Class                                =   tc1
Egressq Queue ID                            =   1265 (LP queue)
Queue Max. BW.                              =   10063882 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)
WRED not configured for this class

Level1 Class                                =   tc035
Egressq Queue ID                            =   1264 (LP queue)
Queue Max. BW.                              =   1011732 kbps (1 %)
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

Level1 Class                                =   class-default
Queue Max. BW.                              =   no max (default)
Queue Min. BW.                              =   0 kbps (default)
Inverse Weight / Weight                     =   0 / (BWR not configured)
```

show policy-map interface bundle-Ether 44 の出力例

```
Bundle-Ether44 output: tc_pmap

Class tc1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :             429444/53823648             0
    Transmitted         :             429444/53823648             0
    Total Dropped       :                   0/0                   0
  Queueing statistics
    Queue ID                             : None (Bundle)
    Taildropped(packets/bytes)           : 0/0
Class tc035
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            1288331/161470820            0
    Transmitted         :            1288331/161470820            0
    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             :                   0/0                   0
    Transmitted         :                   0/0                   0
    Total Dropped       :                   0/0                   0
```

```
  Queueing statistics
    Queue ID                                : None (Bundle)
    Taildropped(packets/bytes)              : 0/0
Policy Bag Stats time: 1557216940000  [Local Time: 05/07/19 08:15:40.000]
RP/0/RP0/CPU0:BB1#
```

使用例

同じ一致基準を満たす入力トラフィックにより、出力トラフィックを最大 3 つの一意の TC マッピングプロファイルにグループ化できます。この機能を使用すると、顧客が申し込んだ SLA に基づいて、顧客に差別化サービスを提供できます。

次の例では、入力ポリシーマップによって、0 ～ 5 のトラフィッククラスの入力一致基準が設定されています。SLA に基づいて、出力 PM で TC 値をグループ化して差別化サービスを提供できます。

TC 値をグループ化した後、そのクラスに特定の出力アクションを適用できます。

入力一致：

```
class EXP1
  set traffic-class 1
!
class EXP2
  set traffic-class 2
!
class EXP3
  set traffic-class 3
!
class EXP4
  set traffic-class 4
!
class EXP5
  set traffic-class 5
!
class class-default
!
end-policy-map
!
```

出力一致：

ポリシーマップ PM1 の TC マッピングクラスの例

```
class-map match-any TC2:1
match traffic-class 0 1
end-class-map
```

ポリシーマップ PM2 の TC マッピングクラスの例

```
class-map match-any TC3:1
match traffic-class 0 1 2
end-class-map
```

ポリシーマップ PM3 の TC マッピングクラスの例

```
class-map match-any TC6:1
match traffic-class 0 1 2 3 4 5
end-class-map
```

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
Route(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
Route(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。

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と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と、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と、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。

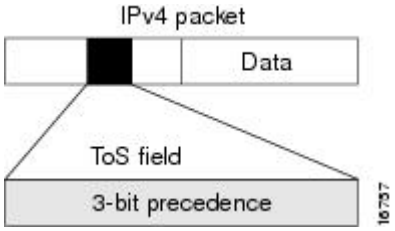
モジュラ QoS サービスパケットの分類の参照

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 *2: 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ので、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

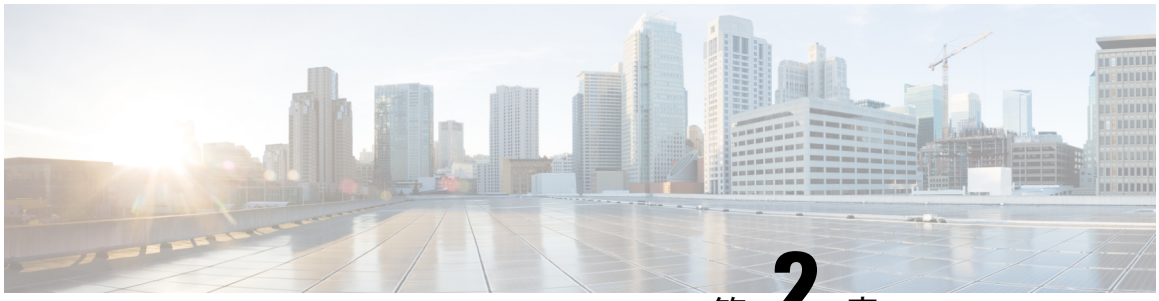
ルータは、各出力インターフェイスで最大 8 つの CoSQ をサポートしています。範囲は 0 ～ 7 で、0 はデフォルトの CoSQ です。**qos-group** 値は、CoSQ と最終的には仮想出力キュー（VOQ）を選択するために使用されます。

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 prec1
set traffic-class 1
then, class-map tc1
match traffic-class 1
then,
policy-map test-egress
class tc1
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 （27 ページ）
- ランダム早期検出と TCP （29 ページ）
- 重み付けランダム早期検出 （31 ページ）

- テール ドロップと FIFO キュー （27 ページ）
- ランダム早期検出と TCP （29 ページ）
- 重み付けランダム早期検出 （31 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

クラスの一致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 （27 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. 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. 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
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. 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 （29 ページ）

関連コマンド

- random-detect

重み付けランダム早期検出

重み付けランダム早期検知（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、キューの前回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。

average = (old_average * (1-2 -x)) + (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

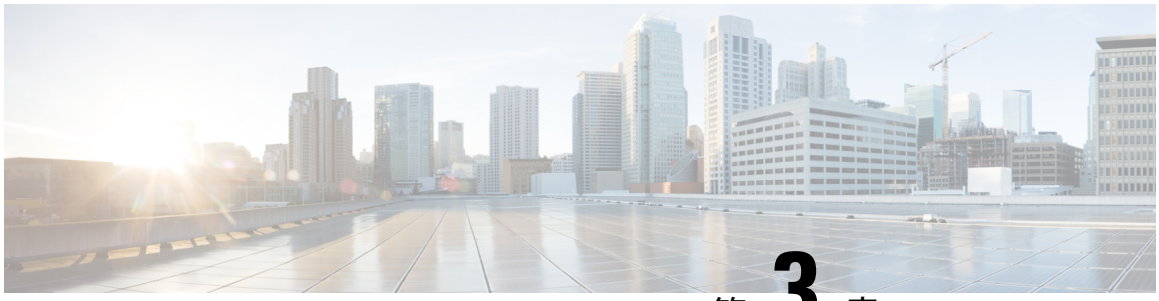
```
Router# show qos int hundredGigE 0/6/0/18 output

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

- 重み付けランダム早期検出 （31 ページ）
- ランダム早期検出の設定 （29 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。

- 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 （38 ページ）
- トラフィック シェーピング （39 ページ）
- トラフィック ポリシング （40 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

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、 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 （35 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

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 のみがサポートされています。
- 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。

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. 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
Router(config-pmap)# class qos1
Router(config-pmap-c)# priority level
Router(config-pmap-c# exit
Router(config-pmap)# exit
```

```
Router(config)# interface
Router(config-if)# service-policy output
Router(config-if)# no shutdown
Router(config-if)# commit
```

実行コンフィギュレーション

確認

関連コマンド

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。

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
Router(config-pmap-c# exit
Router(config-pmap)# exit
Router(config)# interface
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

確認

関連項目

- 輻輳管理の概要 （35 ページ）

関連コマンド

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す。

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 （41 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 （41 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。

認定バースト

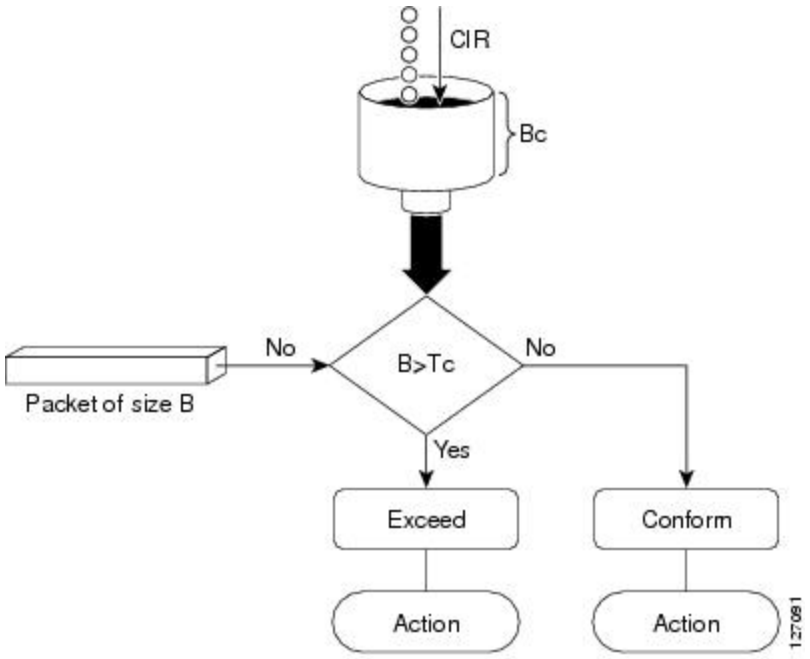
トラフィック シェーパーとは異なり、トラフィック ポリサーは超過パケットをバッファせず、後で送信します。代わりに、ポリサーはバッファリングせずに「送信または送信なし」のポリシーを実行します。ポリシングは、通常のバースト値または認定バースト（bc）値を使用して、ルータが設定された設定情報レート（CIR）に到達できるようにします。ポリシングは、設定したバースト値に基づいて、パケットが CIR に適合しているか、または CIR を超過しているかを決定します。バースト パラメータは、ルータの一般的なバッファリング ルールに基づいており、ラウンドトリップ時間のビットレートと同じになるようにバッファリングを設定して、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、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。

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 *3:* 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、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、異なるアクションが実行されます。

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
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                                =   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)

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 （40 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 （40 ページ）

関連コマンド

- police rate

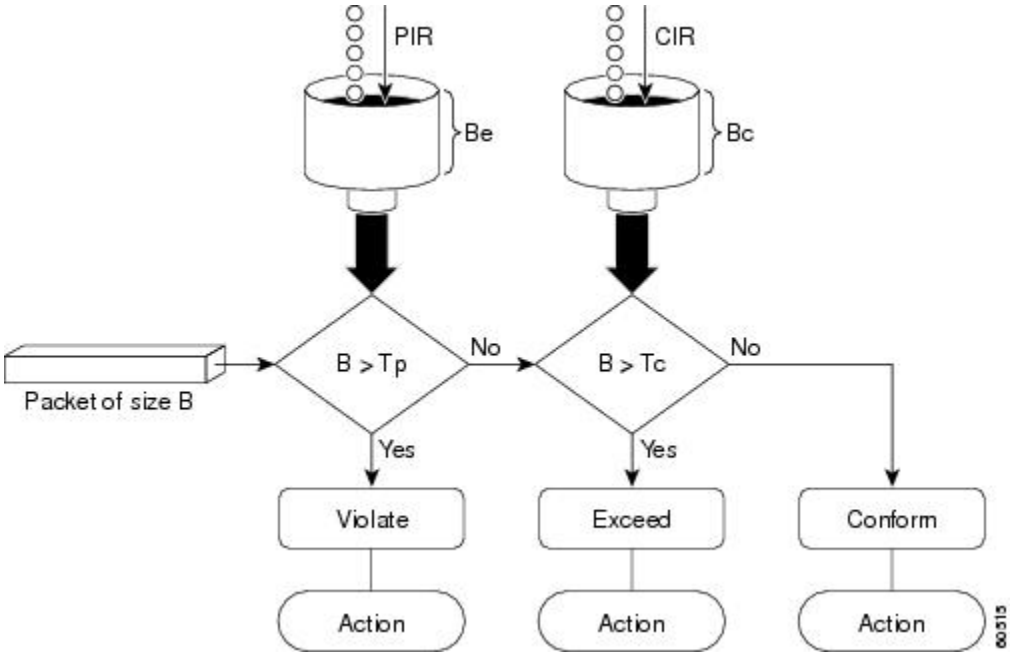
2 つのレートを使用したポリシング機能

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。

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 *4:* 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 （49 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)
------------------------------------------------------------------------------
Level1 Class                                =   ipv4-4
- - -
- - -
Level1 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)

Level1 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 （45 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で、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、メートルは 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。

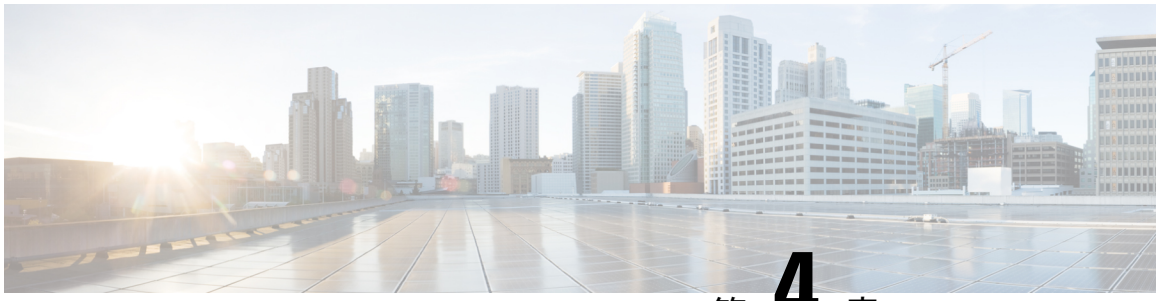
- 100 kbps はレートに適合

- 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 バ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 （45 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。

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 （6 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

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。

確認

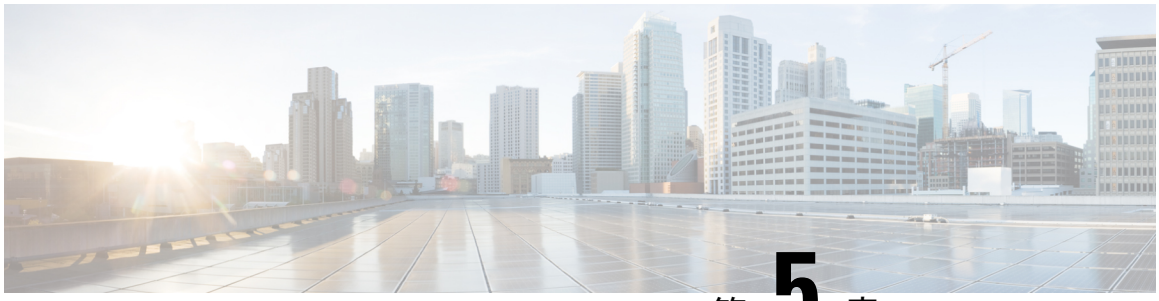
- バンドルのステータスが UP であることを確認します。

関連項目

- リンク バンドルの QoS （51 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 シェーパー 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 シェーパーを適用すると、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 シェーパーはポート シェーパーと見なされ、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ー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 シェーパーのベスト 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 シェーパー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 シェーパー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 シェーパー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。効果的なシェーパー値は、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 シェーパー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パケット/バイトカウンタは反映されませんが、ポートシェーパー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パケット/バイト カウントのポストポート シェーパー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、ルータをリロードします。

```
Router# configure
Router(config)# hw-module profile qos hqos-enable
Router(config)# commit
Router# reload
Router# admin
sysadmin-vm:0_RP0# hw-module location all 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
```

階層型ポリサーを使用する場合、親ポリサ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、親ポリサーの統計情報は、同じポリシーマップにあるすべての子ポリサーの合計として、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 シェーパーまたは EFP グループ シェーパーを設定します。
2. EFP 親シェーパー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 シェーパーまたは EFP グループ シェーパー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

XR EXEC 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ーの適用を表示します。