



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。

- [トラフィック クラスの要素 \(1 ページ\)](#)
- [トラフィック ポリシーの要素 \(4 ページ\)](#)
- [ACL を使用した QoS グループの設定 \(10 ページ\)](#)
- [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 \(13 ページ\)](#)
- [制約事項 \(16 ページ\)](#)
- [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 \(18 ページ\)](#)

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 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
- パケットを分類するための各種基準を指定するための、一連の **match** コマンド。
- 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、Cisco NCS 540 シリーズ ルータ Cisco NCS 540 シリーズ 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	○	○	入力
IPv4 Precedence IPv6 Precedence Precedence	(0, 7)	8	○	×	入力
MPLS Experimental Topmost	(0, 7)	8	○	×	入力
Access-group	N/A	8	×	N/A	入力
QoS-group	(1, 7)	7	×	×	出力
CoS	(0, 7)	8	×	○	入力
プロトコル	(0, 255)	1	○	N/A	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、出力に対応する **match qos-group x** を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 \(20 ページ\)](#) 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。

出力分類の場合、**qos-group** (1-7) での一致がサポートされます。一致 **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、指定していないフィールドの値に基づいて照合を行います。
- 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** を指定すると、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、IPv4 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ていません。

- **match access-group** コマンドの場合、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が、これらは出力方向でサポートされる唯一の一致条件です。
- 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。
-
-
-

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 \(1 ページ\)](#) 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 \(1 ページ\)](#)
- [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。

Cisco NCS 540 シリーズルータは、入力方向の（デフォルトのプロファイルで）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、Cisco NCS 540 シリーズルータ 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 (7 ページ) を参照)。
police	入力
priority	出力 (レベル 1) 出力 (レベル 1~レベル 7)
shape	出力

WRED は、**default** オプションおよび **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 \(6 ページ\)](#) 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 \(1 ページ\)](#)

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。



- (注) NCS 540 シリーズルータでは、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 \(5 ページ\)](#) 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 \(1 ページ\)](#)

関連コマンド

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。Cisco NCS 540 シリーズ ルータ Cisco NCS 540 シリーズ ルータは出力パケットマーキングのみをサポートしています (discard-class で使用する場合のみ)。

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、Cisco NCS 540 シリーズルータCisco NCS 540 シリーズルータで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	いいえ
set qos-group	0 ~ 7	入力	いいえ

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 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。の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

Cisco NCS 540 シリーズ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

Cisco NCS 540 シリーズルータは出力方向において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。



(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](#)を参照してください。

ACLを使用したQoSグループの設定

QoSグループを作成してACLを設定し、指定した一致条件に基づいてトラフィックをグループに分類できます。次の例では、QoSグループ値（0～511）で照合します。

前提条件

ACLを使用してQoSグループを設定する前に、QoSピアリングプロファイルをルータまたはラインカード上で有効にする必要があります。QoSピアリングを有効にした後に、次の設定に示すようにルータまたはラインカードをリロードする必要があります。

ルータ上でのQoSピアリングプロファイルの有効化

グローバルコンフィギュレーションモードを開始して、次のようにルータのQoSピアリングプロファイルを有効にします。

```

RP/0/RP0/CPU0:router(config)# hw-module profile qos ingress-model peering
RP/0/RP0/CPU0:router(config)# exit
RP/0/RP0/CPU0:router# reload

```

ラインカード上でのQoSピアリングプロファイルの有効化

グローバルコンフィギュレーションモードを開始して、次のようにラインカードの QoS ピアリングプロファイルを有効にします。

```
RP/0/RP0/CPU0:router(config)# hw-module profile qos ingress-model peering location 0/0/CPU0
RP/0/RP0/CPU0:router(config)# exit
RP/0/RP0/CPU0:router# reload location 0/0/CPU0
```

設定

次の一連の設定ステートメントを使用して、QoS グループで ACL を設定します。

```
/*
Enter the global configuration mode, and configure an ACL with the required QoS groups.
*/
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 access-list qos-acl
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 host 5.0.0.1 any set qos-group 1
RP/0/RP0/CPU0:router(config-ipv4-acl)# 11 permit ipv4 host 6.0.0.1 any set qos-group 2
RP/0/RP0/CPU0:router(config-ipv4-acl)# 12 permit ipv4 host 7.0.0.1 any set qos-group 3
RP/0/RP0/CPU0:router(config-ipv4-acl)# 13 deny ipv4 any any

/* Create a policy map with the required classes.
In this example, we also create a default class for traffic that does not belong to any
of the specified
classes. */
RP/0/RP0/CPU0:router(config)# policy-map qos-acl-map
RP/0/RP0/CPU0:router(config-pmap)# class qos1
RP/0/RP0/CPU0:router(config-pmap-c)# set dscp af43
RP/0/RP0/CPU0:router(config-pmap-c)# set traffic-class 2
RP/0/RP0/CPU0:router(config-pmap-c)# exit

RP/0/RP0/CPU0:router(config-pmap)# class qos2
RP/0/RP0/CPU0:router(config-pmap-c)# set precedence critical
RP/0/RP0/CPU0:router(config-pmap-c)# set traffic-class 7
RP/0/RP0/CPU0:router(config-pmap-c)# exit

RP/0/RP0/CPU0:router(config-pmap)# class qos3
RP/0/RP0/CPU0:router(config-pmap-c)# set precedence 2
RP/0/RP0/CPU0:router(config-pmap-c)# set traffic-class 2
RP/0/RP0/CPU0:router(config-pmap-c)# exit

RP/0/RP0/CPU0:router(config-pmap)# class qos4
RP/0/RP0/CPU0:router(config-pmap-c)# set traffic-class 4
RP/0/RP0/CPU0:router(config-pmap-c)# set dscp cs4
RP/0/RP0/CPU0:router(config-pmap-c)# exit

RP/0/RP0/CPU0:router(config-pmap)# class class-default
RP/0/RP0/CPU0:router(config-pmap-c)# police rate percent 20
RP/0/RP0/CPU0:router(config-pmap-c-police)# exit

/* Create the class maps for specifying the match conditions. */
RP/0/RP0/CPU0:router(config)# class-map match-any qos1
RP/0/RP0/CPU0:router(config-cmap)# match qos-group 1
RP/0/RP0/CPU0:router(config-cmap)# end-class-map

RP/0/RP0/CPU0:router(config)# class-map match-any qos2
RP/0/RP0/CPU0:router(config-cmap)# match qos-group 2
RP/0/RP0/CPU0:router(config-cmap)# end-class-map
```

```

RP/0/RP0/CPU0:router(config)# class-map match-any qos3
RP/0/RP0/CPU0:router(config-cmap)# match qos-group 3
RP/0/RP0/CPU0:router(config-cmap)# end-class-map

RP/0/RP0/CPU0:router(config)# class-map match-any qos4
RP/0/RP0/CPU0:router(config-cmap)# match qos-group 4
RP/0/RP0/CPU0:router(config-cmap)# end-class-map

/* Apply the access list and the QoS map to the Gigabit interface, and commit your
configuration. */
RP/0/RP0/CPU0:router(config)# interface TenGigE0/0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 12.0.0.1/24
RP/0/RP0/CPU0:router(config-if)# no shut
RP/0/RP0/CPU0:router(config-if)# service-policy input qos-acl-map
RP/0/RP0/CPU0:router

RP/0/RP0/CPU0:router(config-if)# commit
Tue Mar 28 10:23:34.106 IST

RP/0/0/CPU0:Mar 28 10:37:48.570 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : Interface
TenGigE0/0/1/0/0, changed state to Down
RP/0/0/CPU0:Mar 28 10:37:48.608 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : Interface
TenGigE0/0/1/0/0, changed state to Up

RP/0/RP0/CPU0:router(config-if)# exit

```

実行コンフィギュレーション

設定を確認します。

```

RP/0/RP0/CPU0:router(config)# show run
Tue Mar 28 10:37:55.737 IST

Building configuration...
!! IOS XR Configuration 0.0.0

ipv4 access-list qos-acl
10 permit ipv4 host 5.0.1.1 any set qos-group 1
11 permit ipv4 host 6.0.1.1 any set qos-group 2
12 permit ipv4 host 7.0.1.1 any set qos-group 3
13 deny ipv4 any any

class-map match-any qos1
match qos-group 1
end-class-map
!
class-map match-any qos2
match qos-group 2
end-class-map
!
class-map match-any qos3
match qos-group 3
end-class-map
!
class-map match-any qos4
match qos-group 4
end-class-map
!

policy-map qos-acl-map

```

```
class qos1
  set dscp af43
  set traffic-class 2
!
class qos2
  set precedence critical
  set traffic-class 7
!
class qos3
  set precedence 2
  set traffic-class 2
!
class qos4
  set traffic-class 4
  set dscp cs4
!
class class-default
  police rate percent 20
!
!
end-policy-map
!

interface TenGigE0/0/1/0/0
  service-policy input qos-acl-map
  ipv4 address 12.0.0.1 255.255.255.0
  ipv4 access-group qos-acl ingress compress level 3
!
```

QoS グループを使用して ACL を正常に設定しました。

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、Cisco NCS 540 シリーズ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。

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

QoS モード	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
標準	4	1024	2000
標準	8	512	1024
標準	16	256	512
標準	32	128	256
拡張	4	872	1744
拡張	8	436	872
拡張	16	218	436
拡張	32	109	218



(注) NCS 540 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。

例：デフォルト設定である標準（2 カウンタ モード）QoS モードでクラス マップサイズが 32 の場合、コアごとに入力ポリシーで 128 のインターフェイスを設定できます。

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。

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。

確認

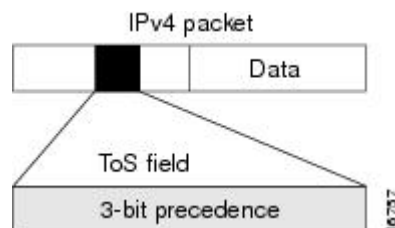
In-Place ポリシーの変更時に回復不可能なエラーが発生した場合は、ポリシーは対象のインターフェイスに対して矛盾した状態になります。コンフィギュレーションセッションのブロックが解除されるまで、新たな設定を行うことはできません。インターフェイスからポリシーを削除し、変更されたポリシーを確認し、それに応じて再適用することを推奨します。

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、Cisco NCS 540 シリーズルータ Cisco NCS 540 シリーズルータは IP precedence 値をそのままにします。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

Cisco NCS 540 シリーズ ルータ Cisco NCS 540 シリーズ 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 がデフォルトの 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
```

L3VPN トラフィックの MPLS 検出ビットの条件付きマーキング

MPLS 検出ビットの条件付きマーキングは、入力と出力のポリシーマップの組み合わせをプロバイダー エッジ（PE）ルータ上に適用することで、レイヤ 3 バーチャルプライベート ネットワーク（L3VPN）トラフィックに対して実行されます。入力ポリシーマップでは、**qos-group** または **discard-class** がポリシー アクションの結果に基づいて設定されるか、または暗黙的に設定されます。出力ポリシー マップは **qos-group** または **discard-class** で照合し、MPLS 検出ビットを対応する値に設定します。

L3VPN ネットワーク内の IPv4 トラフィックと IPv6 トラフィックの両方でこの機能がサポートされています。条件付きマーキングは、**in-contract** パケットと **out-of-contract** パケットに異なる MPLS 検出ビットをマークするために使用できます。**in-contract** パケットは、緑色の確認済パケットで、**discard-class** は 0 に設定されます。**out-of-contract** パケットは、制限を超過したパケットで、黄色で示され、**discard-class** は 1 に設定されます。

L3VPN トラフィックの MPLS 検出ビットの条件付きマーキングは、物理およびバンドルの両方のメイン インターフェイスとサブインターフェイスでサポートされています。

L3VPN の MPLS 検出ビットの条件付きマーキングの制約事項

1. 2 台の PE ルータが背面接続されており、ルータ間のトラフィックのラベルが BGP ラベルのみである場合は、明示的ヌル ラベルを設定する必要があります。

2. MPLS 検出ビットの条件付きマーキングを実行するポリシーマップは、Cisco NCS 5500 シリーズルータのネットワークプロセッサユニット (NPU) ごとに最大3つのポリシーマップを設定できます。
3. 入力ポリシーマップで qos-group を着信トラフィック パッケージに設定している場合、DSCP と MPLS の検出ビットの設定は機能しません。
4. 予想どおりの動作を得るには、入力ポリシーマップと出力ポリシーマップの両方を適用する必要があります。それらのいずれか1つが適用されていない場合は、未定義の動作になる可能性があります。
5. 出力ポリシーマップが qos-group または discard-class で一致せず、MPLS 検出ビットが必要な値に設定されている場合は、MPLS検出ビットはデフォルトで値ゼロに設定されます。

