QoS for IPv6 の実装

この章では、IPv6 環境に Quality of Service（QoS; サービス品質）機能を実装するための情報および作業について説明します。具体的には、IPv6 パケットへの Differentiated Service（DiffServ; ディファレンシエーテッド サービス）QoS 機能の適用について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「QoS for IPv6 を実装するための機能情報」（P.18）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

QoS for IPv6 の実装の前提条件

このマニュアルでは、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「その他の関連資料」の関連資料を参照してください。

QoS for IPv6 の実装の制約事項

次の QoS 機能は、IPv6 トラフィックの管理ではサポートされません。

- Compressed Real-Time Protocol（CRTP）
- Network-Based Application Recognition（NBAR）
- Committed Access Rate（CAR; 専用アクセス レート）
- Priority Queueing（PQ; プライオリティ キューイング）
- Custom Queueing（CQ）

プラットフォーム固有の情報および制約事項

IPv6 QoS は、Cisco IOS Release 12.0(28)S が稼動する Cisco 12000 シリーズ インターネット ルータ上でサポートされます。IPv6 QoS の機能の中には、Release 12.0(28)S でサポートされない機能もあります。これには、パケット分類などがあります。

QoS for IPv6 の実装に関する情報

IPv6 トラフィックの管理に使用できる QoS 機能に関する詳細については、次の各項を参照してください。

- 「QoS for IPv6 の実装方針」（P.2）
- 「IPv6 でのパケット分類」（P.3）
- 「IPv6 ネットワークでのポリシーおよびクラスベース パケット マーキング」（P.3）
- 「IPv6 ネットワークでの輻輳管理」（P.4）
- 「IPv6 トラフィックの輻輳回避」（P.4）
- 「IPv6 環境でのトラフィック ポリシング」（P.4）

QoS for IPv6 の実装方針

IPv6 パケットは、IPv4 パケットとは別のパスで転送されます。IPv6 環境でサポートされている QoS 機能には、パケット分類、キューイング、トラフィック シェーピング、Weighted Random Early Detection（WRED; 重み付けランダム早期検出）、クラスベース パケット マーキング、および IPv6 パケットのポリシングが含まれます。これらの機能は、IPv6 のプロセス スイッチング パスとシスコ エクスプレス フォワーディング スイッチング パスのどちらでも使用できます。

IPv6 環境で使用可能な QoS 機能はすべて、Modular QoS Command-Line Interface（CLI; コマンドライン インターフェイス）から管理します。Modular QoS CLI を使用すると、トラフィック クラスを定義し、トラフィック ポリシー（ポリシー マップ）を作成および設定してから、それらのトラフィック ポリシーをインターフェイスに対応付けることができます。

IPv6 が稼動しているネットワークに QoS を実装するには、IPv4 だけが稼動しているネットワークに QoS を実装する手順に従ってください。高度なレベルで QoS を実装するための基本手順は、次のとおりです。

1. QoS を必要とするネットワーク内のアプリケーションを特定します。
2. どの QoS 機能が適切であるかを判断するために、アプリケーションの特性を理解します。
3. 変更と転送がリンク レイヤ ヘッダー サイズに及ぼす影響を理解するために、ネットワーク トポロジについて理解します。
4. ネットワークに確立する基準に基づいて、クラスを作成します。具体的には、同じネットワークで IPv6 トラフィックとともに IPv4 トラフィックも伝送されている場合、IPv6 トラフィックと IPv4 トラフィックを同様に処理するか、それとも別の方法で処理し、それぞれに応じた一致基準を指定するかを決定します。両者を同様に処理する場合は、**match precedence**、**match dscp**、**set precedence**、**set dscp** などの match 文を使用します。両者を別の方法で処理する場合は、match-all クラス マップ内に **match protocol ip** や **match protocol ipv6** などの一致基準を追加します。
5. 各クラスにマーキングするためのポリシーを作成します。
6. QoS 機能を適用する際は、エッジからコアに向かって作業します。
7. トラフィックを処理するためのポリシーを構築します。
8. ポリシーを適用します。

IPv6 でのパケット分類

パケット分類は、プロセス スイッチング パスとシスコ エクスプレス フォワーディング スイッチング パスの両方で使用可能です。分類は、IPv6 precedence、Differentiated Services Control Point（DSCP）、および IPv6 アクセス リスト内に指定可能なその他の IPv6 プロトコル固有値に基づいて行うことができます。また、COS、パケット長、QOS グループなどのその他の IPv6 プロトコル固有でない値に基づいて行うこともできます。QoS を必要とするアプリケーションを決定したあとは、アプリケーションの特性に基づいてクラスを作成できます。さまざまな一致基準を使用して、トラフィックを分類できます。さまざまな一致基準を組み合せて、トラフィックを隔離、分離、および区別できます。

Modular QoS CLI（MQC）の機能拡張によって、IPv4 パケットと IPv6 パケットのどちらにも、precedence、DSCP、および IPv6 アクセス グループ値に基づく一致を作成できます。**match** コマンドを使用すると、IPv4 パケットと IPv6 パケットのどちらにも、DSCP 値および precedence に基づいて一致を作成できます。設定のガイドライン、および **match dscp** コマンドと **match precedence** コマンドの説明については、「IPv6 トラフィック フローを管理するための一致基準の使用」（P.6）を参照してください。

IPv6 ネットワークでのポリシーおよびクラスベース パケット マーキング

DSCP か precedence のどちらかを使用して、各トラフィック クラスを適切なプライオリティ値でマーキングするためのポリシーを作成できます。クラスベース マーキングを使用すると、トラフィック管理に対して IPv6 precedence および DSCP の値を設定できます。トラフィックは、ルータの入力インターフェイスに入るときにマーキングされます。このマーキングは、トラフィックがルータの出力インターフェイスを出るときに、トラフィックを処理（転送やキューイング）するために使用されます。トラフィックのマーキングと処理は、できるだけ送信元の近くで行ってください。

パケット マーキングには、**set dscp** コマンドおよび **set precedence** コマンドを使用します。これらのコマンドは、IPv4 トラフィックと IPv6 トラフィックの両方を処理するように変更されています。これらのコマンドを使用する際の設定ガイドラインについては、「IPv6 パケットのマーキング基準の指定」（P.5）を参照してください。

IPv6 ネットワークでの輻輳管理

トラフィックをマーキングしたあとは、そのマーキングを使用してポリシーを構築し、残りのネットワーク セグメントのトラフィックを分類できます。ポリシーを簡潔にしておく（4 クラスを越えないようにする）と、管理が容易になります。IPv6 では、クラスベース キューイングとフローベース キューイングがサポートされています。各種のキューイング オプションを設定するためにプロセスおよびタスクで使用されるコマンドおよび引数は、IP と IPv6 のどちらでも同じです。キューイング機能の設定および使用の手順については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

IPv6 トラフィックの輻輳回避

WRED は、Class-Based Weighted Fair Queueing（CBWFQ; クラスベース均等化キューイング）の制限を超える可能性のあるパケットに対して RED ベースのドロップ ポリシーを実装します。WRED では、（DSCP または precedence の値を使用する）クラスベース キューイングとフローベース キューイングをサポートしています。WRED コマンドは、何も変更しなくても IPv4 と IPv6 の両方に適用されます。

IPv6 環境でのトラフィック ポリシング

IPv6 での輻輳管理は、IP パケットでの輻輳管理の実装と似ています。また、IPv6 環境でキューイングおよびトラフィック シェーピング機能の設定に使用するコマンドは、IP で使用するコマンドと同じです。トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。トラフィック シェーピングでは、デフォルトでフローベース キューイングが使用されます。パケットの分類およびプライオリティ設定には、CBWFQ を使用できます。トラフィックのコンディショニングおよびポリシングには、Class-Based Policer と Generic Traffic Shaping（GTS）、または Frame Relay Traffic Shaping（FRTS; フレーム リレー トラフィック シェーピング）を使用できます。

IPv6 環境で使用するために、ポリシングの既存の設定やコマンド使用法を変更する必要はありませんが、**police** コマンドが拡張されたため、確認アクション、超過アクション、および違反アクションで次のキーワード オプションが使用されているとき、IPv4 パケットと IPv6 パケットの両方がマーキングされるようになりました。

- **set-dscp-transmit**
- **set-precedence-transmit**

QoS for IPv6 の実装方法

ここでは、一致基準を使用したトラフィックの分類方法と、一致基準を使用したトラフィック フローの管理方法について説明します。次の各項で構成されます。

- 「IPv6 ネットワークでのトラフィック分類の制約事項」（P.5）（必須）

- 「IPv6 パケットのマーキング基準の指定」（P.5）（必須）
- 「IPv6 トラフィック フローを管理するための一致基準の使用」（P.6）（必須）
- 「パケット マーキング基準の確認」（P.8）（任意）
- 「サービス ポリシーの確認」（P.13）（任意）

IPv6 ネットワークでのトラフィック分類の制約事項

match dscp コマンドと **match precedence** コマンドが変更されたこと、および IPv6 固有の **match access-group name** コマンドが追加されたことを除いて、**match** コマンドの機能は IPv4 と IPv6 のどちらでも同じです。

802.1Q（dot1Q）インターフェイス用の **set cos** コマンドと **match cos** コマンドは、シスコ エクスプレス フォワーディング スイッチド パケットに対してだけサポートされます。これらのオプションが使用されている場合、プロセス スイッチド パケット（ルータ生成パケットなど）はマーキングされません。

IPv6 パケットのマーキング基準の指定

ここでは、ネットワーク トラフィックを分類するためにあとでパケットのマッチングに使用される一致基準を確立します（つまり、パケットをマーキングします）。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}

   または

   set [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**policy map** *policy-map-name* **例：** `Router(config)# policy map policy1`	指定された名前を使用してポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。 • 作成するポリシー マップの名前を入力します。
ステップ 4	**class** {*class-name* | **class-default**} **例：** `Router(config-pmap)# class class-default`	指定されたクラス（またはデフォルト クラス）のトラフィックの処理を指定し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

ステップ 5	**set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}
	
	または
	
	set [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]}
	
	例：
	`Router(config-pmap-c)# set dscp cos table table-map1`
	
	または
	
	`Router(config-pmap-c)# set precedence cos table table-map1`
		precedence 値を設定します。
		• この例は、指定したテーブル マップ内で定義されている CoS 値（およびアクション）に基づいています。
		• 同じパケット内で precedence と DSCP の両方を変更することはできません。
		• 指定したテーブル マップ内で定義されている CoS 値（およびアクション）に基づいて、DSCP 値を設定します。

トラブルシューティングのヒント

シスコ エクスプレス フォワーディングがイネーブルになっていることを確認する

show cef interface、**show ipv6 cef**、**show ipv6 interface neighbors**、および **show interface statistics** コマンドを使用して、シスコ エクスプレス フォワーディングがイネーブルになっていることと、パケットがシスコ エクスプレス フォワーディングでスイッチングされていることを確認します。

パケットがシスコ エクスプレス フォワーディングでスイッチングされていることを確認する

show policy-map interface コマンドを使用して、インターフェイスごと、ポリシーごとのシスコ エクスプレス フォワーディングによるスイッチング統計情報を表示します。

IPv6 トラフィック フローを管理するための一致基準の使用

次の作業では、**match** コマンドを使用して、トラフィックを、確立したポリシーとマッチングする方法を示します。複数の match 文を使用できます。クラスのタイプに応じて、すべてのクラスとマッチングするか、それともいずれかのクラスとマッチングするかを指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map** {*class-name* | **class-default**}
4. **match precedence** *precedence-value* [*precedence-value precedence-value*]

または

match access-group name *ipv6-access-group*

または

match [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map** {*class-name* | **class-default**} **例：** `Router(config-pmap-c)# class cls1`	指定されたクラスを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。

ステップ 4	**match precedence** *precedence-value* [*precedence-value precedence-value*]
	
	または
	
	match access-group name *ipv6-access-group*
	
	または
	
	match [ip] dscp *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]
	
	例：
	`Router(config-pmap-c)# match precedence 5`
	
	または
	
	`Router(config-pmap-c)# match access-group name ipv6acl`
	
	または
	
	`Router(config-pmap-c)# match ip dscp 15`
		precedence 値とマッチングします。precedence は、IPv4 パケットと IPv6 パケットの両方に適用されます。
		
		または
		
		コンテンツ パケットがトラフィック クラスに属しているかどうかをチェックする IPv6 アクセス リストの名前を指定します。
		
		または
		
		特定の IP DSCP 値を一致基準として識別します。

例

次に、**match precedence** コマンドを使用して IPv6 トラフィック フローを管理する例を示します。

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
 Router(config)# class-m c1
  Router(config-cmap)# match precedence 5
  Router(config-cmap)# end
Router#
 Router(config)# policy p1
  Router(config-pmap)# class c1
  Router(config-pmap-c)# police 10000 conform set-prec-trans 4
```

パケット マーキング基準の確認

パケット マーキングが正常に行われることを確認するには、show policy コマンドを使用します。このコマンドの出力の注目すべき情報は、合計のパケット数とマーキングされたパケット数の差です。

```
Router# show policy p1

  Policy Map p1
    Class c1
      police 10000 1500 1500 conform-action set-prec-transmit 4 exceed-action drop

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface serial 4/1
Router(config-if)# service out p1
Router(config-if)# end

Router# show policy interface s4/1

 Serial4/1
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: precedence 5
      police:
        10000 bps, 1500 limit, 1500 extended limit
        conformed 0 packets, 0 bytes; action: set-prec-transmit 4
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps violate 0 bps

    Class-map: class-default (match-any)
      10 packets, 1486 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

show policy-map interface コマンド出力内のパケット カウンタの解釈

発信インターフェイスでの送信輻輳中、パケットは、インターフェイスが送信可能な速度より速く到達します。シスコの Modular QoS CLI で作成されたサービスポリシーの結果を監視する場合に役立つ **show policy-map interface** コマンドの出力の解釈方法を理解しておくと便利です。

輻輳は通常、高速な入力インターフェイスが相対的に低速な出力インターフェイスに供給する場合に発生します。一般的な輻輳ポイントは、LAN に面したイーサネット ポートおよび WAN に面したシリアル ポートを持つブランチオフィス ルータです。LAN セグメントのユーザが 10 Mbps のトラフィックを生成すると、それが 1.5 Mbps の帯域幅を持つ T1 に供給されます。

機能的には、輻輳の定義は、インターフェイス上で送信リングがいっぱいになることです（リングとは、特殊なバッファ制御構造のことです）。それぞれのインターフェイスは、1 対のリング、つまりパケット受信用の受信リングとパケット送信用の送信リングをサポートしています。リングのサイズは、インターフェイス コントローラやインターフェイスまたは Virtual Circuit（VC; 仮想回線）の帯域幅によって異なります。次の例に示すように、**show atm vc** *vcd* コマンドを使用して、PA-A3 ATM ポートアダプタ上の送信リングの値を表示します。

```
Router# show atm vc 3

ATM5/0.2: VCD: 3, VPI: 2, VCI: 2
VBR-NRT, PeakRate: 30000, Average Rate: 20000, Burst Cells: 94
AAL5-LLC/SNAP, etype:0x0, Flags: 0x20, VCmode: 0x0
OAM frequency: 0 second(s)
PA TxRingLimit: 10
InARP frequency: 15 minutes(s)
Transmit priority 2
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
OAM cells received: 0
OAM cells sent: 0
Status: UP
```

Cisco IOS（レイヤ 3 プロセッサとも呼ばれる）およびインターフェイス ドライバは、パケットを物理メディアに移動する際に送信リングを使用します。この 2 つのプロセッサは、次のように連携します。

- インターフェイスは、インターフェイス レートまたはシェイプド レートに応じてパケットを送信します。
- インターフェイスは、物理ワイヤへの送信を待機するパケットの格納場所であるハードウェア キューまたは送信リングを維持します。
- ハードウェア キューまたは送信リングがいっぱいになると、インターフェイスはレイヤ 3 プロセッサ システムへの明示的なバック プレッシャを提供します。インターフェイスは、送信リングがいっぱいになっているためインターフェイスの送信リングへのパケットのデキューを停止するようレイヤ 3 プロセッサに通知します。レイヤ 3 プロセッサは、超過パケットをレイヤ 3 キューに格納します。
- インターフェイスが送信リング上のパケットを送信してリングを空にすると、パケットを格納するために十分なバッファが再び利用可能になります。インターフェイスはバック プレッシャを解放し、レイヤ 3 プロセッサはインターフェイスへの新しいパケットをデキューします。

この通信システムの最も重要な側面は、インターフェイスが送信リングがいっぱいであることを認識し、レイヤ 3 プロセッサ システムからの新しいパケットの受信を制限するということです。したがって、インターフェイスが輻輳状態になった場合、ドロップの決定は、送信リングの First In, First Out（FIFO; 先入れ先出し）キュー内のランダムな後入れ先ドロップ決定から、レイヤ 3 プロセッサによって実装される IP レベルのサービス ポリシーに基づいたディファレンシエーテッド決定に移行されます。

パケット数および一致パケット数

サービス ポリシーは、レイヤ 3 キューに格納されているパケットにだけ適用されます。表 1 に、レイヤ 3 キューに格納されるパケットを示します。ローカルに生成されたパケットは常にプロセス スイッチド パケットとなり、インターフェイス ドライバに渡される前にまずレイヤ 3 キューに送信されます。ファスト スイッチド パケットおよびシスコ エクスプレス フォワーディング スイッチド パケットは、送信リングに直接送信され、送信リングがいっぱいになったときにだけレイヤ 3 キューに入れられます。

表 1　パケット タイプおよびレイヤ 3 キュー

パケット タイプ	輻輳	非輻輳
ローカルに生成されたパケット（Telnet パケットおよび ping を含む）	あり	あり
プロセス スイッチングが行われる他のパケット	あり	あり
シスコ エクスプレス フォワーディング スイッチングまたはファストスイッチングが行われるパケット	あり	なし

次の例では、これらのガイドラインが **show policy-map interface** コマンド出力に適用されています。4 つの主要なカウンタを太字で示しています。

```
Router# show policy-map interface atm 1/0.1

ATM1/0.1: VC 0/100 -
 Service-policy output: cbwfq (1283)
   Class-map: A (match-all) (1285/2)
    28621 packets, 7098008 bytes
     5 minute offered rate 10000 bps, drop rate 0 bps
     Match: access-group 101 (1289)
     Weighted Fair Queueing
       Output Queue: Conversation 73
       Bandwidth 500 (kbps) Max Threshold 64 (packets)
       (pkts matched/bytes matched) 28621/7098008
       (depth/total drops/no-buffer drops) 0/0/0
   Class-map: B (match-all) (1301/4)
     2058 packets, 148176 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
     Match: access-group 103 (1305)
     Weighted Fair Queueing
       Output Queue: Conversation 75
       Bandwidth 50 (kbps) Max Threshold 64 (packets)
       (pkts matched/bytes matched) 0/0
       (depth/total drops/no-buffer drops) 0/0/0
   Class-map: class-default (match-any) (1309/0)
     19 packets, 968 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: any  (1313)
```

表 2 に、例に太字で示されているカウンタを定義します。

表 2　show policy-map interface 出力内のパケット カウンタ

カウンタ	説明
28621 packets, 7098008 bytes	クラスの基準に一致するパケットの数。このカウンタは、インターフェイスが輻輳しているかどうかにかかわらず、増分します。
(pkts matched/bytes matched) 28621/709800	インターフェイスが輻輳していたときの、クラスの基準に一致するパケットの数。つまり、インターフェイスの送信リングがいっぱいになり、ドライバと L3 プロセッサ システムが連携して、サービス ポリシーが適用される L3 キューに超過パケットを入れました。プロセス スイッチド パケットは常に L3 キューイング システムを通過するため、「一致パケット」カウンタが増分することになります。
Class-map: B (match-all) (1301/4)	これらの番号は、CISCO-CLASS-BASED-QOS-MIB Management Information Base（MIB; 管理情報ベース）で使用される内部 ID を定義します。現行リリースの Cisco IOS では、この値は **show policy-map** コマンド出力に表示されません。
5 minute offered rate 0 bps, drop rate 0 bps	この値を変更し、より瞬間的な値にするには、**load-interval** コマンドを使用します。最小値は 30 秒ですが、**show policy-map interface** コマンド出力に表示される統計情報は、10 秒ごとに更新されます。このコマンドは特定の瞬間におけるスナップショットを提供するため、統計情報はキュー サイズの一時的な変更を反映していないことがあります。

輻輳がない場合、超過パケットをキューイングする必要はありません。輻輳が発生した場合、パケット（シスコ エクスプレス フォワーディング スイッチド パケットおよびファスト スイッチド パケットを含む）は、レイヤ 3 キューに入れられる可能性があります。輻輳管理機能を使用する場合、インターフェイスに累積されるパケットは、インターフェイスがそれらのパケットを送信するように解放されるまでキューイングされます。そのあと、割り当てられた優先順位およびインターフェイスに対して設定されたキューイング メカニズムに従ってスケジュールされます。

通常、パケット カウンタの方が、一致パケット カウンタよりもはるかに大きくなります。2 つのカウンタの値がほぼ等しい場合、インターフェイスが大量のプロセス スイッチド パケットを受信しているか、または重度に輻輳しています。確実に最適なパケット転送を行うために、この両方の条件を調査する必要があります。

カンバセーション番号の割り当て

ルータは、サービス ポリシーが適用されたときに作成されたキューに対してカンバセーション番号を割り当てます。次に、キューおよび関連情報を表示する例を示します。

```
Router# show policy-map interface s1/0.1 dlci 100

      Serial1/0.1: DLCI 100 -
      output : mypolicy
       Class voice
         Weighted Fair Queueing
```

```
     Strict Priority
     Output Queue: Conversation 72
       Bandwidth 16 (kbps) Packets Matched 0
      (pkts discards/bytes discards) 0/0
Class immediate-data
 Weighted Fair Queueing
     Output Queue: Conversation 73
       Bandwidth 60 (%) Packets Matched 0
       (pkts discards/bytes discards/tail drops) 0/0/0
       mean queue depth: 0
       drops: class  random   tail     min-th   max-th   mark-prob
              0      0        0        64       128      1/10
              1      0        0        71       128      1/10
              2      0        0        78       128      1/10
              3      0        0        85       128      1/10
              4      0        0        92       128      1/10
              5      0        0        99       128      1/10
              6      0        0        106      128      1/10
              7      0        0        113      128      1/10
              rsvp   0        0        120      128      1/10
Class priority-data
 Weighted Fair Queueing
     Output Queue: Conversation 74
       Bandwidth 40 (%) Packets Matched 0 Max Threshold 64 (packets)
       (pkts discards/bytes discards/tail drops) 0/0/0
Class class-default
 Weighted Fair Queueing
     Flow Based Fair Queueing
     Maximum Number of Hashed Queues 64  Max Threshold 20 (packets)
```

各クラスに対して報告される情報には、次のものが含まれます。

- クラス定義
- 適用されるキューイング方式
- 出力キュー カンバセーション番号
- 使用されている帯域幅
- 廃棄されたパケット数
- 廃棄されたバイト数
- ドロップされたパケット数

class-default クラスは、トラフィックが、ポリシー マップ内にポリシーが定義されている他のクラスの一致基準を満たしていない場合に、そのトラフィックが誘導される宛先のデフォルト クラスです。**fair-queue** コマンドを使用すると、IP フローをソートおよび分類するダイナミック キューの数を指定できます。あるいは、ルータは、インターフェイスまたは VC 上の帯域幅から導出したデフォルトのキュー数を割り当てます。いずれの場合も、サポートされる値は 2 の累乗（16 ～ 4096 の範囲）です。

表 3 に、インターフェイスおよび ATM Permanent Virtual Circuit（PVC; 相手先固定接続）のデフォルト値を示します。

表 3　インターフェイス帯域幅の関数としてのデフォルトのダイナミック キュー数

帯域幅範囲	ダイナミック キューの数
64 kbps 以下	16
64 kbps より大きく、128 kbps 以下	32
128 kbps より大きく、256 kbps 以下	64

表 3　インターフェイス帯域幅の関数としてのデフォルトのダイナミック キュー数（続き）

帯域幅範囲	ダイナミック キューの数
256 kbps より大きく、512 kbps 以下	128
512 kbps より大きい	256

表 4 に、ATM PVC 帯域幅に関連するデフォルトのダイナミック キュー数を示します。

表 4　ATM PVC 帯域幅の関数としてのデフォルトのダイナミック キュー数

帯域幅範囲	ダイナミック キューの数
128 kbps 以下	16
128 kbps より大きく、512 kbps 以下	32
512 kbps より大きく、2000 kbps 以下	64
2000 kbps より大きく、8000 kbps 以下	128
8000 kbps より大きい	256

WFQ に予約されているキューの数に基づいて、Cisco IOS ソフトウェアは、表 5 に示すようにカンバセーションまたはキューの番号を割り当てます。

表 5　キューに割り当てられたカンバセーション番号

番号	トラフィックのタイプ
1 ～ 256	一般的なフローベースのトラフィック キュー。ユーザが作成したクラスに一致しないトラフィックは、class-default およびフローベースのキューの 1 つに一致します。
257 ～ 263	Cisco Discovery Protocol（CDP; シスコ検出プロトコル）用、および内部の高プライオリティ フラグでマーク付けされたパケット用に予約されています。
264	プライオリティ クラス（priority コマンドで設定されたクラス）用に予約されているキュー。**show policy-map** interface の出力で、クラスの「Strict Priority」値を確認してください。プライオリティ キューでは、ダイナミック キューに 8 を加算した数値に等しいカンバセーション ID が使用されます。
265 以上	ユーザ作成クラス用のキュー。

サービス ポリシーの確認

この作業では、一致パケット カウンタおよびサービス ポリシーをテストします。トラフィック フローがポリシーの入力パラメータまたは出力パラメータに一致することを確認します。たとえば、FTP サーバからファイルをダウンロードすると、受信方向に輻輳が発生します。これは、サーバが大きい MTU サイズのフレームを送信し、クライアント PC が小さい Acknowledgment（ACK; 確認応答）を返すためです。

この作業の開始前に、大きいサイズの ping および多数の ping を使用した拡張 ping で輻輳をシミュレートします。また、FTP サーバから大きいサイズのファイルのダウンロードを試行します。そのファイルは「障害となる」データであり、インターフェイス帯域幅をいっぱいにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface atm slot/0.***subinterface-number* **{multipoint | point-to-point}**
4. **ip address ip-address mask** [*secondary*]
5. **pvc** [*name*] *vpi*/*vci* [**ces** | **ilmi** | **qsaal** | **smds**]
6. **tx-ring-limit** *ring-limit*
7. **service-policy** {**input** | **output**} *policy-map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface atm slot/0.** *subinterface-number* {**multipoint** | **point-to-point**} **例：** `Router(config)# interface atm 1/0.1 point-to-point}`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address ip-address mask** [*secondary*] **例：** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	テストするインターフェイスの IP アドレスを指定します。
ステップ 5	**pvc** [*name*] *vpi*/*vci* [**ces** | **ilmi** | **qsaal** | **smds**] **例：** `Router(config-if)# pvc cisco 0/5`	ATM PVC に名前を作成または割り当てます。任意で、ATM PVC にカプセル化タイプを指定し、インターフェイス ATM-VC コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**tx-ring-limit** *ring-limit* **例：** `Router(config-if-atm-vc)# tx-ring-limit 10`	インターフェイスの送信リングのサイズを縮小します。この値を小さくすると、Cisco IOS ソフトウェアでの QoS の使用が加速されます。 • 2600 および 3600 シリーズ ルータの場合は、リング制限をパケット数として指定します。7200 および 7500 シリーズ ルータの場合は、メモリ パーティクル数として指定します。
ステップ 7	**service-policy** {**input** | **output**} *policy-map-name* **例：** `Router(config-if-atm-vc)# service-policy output policy9`	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。 • 一致パケット カウンタはキューイング機能の一部であり、出力方向に対応付けられたサービス ポリシーに対してだけ使用できることに注意してください。

QoS for IPv6 を実装するための設定例

ここでは、次の設定例について説明します。

- 「シスコ エクスプレス フォワーディング スイッチングの確認：例」（P.15）
- 「DSCP 値のマッチング：例」（P.16）

シスコ エクスプレス フォワーディング スイッチングの確認：例

次に、イーサネット インターフェイス 1/0/0 の **show cef interface detail** コマンドの出力例を示します。このコマンドを使用して、ポリシー決定が行われるようにシスコ エクスプレス フォワーディング スイッチングがイネーブルになっていることを確認します。シスコ エクスプレス フォワーディング スイッチングがイネーブルになっていることが示されます。

```
Router# show cef interface Ethernet 1/0/0 detail

Ethernet1/0/0 is up (if_number 9)
  Corresponding hwidb fast_if_number 9
  Corresponding hwidb firstsw->if_number 9
  Internet address is 10.2.61.8/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is Ethernet1/0/0
  Fast switching type 1, interface type 5
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A82 (0x48001A82)
  IP MTU 1500
```

DSCP 値のマッチング：例

次に、priority50 という名前のサービス ポリシーを設定してインターフェイスに対応付ける例を示します。この例では、**match dscp** コマンドに、任意のキーワード **ip** が含まれています。これは、IPv4 パケットに対してだけマッチングを行うという意味です。ipdscp15 という名前のクラス マップによって、インターフェイス ファスト イーサネット 1/0/0 に入ってくるすべてのパケットが評価されます。パケットが IPv4 パケットであり、その DSCP 値が 15 の場合、そのパケットはプライオリティ トラフィックとして処理され、50 kbps の帯域幅が割り当てられます。

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority55
```

IPv6 パケットに対してだけマッチングを行う場合は、**match protocol** コマンドに続けて、**ip** キーワードを指定せずに **match dscp** コマンドを使用します。クラス マップが **match-all** アトリビュートを持つこと（デフォルト）を確認します。

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match dscp 15
Router(config)# exit
```

IPv4 プロトコルと IPv6 プロトコルの両方に対してパケットをマッチングする場合は、**match dscp** コマンドを使用します。

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match dscp 15
Router(config)# exit
```

その他の関連資料

ここでは、QoS for IPv6 機能の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』
RFC 2475	『*An Architecture for Differentiated Services Framework*』
RFC 2597	『*Assured Forwarding PHB*』
RFC 2598	『*An Expedited Forwarding PHB*』
RFC 2640	『*Internet Protocol, Version 6 Specification*』
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする • Product Alert の受信登録 • Field Notice の受信登録 • Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

QoS for IPv6 を実装するための機能情報

表 6 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(2)T 以降のリリースで導入または変更された機能だけを示します。

ここに記載されていないこのテクノロジーの機能情報については、「*Start Here: Cisco IOS Software Release Specifics for IPv6 Features*」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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

（注） 表 6 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 6　QoS for IPv6 を実装するための機能情報

機能名	リリース	機能情報
IPv6 Quality of Service（QoS; サービス品質）	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 環境でサポートされている QoS 機能には、パケット分類、キューイング、トラフィック シェーピング、WRED、クラスベース パケット マーキング、および IPv6 パケットのポリシングが含まれます。
IPv6 QoS：MQC パケット分類	12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	Modular QoS CLI を使用すると、トラフィック クラスを定義し、トラフィック ポリシー（ポリシー マップ）を作成および設定してから、それらのトラフィック ポリシーをインターフェイスに対応付けることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 でのパケット分類」（P.3） • 「IPv6 パケットのマーキング基準の指定」（P.5）
IPv6 QoS：MQC トラフィック シェーピング	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 環境でのトラフィック ポリシング」（P.4） • 「show policy-map interface コマンド出力内のパケット カウンタの解釈」（P.8）
IPv6 QoS：MQC トラフィック ポリシング	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 環境でのポリシングの設定またはコマンド使用法は、IPv4 環境の場合と同じです。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 環境でのトラフィック ポリシング」（P.4）

表 6　QoS for IPv6 を実装するための機能情報（続き）

機能名	リリース	機能情報
IPv6 QoS：MQC パケット マーキング/再マーキング	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	クラスベース マーキングを使用すると、トラフィック管理に対して IPv6 precedence および DSCP の値を設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 ネットワークでのポリシーおよびクラスベース パケット マーキング」（P.3） • 「IPv6 環境でのトラフィック ポリシング」（P.4）
IPv6 QoS：キューイング	12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 では、クラスベース キューイングとフローベース キューイングがサポートされています。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 ネットワークでの輻輳管理」（P.4） • 「IPv6 環境でのトラフィック ポリシング」（P.4） • 「show policy-map interface コマンド出力内のパケット カウンタの解釈」（P.8）
IPv6 QoS：MQC WRED ベース ドロップ	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	WRED は、CBWFQ の制限を超える可能性のあるパケットに対して RED ベースのドロップ ポリシーを実装します。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 トラフィックの輻輳回避」（P.4）

1. この機能は、Cisco IOS Release 12.0(28)S が稼動する Cisco 12000 シリーズ インターネット ルータ上でサポートされます。
2. Cisco IOS Release 12.2(18)SXE は、この機能をサポートしています。Cisco IOS Release 12.2(18)SXE は、Cisco Catalyst 6500 および Cisco 7600 シリーズ ルータに固有です。