QoS：分類の設定ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

有効な 2 つのリリースとしての Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）が、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと展開（マージ）されています。これにより、スイッチングおよびルーティング ポートフォリオの広範なアクセスおよびエッジ製品が盛り込まれた 1 つのリリースが実現しました。

（注） 技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディング ページに表示されている場合は、その機能がそのプラットフォームでサポートされていることを示します。

第 2 章

IPv6 Quality of Service

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、重み付けランダム早期検出（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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 Quality of Service に関する情報

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、重み付けランダム早期検出（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。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、モジュラ QoS コマンドライン インターフェイス（MQC）から管理します。MQC 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適用することができます。

IPv6 が稼働しているネットワークに QoS を実装するには、IPv4 だけが稼働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。

- 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。
- 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。
- 変更と転送がリンク層ヘッダー 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。
- 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、**matchprecedence**、**matchdscp**、**setprecedence**、**setdscp** 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 **matchprotocolip** や **matchprotocolipv6** などの一致基準を追加します。
- 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。
- 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。
- トラフィックを処理するためのポリシーを構築します。
- 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わせて、トラフィックを隔離、分離、および区別できます。

モジュラ 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。

IPv6 Quality of Service の設定方法

IPv6 ネットワークでのトラフィックの分類

802.1Q（dot1Q）インターフェイス用の **setcos** コマンドと **matchcos** コマンドは、シスコ エクスプレス フォワーディングによって切り替えられるパケットに対してのみサポートされます。これらのオプションが使用されている場合は、デバイス生成パケットなどのプロセススイッチドパケットが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

ネットワーク トラフィックを分類するためのパケットマッチングに使われる一致基準を構築する（またはパケットをマーキングする）には、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policymap***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. 次のいずれかを実行します。
   - **setprecedence** {*precedence-value* | *from-field* [**table***table-map-name*]}
   - **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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**policymap***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	次のいずれかを実行します。
	• **setprecedence** {*precedence-value* | *from-field* [**table***table-map-name*]}
	• **set** [**ip**] **dscp**{*dscp-value* | *from-field* [**table***table-map-name*]}
	
	例：
	`Router(config-pmap-c)#`
	`set dscp cos table table-map1`
	
	例：
	`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。

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

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. **configureterminal**
3. **class-map** {*class-name*| **class-default**}
4. 次のいずれかを実行します。
   - **matchprecedence***precedence-value*[*precedence-valueprecedence-value*]
   - **matchaccess-groupname***ipv6-access-group*
   - **match[ip]dscp***dscp-value* [*dscp-valuedscp-valuedscp-valuedscp-valuedscp-valuedscp-valuedscp-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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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 clsl`	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	次のいずれかを実行します。 • **matchprecedence***precedence-value*[*precedence-valueprecedence-value*] • **matchaccess-groupname***ipv6-access-group* • **match[ip]dscp***dscp-value* [*dscp-valuedscp-valuedscp-valuedscp-valuedscp-valuedscp-valuedscp-value*	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

	コマンドまたはアクション	目的

	例：
	`Router(config-pmap-c)# match precedence 5`
	例：
	`Router(config-pmap-c)# match ip dscp 15`
		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。

IPv6 Quality of Service の設定例

例：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

次に、GigabitEthernet インターフェイス 1/0/0 に対する **showcefinterfacedetail** コマンドの出力例を示します。このコマンドを使用して、ポリシーデシジョンが発生するように、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。この表示では、シスコ エクスプレス フォワーディングはイネーブルになっていることに注意してください。

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

GigabitEthernet1/0/0 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 GigabitEthernet1/0/0
  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
```

例：パケット マーキング基準の確認

次に、**matchprecedence** 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 マーキングが予想どおりに動作していることを確認するには、**showpolicy** コマンドを使用します。このコマンドの出力には、パケット総数とマーキングされたパケット数の差が表示されます。

```
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
```

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。**showpolicy-mapinterface** コマンド出力の解釈方法を理解しておくと、シスコの MQC を使って作成されたサービス ポリシーの結果をモニタリングするうえで役に立ちます。

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。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仮想回線（VC）の帯域幅によって異なります。次の例に示すように、**showatmvc***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
```

シスコ ソフトウェア（レイヤ 3 プロセッサとも呼ばれる）とインターフェイス 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であるため、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、送信リングの先入れ先出し（FIFO）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。

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。次の表に、どのパケットがレイヤ 3 キューに含まれるかを示します。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）	はい	はい
プロセス スイッチングが行われる他のパケット	はい	はい
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	はい	いいえ

次の例では、これらのガイドラインが **showpolicy-mapinterface** コマンド出力に適用されています。

```
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)
```

次の表は、例に示されるカウンタを定義しています。

表 *2*：***show policy-map interface*** 出力からのパケット 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 パケットは必ず L3 キューイング システムを通過するため、「一致パケット」カウンタが増加します。
Class-map: B (match-all) (1301/4)	これらの番号は、CISCO-CLASS-BASED-QOS-MIB 管理情報ベース（MIB）で使用される内部 ID を定義します。
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、**showpolicy-mapinterface** 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。

ルータは、サービス ポリシーが適用された際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 マップ内でポリシーの定義されている他のどのクラスの条件も満たさなかった場合に、そのトラフィックの送信先となるデフォルト 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。

次の表に、インターフェイスのデフォルト値とATM相手先固定接続（PVC）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
256 kbps より大きく 512 kbps 以下	128
512 kbps より大きい	256

次の表に、ATM PVC 帯域幅に関連するダイナミック キューのデフォルト数を示します。

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 ～ 512 kbp（128 kbps は含まない）	32
512 ～ 2000 kbp（512 kbps は含まない）	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、シスコ ソフトウェアは、下の表に示すカンバセーション番号またはキュー番号を割り当てます。

表 *5*：キューに割り当てられるカンバセーション番号

番号	トラフィックのタイプ
1 ～ 256	汎用フローベース トラフィック キュー。ユーザ作成クラスと一致しないトラフィックは、class-default およびいずれかのフローベース キューと一致します。

番号	トラフィックのタイプ
257 ～ 263	Cisco Discovery Protocol 用、および内部高優先順位フラグでマーキングされたパケット用として予約されています。
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）用のキューとして予約されています。**showpolicy-map** インターフェイス出力でクラスに関する Strict Priority 値を探します。プライオリティ キューは、ダイナミック キューの数に 8 を加えた数に一致するカンバセーション ID を使用します。
265 以降	ユーザ作成クラス用のキュー。

例：DSCP 値のマッチング

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、**matchdscp** 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 ギガビット 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 gigabitethernet1/0/0
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、**matchprotocol** コマンドに続けて、**ip** キーワードを指定せずに **matchdscp** コマンドを使用します。クラス マップが **match-all** 属性を持つこと（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、**matchdscp** コマンドを使用します。

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

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
ポリシーマップのインターフェイスへの適用に関する MQC および情報	「Applying QoS Features Using the MQC」モジュール
パケット分類に使用できる追加の一致基準	『Classifying Network Traffic』モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

標準

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-CAPABILITY-MIB • CISCO-CLASS-BASED-QOS-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、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
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

IPv6 Quality of Service の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6*：***IPv6 Quality of Service*** の機能情報

機能名	リリース	機能情報
IPv6 Quality of Service	12.2(13)T 12.3 12.2(50)SG 3.2.0SG 15.0(2)SG 12.2(33)SRA 12.2(18)SXE Cisco IOS XE Release 2.1	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。 **match dscp** コマンド、**match precedence** コマンド、**set dscp** コマンド、および **set precedence** コマンドが導入または変更されています。 **match access-group name** コマンド、**match dscp** コマンド、**match precedence** コマンド、**set dscp** コマンド、および **set precedence** コマンドが導入または変更されています。

第 3 章

IPv6 QoS：MQC Packet Classification

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 QoS：MQC Packet Classification に関する情報

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、重み付けランダム早期検出（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。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、モジュラQoSコマンドラインインターフェイス（MQC）から管理します。MQC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適用することができます。

IPv6 が稼働しているネットワークに QoS を実装するには、IPv4 だけが稼働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。

- 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。
- 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。
- 変更と転送がリンク層ヘッダー 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。
- 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、**matchprecedence**、**matchdscp**、**setprecedence**、**setdscp** 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 **matchprotocolip** や **matchprotocolipv6** などの一致基準を追加します。
- 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。
- 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。
- トラフィックを処理するためのポリシーを構築します。
- 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わせて、トラフィックを隔離、分離、および区別できます。

モジュラ 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。

IPv6 QoS：MQC Packet Classification の設定方法

IPv6 ネットワークでのトラフィックの分類

802.1Q（dot1Q）インターフェイス用の **setcos** コマンドと **matchcos** コマンドは、シスコ エクスプレス フォワーディングによって切り替えられるパケットに対してのみサポートされます。これらのオプションが使用されている場合は、デバイス生成パケットなどのプロセススイッチドパケットがマーキングされません。

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

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. **configureterminal**
3. **class-map** {*class-name*| **class-default**}
4. 次のいずれかを実行します。
   - **matchprecedence***precedence-value*[*precedence-valueprecedence-value*]
   - **matchaccess-groupname***ipv6-access-group*
   - **match[ip]dscp***dscp-value* [*dscp-valuedscp-valuedscp-valuedscp-valuedscp-valuedscp-valuedscp-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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**class-map** {*class-name*| **class-default**} 例： `Router(config-pmap-c)# class clsl`	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	次のいずれかを実行します。
	• **matchprecedence***precedence-value*[*precedence-valueprecedence-value*]
	• **matchaccess-groupname***ipv6-access-group*
	• **match[ip]dscp***dscp-value* [*dscp-valuedscp-valuedscp-valuedscp-valuedscp-valuedscp-valuedscp-value*
	
	例：
	`Router(config-pmap-c)#`
	`match precedence 5`
	
	例：
	`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。

サービス ポリシーの確認

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 が小さい確認応答（ACK）を返すためです。

この作業を始める前に、サイズの大きい ping および多数の ping を使用して、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. **configureterminal**
3. **interface***typenumber***multipoint** | **point-to-point**
4. **ipaddressip-addressmask** [*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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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***typenumber***multipoint** | **point-to-point** 例： `Router(config)# interface gigabitethernet1/1/0 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	**ipaddressip-addressmask** [*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 の名前を割り当てまたは作成し、任意で ATM PVC のカプセル化タイプを指定して、interface-ATM-VC コンフィギュレーション モードに入ります。

	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小さくします。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。 • リング制限を 2600 および 3600 シリーズ ルータのパケット数、または 7200 および 7500 シリーズ ルータのメモリ パーティクル数に指定します。
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ます。

IPv6 QoS：MQC Packet Classification の設定例

例：DSCP 値のマッチング

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、**matchdscp** 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 ギガビット 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 gigabitethernet1/0/0
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、**matchprotocol** コマンドに続けて、**ip** キーワードを指定せずに **matchdscp** コマンドを使用します。クラス マップが **match-all** 属性を持つこと（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、**matchdscp** コマンドを使用します。

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

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
ネットワーク トラフィックの分類	「Classifying Network Traffic」モジュール

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

IPv6 QoS：MQC Packet Classification の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *7*：*IPv6 QoS*：*MQC Packet Classification* の機能情報

機能名	リリース	機能情報
IPv6 QoS：MQC Packet Classification	Cisco IOS XE Release 2.1	モジュラ QoS CLI を使用すれば、トラフィック クラスを定義し、トラフィック ポリシーを作成して設定してから、それらのトラフィック ポリシーをインターフェイスに適用できます。 **match access-group name** コマンド、**match dscp** コマンド、**match precedence** コマンド、**set dscp** コマンド、および **set precedence** コマンドが導入または変更されています。

第 4 章

レイヤ3パケット長に基づくパケット分類

この機能は、IPヘッダーのレイヤ3パケット長に基づいて、トラフィックを照合して分類する追加機能を提供します。レイヤ3パケット長とは、IPデータグラム長とIPヘッダー長の合計です。この新しい一致基準は、IP precedence、Diffserv コード ポイント（DSCP）値、サービス クラス（CoS）などの他の一致基準を補完するものです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

レイヤ 3 パケット長に基づくパケット分類の前提条件

この機能を設定する場合は、先に、モジュラ QoS コマンドライン インターフェイス（CLI）（MQC）を使用してポリシー マップ（サービス ポリシーまたはトラフィック ポリシーと呼ばれることもある）を作成する必要があります。そのため、MQC を使用してポリシーを作成するための手順に精通しておく必要があります。

MQC を使用したポリシー マップ（トラフィック ポリシー）の作成方法については、『Applying QoS Features Using the MQC』モジュールを参照してください。

レイヤ 3 パケット長に基づくパケット分類の制約事項

- この機能は、IP パケットでのみ使用するように意図されています。
- この機能では、IP ヘッダー内のレイヤ 3 パケット長のみが考慮されます。レイヤ 2 オーバーヘッドは考慮されません。

レイヤ 3 パケット長に基づくパケット分類に関する情報

MQC とレイヤ 3 パケット長に基づくパケット分類

レイヤ 3 パケット長に基づくパケット分類をイネーブルにするには、MQC を使用します。MQC は、トラフィック ポリシーを作成し、QoS 機能（パケット分類など）をイネーブルにし、それらのポリシーをインターフェイスに適用するための CLI です。

MQC では、**class-map** コマンドを使ってトラフィック クラスを定義します（トラフィック クラスはその後、トラフィック ポリシーに関連付けられます）。トラフィック クラスの目的は、トラフィックを分類することです。

MQC は、次の 3 つのプロセスで構成されます。

- **class-map** コマンドを使用したトラフィック クラスの定義
- トラフィック クラスを 1 つまたは複数の QoS 機能と関連付けてトラフィック ポリシーを作成（**policy-map** コマンドを使用）
- **service-policy** コマンドを使用した、トラフィック ポリシーのインターフェイスへのアタッチ

トラフィック クラスに含まれる 3 つの主な要素は、名前、一連の **match** コマンド、そしてトラフィック クラスに複数の **match** コマンドが存在する場合に **match** コマンドを評価する方法です。トラフィック クラスの名前は、**class-map** コマンド ラインで指定します。たとえば、CLI でトラフィック クラスを設定するときに **class-mapcisco** コマンドを入力すると、トラフィック クラスの名前は「cisco」になります。

match コマンドは、パケット分類のためのさまざまな基準を指定するために使用します。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。

レイヤ 3 パケット長に基づくパケット分類の設定方法

レイヤ 3 パケット長に基づいて照合するためのクラス マップの設定

クラス マップは、特定の QoS 機能を受信可能なグループにパケットを分類するために使用できます。たとえば、1 つ以上のユーザ指定基準（DSCP 値やアクセス リスト番号など）に基づいてパケットを照合するようにクラス マップを設定できます。この手順では、レイヤ 3 パケット長に基づいて照合するようにクラス マップを設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map***class-map-name*
4. **matchpacketlength** {**max***maximum-length-value* [**min***minimum-length-value*] | **min***minimum-length-value* [**max***maximum-length-value*]}
5. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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-map-name* 例： `Router(config)# class-map class1`	作成するクラス マップの名前を指定し、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。 • クラス マップ名を入力します。

	コマンドまたはアクション	目的
ステップ 4	**matchpacketlength** {**max***maximum-length-value* [**min***minimum-length-value*] | **min***minimum-length-value* [**max***maximum-length-value*]} 例： `Router(config-cmap)# match packet length min 100 max 300`	レイヤ 3 パケット長に基づいてトラフィックを照合するようにクラス マップを設定します。 • レイヤ 3 パケット長をバイト単位で入力します。
ステップ 5	**end** 例： `Router(config-cmap)# end`	（任意）クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ポリシー マップのインターフェイスへの接続

はじめる前に

ポリシー マップをインターフェイスに適用する前に、MQC を使用してポリシー マップを作成する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input**| **output**} *policy-map-name*
6. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface serial4/0/0`	インターフェイス（またはサブインターフェイス）タイプを設定し、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	**pvc** [*name*] *vpi/vci* [**ilmi** | **qsaal** | **smds**] 例： `Device(config-if)# pvc cisco 0/16 ilmi`	（任意）ATM PVC の名前を作成するか、名前を割り当てて、ATM PVC 上のカプセル化タイプを指定し、ATM VC コンフィギュレーション モードを開始します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。ポリシー マップを ATM PVC に適用しない場合は、この手順を省略します。

ステップ 5	**service-policy** {**input**| **output**} *policy-map-name*
	
	例：
	
	`Device(config-if)# service-policy input policy1`
	
	例：
	
	`Device(config-if-atm-vc)# service-policy input policy1`
		インターフェイスの入力または出力方向のいずれかに適用するポリシー マップの名前を指定します。
		（注） ポリシーマップは、入力デバイスまたは出力デバイスで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシーマップを適用する方向（入力または出力）とデバイス（入力または出力）は、ネットワーク構成によって異なります。**service-policy** コマンドを使用してポリシー マップをインターフェイスに適用する場合は、ネットワーク構成に適したデバイスおよびインターフェイスの方向を選択してください。

ステップ 6	**end**
	
	例：
	
	`Device(config-if)# end`
	
	例：
	
	`Device(config-if-atm-vc)# end`
		（任意）インターフェイス コンフィギュレーション モードまたは ATM VC コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

レイヤ 3 パケット長分類設定の確認

手順の概要

1. **enable**
2. **showclass-map** [*class-map-name*]
3. **showpolicy-mapinterface***interface-name*[**vc** [*vpi/*] *vci*] [**dlci***dlci*] [**input**| **output**]
4. **exit**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**showclass-map** [*class-map-name*] 例： `Router# show class-map class1`	（任意）一致基準を含む、クラスマップに関するすべての情報が表示されます。 • クラス マップ名を入力します。

ステップ 3	**showpolicy-mapinterface***interface-name*[**vc** [*vpi/*] *vci*] [**dlci***dlci*] [**input**| **output**]
	
	例：
	`Router#`
	`show policy-map interface serial4/0/0`
		（任意）指定されたインターフェイスまたはサブインターフェイス、またはインターフェイス上の特定の PVC のどちらかで、すべてのポリシーに対して設定されたすべてのクラスのパケット統計値を表示します。
		• インターフェイス名を入力します。

ステップ 4	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

トラブルシューティングのヒント

「レイヤ 3 パケット長分類設定の確認」に示すコマンドを使用すると、意図した設定が完了し、機能が正しく動作していることを確認できます。上記の **show** コマンドの使用後に、設定が正しくない、または機能が予想どおりに働いていないと判明した場合は、次の操作を実行します。

意図した設定になっていない場合は、次の操作を実行します。

- **showrunning-config** コマンドを使用して、コマンドの出力を分析します。
- ポリシー マップが **showrunning-config** コマンドの出力に表示されない場合は、**loggingconsole** コマンドをイネーブルにします。
- ポリシー マップをインターフェイスに再度アタッチします。

パケットが正しく照合されていない（たとえば、パケット カウンタが正しく増加していない）場合は、次の手順を行います。

- **showpolicy-map** コマンドを実行して、コマンドの出力を分析します。
- **showrunning-config** コマンドを実行して、コマンドの出力を分析します。
- **showpolicy-mapinterface** コマンドを実行して、コマンドの出力を分析します。次の点を確認します。
  - ポリシーマップでキューイングが適用され、パケットが正しいクラスに一致しているにもかかわらず、予期しない結果が生じる場合は、キューのパケット数と、一致したパケット数を比較します。
  - インターフェイスが混雑していて、一致するパケット数が少ない場合には、tx リングの調整を確認し、tx リングでキューイングが実行されているかどうかを評価します。これを行うには、**showcontrollers** コマンドを使用し、出力で tx 回数の値を確認します。

レイヤ 3 パケット長に基づくパケット分類の設定例

一致基準としてのレイヤ 3 パケット長の設定例

次の例では、「class 1」という名前のクラス マップが作成され、一致基準としてレイヤ 3 パケット長が指定されています。この例では、最小レイヤ 3 パケット長が 100 バイトで、最大レイヤ 3 パケット長が 300 バイトのパケットが一致基準を満たしているとされています。この基準と一致するパケットが class1 に配置されます。

```
Router(config)# class map class1
Router(config-cmap)# match packet length min 100 max 300
```

レイヤ 3 パケット長設定の確認例

クラス マップとポリシー マップの一致基準として使用されるレイヤ 3 パケット長の値の設定を確認するには、**showclass-map** コマンドと **showpolicy-mapinterface** コマンドのいずれかを使用します。ここでは、まず **showclass-map** コマンドの出力例を示し、その後 **showpolicy-mapinterface** コマンドの出力例を紹介します。

showclass-map コマンドの出力例には、定義されたクラス マップと指定された一致基準が表示されます。次の例では、class1 という名前のクラス マップを定義します。レイヤ 3 パケット長がク

ラスの一致基準として指定されています。レイヤ 3 長が 100 ～ 300 バイトのパケットが class1 に属します。

```
Router# show class-map
class-map match-all class1
    match packet length min 100 max 300
```

showpolicy-mapinterface コマンドの出力例には、「mypolicy」という名前のサービス ポリシーが適用される FastEthernet インターフェイス 4/1/1 の統計情報が表示されます。「mypolicy」という名前のポリシー マップの設定は次のとおりです。

```
Router(config)# policy-map mypolicy
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 20
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet4/1/1
Router(config-if)# service-policy input mypolicy
```

次に、FastEthernet インターフェイス 4/1/1 に適用される「mypolicy」という名前のポリシー マップの統計情報を示します。これらの統計情報で、レイヤ 3 パケット長に基づくマッチングが一致条件として設定されていることが確認できます。

```
Router# show policy-map interface
 FastEthernet4/1/1
 FastEthernet4/1/1
  Service-policy input: mypolicy
    Class-map: class1 (match-all)
       500 packets, 125000 bytes
       5 minute offered rate 4000 bps, drop rate 0 bps
       Match: packet length min 100 max 300
       QoS Set
         qos-group 20
           Packets marked 500
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
ポリシーマップのインターフェイスへの適用に関する MQC および情報	「Applying QoS Features Using the MQC」モジュール
パケット分類に使用できる追加の一致基準	『Classifying Network Traffic』モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

標準

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-CAPABILITY-MIB • CISCO-CLASS-BASED-QOS-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、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
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

レイヤ 3 パケット長に基づくパケット分類の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *8*：レイヤ *3* パケット長に基づくパケット分類の機能情報

機能名	リリース	機能情報
レイヤ 3 パケット長に基づくパケット分類	12.2(13)T 12.2(18)SXE Cisco IOS XE Release 2.2	この機能は、IP ヘッダーのレイヤ 3 パケット長に基づいて、トラフィックを照合して分類する追加機能を提供します。 この機能は、Release 12.2(13)T で初めて導入されました。 この機能は、Cisco IOS Release 12.2(18)SXE に統合されました。 この機能は、Cisco IOS XE Release 2.2 に統合されました。 **matchpacketlength** コマンド（class-map）、**showclass-map** コマンド、および **showpolicy-mapinterface** コマンドが導入または変更されています。

第 5 章

IPv6 QoS：MQC Packet Marking/Remarking

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 QoS：MQC Packet Marking/Remarking に関する情報

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、重み付けランダム早期検出（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。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、モジュラQoSコマンドラインインターフェイス（MQC）から管理します。MQC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適用することができます。

IPv6 が稼働しているネットワークに QoS を実装するには、IPv4 だけが稼働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。

- 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。
- 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。
- 変更と転送がリンク層ヘッダー 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。
- 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、**matchprecedence**、**matchdscp**、**setprecedence**、**setdscp** 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 **matchprotocolip** や **matchprotocolipv6** などの一致基準を追加します。
- 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。
- 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。
- トラフィックを処理するためのポリシーを構築します。
- ポリシーを適用します。

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 または 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。

IPv6 環境でのトラフィック ポリシング

IPv6 での輻輳管理は、IPv4 の場合と似ています。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、IPv4 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、クラスベース ポリシング機能およびフレーム リレー トラフィック シェーピング（FRTS）を使用できます。

IPv6 QoS：MQC Packet Marking/Remarking の指定方法

IPv6 パケットのマーキング基準の指定

ネットワーク トラフィックを分類するためのパケットマッチングに使われる一致基準を構築する（またはパケットをマーキングする）には、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policymap***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. 次のいずれかを実行します。
   - **setprecedence** {*precedence-value* | *from-field* [**table***table-map-name*]}
   - **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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**policymap***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	次のいずれかを実行します。
	• **setprecedence** {*precedence-value* | *from-field* [**table***table-map-name*]}
	• **set** [**ip**] **dscp**{*dscp-value* | *from-field* [**table***table-map-name*]}
	
	例：
	`Router(config-pmap-c)#`
	`set dscp cos table table-map1`
	
	例：
	`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。

IPv6 QoS：MQC Packet Marking/Remarking の設定例

例：パケット マーキング基準の確認

次に、**matchprecedence** 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 マーキングが予想どおりに動作していることを確認するには、**showpolicy** コマンドを使用します。このコマンドの出力には、パケット総数とマーキングされたパケット数の差が表示されます。

```
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
```

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。**showpolicy-mapinterface** コマンド出力の解釈方法を理解しておくと、シスコの MQC を使って作成されたサービス ポリシーの結果をモニタリングするうえで役に立ちます。

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。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仮

想回線（VC）の帯域幅によって異なります。次の例に示すように、**showatmvc***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
```

シスコ ソフトウェア（レイヤ 3 プロセッサとも呼ばれる）とインターフェイス 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であるため、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、送信リングの先入れ先出し（FIFO）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。

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。次の表に、どのパケットがレイヤ 3 キューに含まれるかを示します。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 *9*：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）	はい	はい
プロセス スイッチングが行われる他のパケット	はい	はい
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	はい	いいえ

次の例では、これらのガイドラインが **showpolicy-mapinterface** コマンド出力に適用されています。

```
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)
```

次の表は、例に示されるカウンタを定義しています。

表 *10*：*show policy-map interface* 出力からのパケット 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 パケットは必ず L3 キューイング システムを通過するため、「一致パケット」カウンタが増加します。
Class-map: B (match-all) (1301/4)	これらの番号は、CISCO-CLASS-BASED-QOS-MIB 管理情報ベース（MIB）で使用される内部 ID を定義します。
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、**showpolicy-mapinterface** 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。

ルータは、サービス ポリシーが適用された際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 マップ内でポリシーの定義されている他のどのクラスの条件も満たさなかった場合に、そのトラフィックの送信先となるデフォルト 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。

次の表に、インターフェイスのデフォルト値とATM相手先固定接続（PVC）のデフォルト値を示します。

表 *11*：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
256 kbps より大きく 512 kbps 以下	128
512 kbps より大きい	256

次の表に、ATM PVC 帯域幅に関連するダイナミック キューのデフォルト数を示します。

表 *12*：*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 ～ 512 kbp（128 kbps は含まない）	32
512 ～ 2000 kbp（512 kbps は含まない）	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、シスコ ソフトウェアは、下の表に示すカンバセーション番号またはキュー番号を割り当てます。

表 *13*：キューに割り当てられるカンバセーション番号

番号	トラフィックのタイプ
1 ～ 256	汎用フローベース トラフィック キュー。ユーザ作成クラスと一致しないトラフィックは、class-default およびいずれかのフローベース キューと一致します。

番号	トラフィックのタイプ
257 ～ 263	Cisco Discovery Protocol 用、および内部高優先順位フラグでマーキングされたパケット用として予約されています。
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）用のキューとして予約されています。**showpolicy-map** インターフェイス出力でクラスに関する Strict Priority 値を探します。プライオリティ キューは、ダイナミック キューの数に 8 を加えた数に一致するカンバセーション ID を使用します。
265 以降	ユーザ作成クラス用のキュー。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

IPv6 QoS：MQC Packet Marking/Remarking の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *14*：*IPv6 QoS*：*MQC Packet Marking/Remarking* の機能情報

機能名	リリース	機能情報
IPv6 QoS：MQC Packet Marking/Remarking	Cisco IOS XE Release 2.1	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。

第 6 章

ネットワーク トラフィックのマーキング

ネットワーク トラフィックをマーキングすると、特定のクラスまたはカテゴリに属するトラフィック（パケット）の属性を設定または変更できます。ネットワーク トラフィック マーキングは、ネットワーク トラフィックの分類とともに使用すると、ネットワーク上の多数の Quality of Service（QoS）をイネーブルにする際の基礎になります。このモジュールでは、ネットワーク トラフィック マーキングに必要な概念情報と設定作業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 リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

ネットワークトラフィックマーキングに関する前提基準

ネットワーク トラフィックをマーキングするには、トラフィックを受信するインターフェイスとトラフィックを送信するインターフェイスの両方でシスコエクスプレスフォワーディングを設定する必要があります。

ネットワークトラフィックマーキングに関する制約事項

ネットワーク トラフィックのマーキングに関する情報

ネットワーク トラフィックにマーキングする目的

トラフィック マーキングは、トラフィック固有の処理を行うためにトラフィック タイプの識別に使用される方式です。ネットワーク トラフィックを効率的に異なるカテゴリへ分類できます。

トラフィックの分類によってネットワーク トラフィックをクラスに構成した後は、トラフィック マーキングによって、特定のクラスに属するトラフィックの値（属性）にマーキング（つまり、設定または変更）できます。たとえば、あるクラスのサービス クラス（CoS）値を 2 から 1 に変更し、別のクラスの Diffserv コード ポイント（DSCP）値を 3 から 2 に変更できます。このような値のことをここでは属性と呼びます。

次の属性を設定および変更できます。

- 発信パケットの CoS 値
- discard-class 値
- タイプ オブ サービス（ToS）バイトの DSCP 値
- 入力または出力インターフェイスの最上位ラベルの MPLS EXP フィールド値
- すべての割り当て済みラベル エントリのマルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）フィールド
- パケット ヘッダーの precedence 値
- QoS グループ識別番号（ID）
- IP パケットのヘッダーの ToS ビット

ネットワーク トラフィックにマーキングする利点

ネットワーク パフォーマンスの向上

トラフィック マーキングによって、ネットワーク上のトラフィックの属性を微調整できます。より細かく調整できるようになったことで、特別な処理が必要なトラフィックの検出や最適なアプリケーション パフォーマンスの実現が容易になります。

トラフィック マーキングを使用すると、ネットワーク トラフィックの属性を設定する方法に基づいて、トラフィックの処理方法を決定できます。また、その属性に基づいて、次のようにネットワーク トラフィックを複数のプライオリティ レベルまたはサービス クラスに分類できます。

- 多くの場合、トラフィック マーキングは、ネットワークに着信するトラフィックの IP precedence または IP DSCP 値の設定に使用されます。ネットワーク内のネットワーキング デバイスは、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。たとえば、特定の IP precedence または DSCP を使用して音声トラフィックをマーキングしてから、そのマークのすべてのパケットをプライオリティ キューに配置するようにキューイング メカニズムを設定できます。
- トラフィック マーキングは、任意のクラスベース QoS 機能（policy-map クラス コンフィギュレーション モードで使用できる機能ですが、いくつかの制約事項があります）のトラフィックを識別するために使用できます。
- トラフィック マーキングは、デバイス内の QoS グループにトラフィックを割り当てるために使用できます。デバイスは QoS グループを使用して、送信トラフィックに優先順位を付ける方法を決定できます。一般的に、QoS グループ値は次の 2 つの理由のいずれかに使用されます。
  - 広い範囲のトラフィック クラスを利用する場合。QoS グループ値には 100 種類のマーキングがあるのに対して、DSCP と IP precedence のマーキングの数はそれぞれ 64 と 8 です。

    （注） QoS グループの範囲は、Cisco RSP3 モジュール上で 0 ～ 7 です。

  - IP precedence または DSCP 値の変更はお勧めできません。
- ユーザ定義の QoS サービスを識別するためにマーキングが必要なパケット（トラフィック フロー内など）がデバイスを出てスイッチに入る場合は、スイッチでレイヤ 2 CoS ヘッダー マーキングを処理できるため、デバイスでトラフィックの CoS 値を設定できます。または、スイッチから出るトラフィックのレイヤ 2 CoS 値をレイヤ 3 IP または MPLS 値にマッピングできます。
- Weighted Random Early Detection（WRED）は、precedence 値または DSCP 値を使用して、トラフィックがドロップされる確率を決定します。そのため、precedence と DSCP は WRED と併用できます。

トラフィック属性にマーキングする 2 つの方式

トラフィック属性の指定およびマーキングには、次の 2 つの方式があります。

- **set** コマンドを使用して、トラフィック属性の指定およびマーキングを実行できます。

この方式では、マーキングする個々のトラフィック属性に **set** コマンドを設定します。

この方式では、マーキングするトラフィック属性をテーブル マップに設定してから、ネットワークを介してネットワークをプロパゲートします。

これらの方式の詳細については、以下の項で説明します。

方式 1：set コマンドの使用

ポリシーマップで設定された **set** コマンドを使用して、変更するトラフィック属性を指定します。次の表に、使用可能な **set** コマンドと対応する属性を示します。この表には、トラフィック属性に関連付けられることが多いネットワーク層とネットワーク プロトコルも含まれています。

表 *15*：*set* コマンドと対応するトラフィック属性、ネットワーク層、およびプロトコル

set コマンド[1]	トラフィック属性	ネットワーク層	プロトコル
setcos	発信トラフィックのレイヤ 2 CoS 値	レイヤ 2	
setdiscard-class	discard-class 値	レイヤ 2	
setdscp	ToS バイトの DSCP 値	レイヤ 3	IP
setfr-de	フレームリレーフレームのアドレス フィールドの DE ビット設定	レイヤ 2	
setiptos(route-map)	IP パケットのヘッダーの ToS ビット	レイヤ 3	IP
setmplsexperimentalimposition	すべての割り当て済みラベル エントリの MPLS EXP フィールド	レイヤ 3	MPLS
setmplsexperimentaltopmost	入力または出力インターフェイスの最上位ラベルの MPLS EXP フィールド値	レイヤ 3	MPLS

set コマンド[1]	トラフィック属性	ネットワーク層	プロトコル
setprecedence	パケット ヘッダーの precedence 値	レイヤ 3	IP
setqos-group	QoS グループ ID	レイヤ 3	IP、MPLS

1 シスコの set コマンドはリリースによって異なります。詳細については、お使いのシスコ リリースのコマンド マニュアルを参照してください。

方式 2 テーブル マップの使用

トラフィック属性のマーキングに使用できるテーブル マップを作成します。テーブル マップは 2 方向の変換表の一種で、トラフィック属性を別の属性にマッピングしたリストです。テーブル マップは多対一型の変換およびマッピング スキームをサポートします。テーブル マップはトラフィック属性について to-from 関係を確立し、属性に加える変更を定義します。つまり属性は、別の値から取得された 1 つの値に設定されます。値は、変更される特定の属性に基づいています。たとえば、Precedence 属性は 0 ～ 7 の数値に、一方 DSCP 属性は 0 ～ 63 の数値にそれぞれ設定できます。

次に、テーブル マップの設定例を示します。

```
table-map table-map1
map from 0 to 1
map from 2 to 3
exit
```

次の表に、テーブル マップを使用して to-from 関係を確立できるトラフィック属性の一覧を示します。

表 *16*：*to-from* 関係を確立できるトラフィック属性

「To」属性	「From」属性
Precedence	CoS
	QoS group
DSCP	CoS
	QoS group
CoS	Precedence
	DSCP

「To」属性	「From」属性
QoS group	Precedence
	DSCP
	MPLS EXP topmost
MPLS EXP topmost	QoS group
MPLS EXP imposition	Precedence
	DSCP

テーブル マップを作成した後は、ポリシー マップを設定してテーブル マップを使用します。ポリシーマップでは、マップするテーブルマップ名と属性を指定します。そのために、次の表に記載されているコマンドの 1 つで、**table** キーワードと *table-map-name* 引数を使用します。

表 *17*：属性をマッピングするポリシー マップに使用するコマンド

ポリシー マップに使用するコマンド	マッピングする属性
setcosdscptable*table-map-name*	CoS から DSCP へ
setcosprecedencetable*table-map-name*	CoS から precedence へ
setdscpcostable*table-map-name*	DSCP から CoS へ
setdscpqos-grouptable*table-map-name*	DSCP から qos-group へ
setmplsexperimentalimpositiondscptable*table-map-name*	MPLS EXP imposition から DSCP へ
setmplsexperimentalimpositionprecedencetable*table-map-name*	MPLS EXP imposition から precedence へ
setmplsexperimentaltopmostqos-grouptable*table-map-name*	MPLS EXP topmost から QoS-group へ
setprecedencecostable*table-map-name*	precedence から CoS へ
setprecedenceqos-grouptable*table-map-name*	precedence から QoS-group へ
setqos-groupdscptable*table-map-name*	QoS-group から DSCP へ
setqos-groupmplsexptopmosttable*table-map-name*	QoS-group から MPLS EXP topmost へ
setqos-grouppprecedencetable*table-map-name*	QoS-group から precedence へ

次に、以前に作成したテーブル マップ（table-map1）を使用するように設定されたポリシー マップ（policy2）の例を示します。

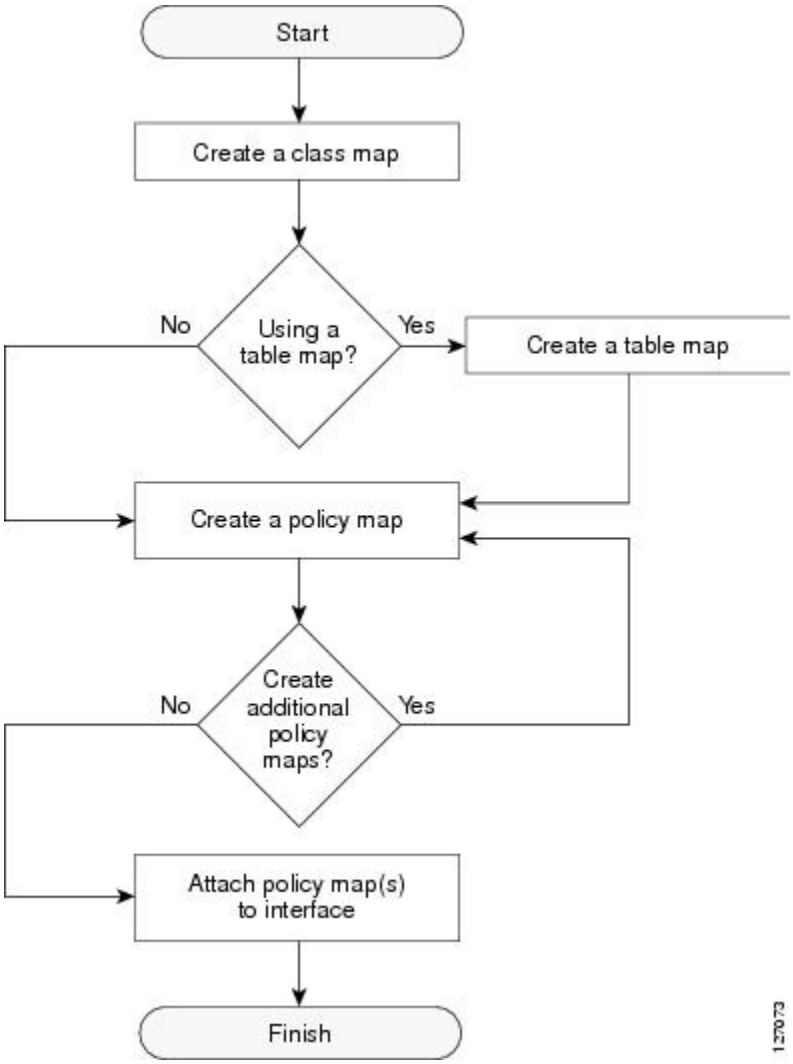
```
policy map policy2
class class-default
set cos dscp table table-map1
exit
```

この例では、テーブル マップの定義に従って、CoS 属性と DSCP 属性の間にマッピング関係が作成されました。

トラフィック マーキングの手順フローチャート

次の図に、トラフィック マーキングを設定する手順を示します。

図 *1*：トラフィック マーキングの手順フローチャート



トラフィック属性のマーキング方式

ポリシーマップで設定された**set**コマンドを使用して、変更するトラフィック属性を指定してマーキングします。

この方式では、マーキングする個々のトラフィック属性に **set** コマンドを設定します。

set コマンドの使用

個別の **set** コマンドを使用している場合、それらの **set** コマンドはポリシー マップで指定されます。次に、上の表で示した **set** コマンドの 1 つを使用して設定されたポリシー マップの例を示します。この設定例では、**setcos** コマンドがポリシー マップ（policy1）で設定され、CoS 値をマーキングしています。

```
policy-map policy1
 class class1
  set cos 1
  end
```

ポリシーマップの設定方法については、「QoS機能をネットワーク トラフィックに適用するためのポリシー マップの作成」の項を参照してください。

最後の作業として、ポリシー マップをインターフェイスに適用します。ポリシー マップをインターフェイスに適用する方法については、「ポリシー マップのインターフェイスへの適用」の項を参照してください。

MQC とネットワーク トラフィック マーキング

ネットワーク トラフィック マーキングを設定するために、モジュラ QoS CLI（MQC）を使用します。

MQC は、次の作業を完了できる CLI 構造です。

- トラフィック クラスの定義に使用される一致基準を指定します。
- トラフィック ポリシー（ポリシー マップ）を作成します。トラフィック ポリシーには、各トラフィック クラスに実行する QoS ポリシー アクションを定義します。
- **service-policy** コマンドを使用して、インターフェイス、サブインターフェイス、または ATM PVC にポリシー マップに指定されたポリシー アクションを適用します。

トラフィックの分類とトラフィック マーキングの比較

トラフィックの分類とトラフィック マーキングには密接に関係があり、併用できます。トラフィック マーキングは、トラフィック クラスで実行される、ポリシーマップに指定された追加アクションとして表示できます。

トラフィックの分類を使用すると、トラフィックが特定の基準に一致するかどうかに基づいて、トラフィック クラスを構成できます。たとえば、CoS 値 2 を持つすべてのトラフィックを 1 つのクラスにグループ分けし、DSCP 値 3 を持つトラフィックを別のクラスにグループ分けします。一致基準はユーザ定義です。

トラフィックをトラフィック クラスに構成した後は、トラフィック マーキングを使用して、そのクラスに属するトラフィックの属性にマーク（つまり、設定または変更）できます。たとえば、CoS 値を 2 から 1 に変更したり、DSCP 値を 3 から 2 に変更したりできます。

トラフィックの分類に使用される一致基準は、クラス マップに **match** コマンドを設定して指定します。トラフィック マーキングによって実行するマーキング アクションは、ポリシー マップで **set** コマンドを設定して指定します。これらのクラス マップとポリシー マップは、MQC を使用して設定されます。

次の表に、トラフィック分類とトラフィック マーキングの機能の比較を示します。

表 *18*：トラフィックの分類とトラフィック マーキングの比較

機能	トラフィック分類	トラフィック マーキング
目標	トラフィックがユーザ定義の基準に一致するかどうかに基づいて、ネットワーク トラフィックを特定のトラフィック クラスにグループ化します。	ネットワーク トラフィックをトラフィック クラスにグループ化した後に、特定のトラフィック クラスのトラフィックの属性を変更します。
設定メカニズム	MQC でクラス マップとポリシー マップを使用します。	MQC でクラス マップとポリシー マップを使用します。
CLI	クラス マップでは、**match** コマンド（たとえば、**matchcos**）を使用して、トラフィック一致基準を定義します。	トラフィックの分類によって指定されたトラフィック クラスと一致基準を使用します。 さらに、ポリシー マップに **set** コマンドを使用して（たとえば **setcos**）、ネットワーク トラフィックの属性を変更します。

ネットワーク トラフィックのマーキング方法

ネットワーク トラフィックにマーキングするためのクラス マップの作成

（注） **matchprotocol** コマンドが次のステップに含まれています。**matchprotocol** コマンドは、使用できる **match** コマンドの単なる一例です。**match** コマンドの完全なリストについては、コマンドマニュアルを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map***class-map-name* [**match-all** | **match-any**]
4. **matchprotocol***protocol-name*
5. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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-map-name* [**match-all** | **match-any**] 例： `Device(config)# class-map class1`	トラフィックを指定したクラスにマッチングするために使用するクラスマップを作成し、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。

	コマンドまたはアクション	目的
ステップ 4	**matchprotocol***protocol-name* 例： `Device(config-cmap)# match protocol ftp`	（任意）指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。 （注） **matchprotocol** コマンドは、使用できる **match** コマンドの単なる一例です。**match** コマンドは、シスコのリリースによって異なります。**match** コマンドの完全なリストについては、コマンドマニュアルを参照してください。
ステップ 5	**end** 例： `Device(config-cmap)# end`	（任意）特権 EXEC モードに戻ります。

ネットワーク トラフィックにマーキングするためのテーブル マップの作成

（注） テーブル マップを使用していない場合は、この手順をスキップし、「QoS 機能をネットワーク トラフィックに適用するためのポリシー マップの作成」に進みます。

手順の概要

1. **enable**
2. **configureterminal**
3. **table-map***table-map-name***mapfrom***from-value***to***to-value*[**default***default-action-or-value*]
4. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**table-map***table-map-name***mapfrom***from-value***to***to-value*[**default***default-action-or-value*] 例： 例： `Device(config)# table-map table-map1 map from 2 to 1`	指定した名前を使用してテーブル マップを作成し、テーブル マップ コンフィギュレーション モードを開始します。 • 作成するテーブル マップの名前を入力します。 • 個々の回線について各値のマッピングを入力します。必要に応じて、マッピングする値の各回線を入力します。 • **default** キーワードと *default-action-or-value* 引数に、値が明示的に指定されなかった場合に使用するデフォルト値（またはアクション）を設定します。

ステップ 4	**end**
	例：
	`Device(config-tablemap)#`
	`end`
		（任意）テーブル マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

QoS機能をネットワーク トラフィックに適用するためのポリシーマップの作成

はじめる前に

次の制限が QoS ポリシー マップの作成に適用されます。

- **setqos-group** コマンドを含むポリシーマップは、入力トラフィック ポリシーとしてのみ適用できます。デバイスを出るトラフィックには QoS グループ値を使用できません。
- **setcos** コマンドを含むポリシーマップは、出力トラフィック ポリシーとしてのみ適用できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **setcos***cos-value*
6. **end**
7. **showpolicy-map**
8. **showpolicy-map***policy-map***class***class-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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**policy-map***policy-map-name* 例： `Device(config)# policy-map policy1`	ポリシー マップの名前を指定して、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。

	コマンドまたはアクション	目的
ステップ 4	**class** {*class-name* | **class-default**} 例： `Device(config-pmap)# class class1`	作成するポリシーのクラス名を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。このクラスは、以前に作成したクラス マップと関連付けられます。
ステップ 5	**setcos***cos-value* 例： `Device(config-pmap-c)# set cos 2`	（任意）タイプ オブ サービス（ToS）バイトの CoS 値を設定します。 （注） **setcos** コマンドは、トラフィックのマーキング時に使用可能な **set** コマンドの一例です。他の **set** コマンドも使用できます。その他の **set** コマンドのリストについては、「ネットワーク トラフィックのマーキングに関する情報」を参照してください。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showpolicy-map** 例： `Device# show policy-map`	（任意）すべての設定済みポリシーマップを表示します。
ステップ 8	**showpolicy-map***policy-map***class***class-name* 例： `Device# show policy-map policy1 class class1`	（任意）指定したポリシー マップの指定したクラスの設定を表示します。

次の作業

実際のネットワークの必要に応じて任意の数を作成および設定します。追加のポリシー マップを作成して設定するには、「QoS機能をネットワーク トラフィックに適用するためのポリシーマップの作成」の手順を繰り返します。その後、「ポリシー マップのインターフェイスへの適用」の手順に従ってポリシー マップを適切なインターフェイスに適用します。

ポリシー マップのインターフェイスへの接続

（注）

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber* [**name-tag**]
4. **pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds** | **l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**} *policy-map-name*
7. **end**
8. **showpolicy-mapinterface***typenumber*

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* [**name-tag**] 例： `Device(config)# interface serial4/0/0`	インターフェイス タイプを設定し、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	**pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds** | **l2transport**] 例： `Device(config-if)# pvc cisco 0/16`	（任意）名前を ATM PVC に作成または割り当て、ATM 相手先固定接続（PVC）でカプセル化を指定し、ATM 仮想回線コンフィギュレーション モード開始します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。ポリシー マップを ATM PVC に適用していない場合は、下の手順 6 に進みます。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-atm-vc)# exit`	（任意）インターフェイス コンフィギュレーション モードに戻ります。 （注） この手順は、ポリシー マップを ATM PVC に適用しており、上の手順 4 を完了している場合にのみ必要です。ポリシー マップを ATM PVC に適用していない場合は、下の手順 6 に進みます。
ステップ 6	**service-policy** {**input** | **output**} *policy-map-name* 例： `Device(config-if)# service-policy input policy1`	ポリシーマップを入力または出力インターフェイスに適用します。 （注） ポリシーマップは、入力デバイスまたは出力デバイスで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシーマップを適用する方向（入力または出力）とデバイス（入力または出力）は、ネットワーク構成によって異なります。**service-policy** コマンドを使用してポリシーマップをインターフェイスに適用する場合は、ネットワーク構成に適したデバイスおよびインターフェイスの方向を選択してください。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**showpolicy-mapinterface***typenumber* 例： `Device# show policy-map interface serial4/0/0`	（任意）指定されたインターフェイスまたはサブインターフェイスとインターフェイス上の特定の PVC のどちらかで、すべてのサービス ポリシーに設定されたすべてのクラスのトラフィック統計情報を表示します。

ネットワーク トラフィックにマーキングするための設定例

例：ネットワーク トラフィックをマーキングするためのクラス マップの作成

次に、ネットワーク トラフィック マーキングに使用するクラス マップの作成例を示します。この例では、class1 というクラスが作成されました。プロトコル タイプが FTP のトラフィックがこのクラスに配置されます。

```
Device> enable
Device# configure terminal
Device(config)# class-map class1
Device(config-cmap)# match protocol ftp
Device(config-cmap)# end
```

QoS機能をネットワーク トラフィックに適用するためのポリシーマップの作成例

次に、トラフィックの分類に使用するポリシー マップの作成例を示します。この例では、policy1 というポリシーマップが作成され、class1 用に **bandwidth** コマンドが設定されました。**bandwidth** コマンドは、QoS 機能の CBWFQ を設定します。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
Router#
show policy-map policy1 class class1
Router# exit
```

（注） この例では、**bandwidth** コマンドを使用します。**bandwidth** コマンドは、QoS 機能の Class-Based Weighted Fair Queuing（CBWFQ）を設定します。CBWFQ は、設定できる QoS 機能の単なる一例です。使用する QoS 機能に適したコマンドを使用してください。

例：ポリシー マップをインターフェイスに適用する

次に、ポリシーマップをインターフェイスに適用する例を示します。この例では、policy1 という名前のポリシー マップがイーサネット インターフェイス 0 への入力方向に適用されています。

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0
Device(config-if)# service-policy input policy1
Device(config-if)# end
```

ネットワーク トラフィックのマーキングに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
MQC	「Applying QoS Features Using the MQC」モジュール
ネットワーク トラフィックの分類	「Classifying Network Traffic」モジュール

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

ネットワーク トラフィック マーキングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *19*：ネットワーク トラフィック マーキングの機能情報

機能名	ソフトウェア リリース	機能の設定情報
クラスベースのマーキング	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2 Cisco IOS XE Release 3.2SE	クラスベース パケット マーキング機能は、パケットを効率的に識別できるパケット マーキングのために、使いやすいコマンドライン インターフェイス（CLI）を提供します。 この機能は、Cisco ASR 1000 シリーズ ルータで実装されました。 この機能は、Cisco IOS XE Release 2.2 に統合されました。

機能名	ソフトウェア リリース	機能の設定情報
Enhanced Packet Marking	Cisco IOS XE Release 3.9S Cisco IOS XE リリース 3.14S	Enhanced Packet Marking 機能を使用すると、テーブル マップという変換表の一種を使用して、パケットのマーキングの値をマッピングおよび変換できます。テーブル マップはある値から別の値への等価性を確立します。たとえば、テーブルマップを使用して、パケットのサービス クラス（CoS）をパケットの precedence 値にマッピングおよび変換できます。この値のマッピングは、必要に応じてネットワークで使用するためにプロパゲートできます。 Cisco IOS XE Release 3.9S では、Cisco CSR 1000V シリーズ ルータのサポートが追加されました。 Cisco IOS XE Release 3.14S では、Cisco 4000シリーズ サービス統合型ルータのサポートが追加されました。

機能名	ソフトウェア リリース	機能の設定情報
QoS Packet Marking	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2 Cisco IOS XE Release 3.5S Cisco IOS XE Release 3.9S Cisco IOS XE リリース 3.14S	QoS パケット マーキング機能を使用すると、IP precedence ビットまたはIP Diffserv コードポイント（DSCP）をタイプ オブ サービス（ToS）バイトで設定することによってパケットにマーキングし、ローカルのQoS グループ値をパケットに関連付けることができます。 この機能は、Cisco ASR 1000 シリーズ ルータで実装されました。 この機能は、Cisco IOS XE ソフトウェア リリース2.2に統合されました。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。 Cisco IOS XE Release 3.9S では、Cisco CSR 1000V シリーズ ルータのサポートが追加されました。 Cisco IOS XE Release 3.14S では、Cisco 4000シリーズ サービス統合型ルータのサポートが追加されました。
フレームリレーPVC のIP DSCP マーキング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで実装されました。
PXF ベースのフレーム リレー DE ビット マーキング	12.2(31)SB2 15.0(1)S	PXF ベースのフレーム リレー DE ビット マーキングが Cisco IOS リリース 15.0(1)S リリースに統合されました。

第 7 章

ネットワーク トラフィックの分類

ネットワーク トラフィックの分類を使用すると、トラフィックが指定した基準に一致するかどうかに基づいて、トラフィック（つまりパケット）をトラフィック クラスまたはカテゴリに構成できます。ネットワーク トラフィックの分類は、ネットワークで多数の Quality of Service（QoS）機能をイネーブルにするための基礎です。このモジュールでは、ネットワーク トラフィックの分類に必要な概念情報と設定作業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 リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

ネットワーク トラフィックの分類に関する情報

ネットワーク トラフィックを分類する目的

ネットワーク トラフィックの分類を使用すると、現在のトラフィック タイプを確認して、トラフィックが指定した基準に一致するかどうかに基づいてトラフィック（つまりパケット）をトラフィック クラスまたはカテゴリに構成し、一部のトラフィック タイプをその他のタイプと区別して扱うことができます。ネットワーク トラフィックの分類は、ネットワークでトラフィック シェーピングやトラフィック ポリシングなどの他の QoS 機能をイネーブルにするための基礎です。

ネットワーク トラフィックの分類の目標は、ユーザ定義の基準に基づいてトラフィックをグループ化することです。その結果、ネットワーク トラフィックのグループは特定の QoS 処理に従うことができるようになります。QoS 処理には、中間ルータおよびスイッチによる高速なフォワーディング、バッファリング リソースがないためにトラフィックがドロップされる可能性の削減などがあります。

ネットワーク トラフィックをトラフィック クラスに識別および分類すること（つまり、パケットの分類）によって、トラフィックのタイプごとに処理を区別し、ネットワーク トラフィックを効率的に異なるカテゴリへと分類できます。この分類は、IP Precedence 値、Diffserv コード ポイント（DSCP）値、サービス クラス（CoS）値、ソースおよび宛先の MAC アドレス、入力インターフェイス、プロトコル タイプなど、多様な一致基準に関連付けることができます。クラスマップとポリシーマップをモジュラ QoS コマンドライン インターフェイス（MQC）とともに使用して、ネットワーク トラフィックを分類します。たとえば、QoS グループ、Frame Relay DLCI 番号、レイヤ 3 パケット長、またはその他の指定した基準に基づいて、クラス マップとポリシー マップを設定してネットワーク トラフィックを分類できます。

ネットワーク トラフィックの分類に関する制約事項

- アクセス リストを QoS ポリシーで分類のために使用するときは、次の制限事項が適用されます。
  - permit 文または deny 文の送信元アドレスまたは宛先アドレスにワイルドカードを使用すると（たとえば、任意のキーワード、172.0.0.0 などゼロを使用したマスク、サブネット マスク）、デバイスのメモリ消費が増えます。この動作は、ソフトウェア ベースの分類を使用するデバイス（Cisco ISR 4000 シリーズ デバイスまたは CSR1000v など）、およびメモリ容量が小さくて Ternary Content Addressable Memor（TCAM）が設定されているローエンドのプラットフォームにおいて特に重要です。
  - deny 文を使用すると、HW ベースの分類（ASR1k）を使用するシステムで TCAM リソースがより多く消費されます。

ネットワーク トラフィックを分類する利点

ネットワーク トラフィックを分類すると、現在のトラフィック タイプを確認し、多様なネットワーク トラフィックをトラフィック クラスに構成し、一部のトラフィック タイプをその他のタイプと区別して扱うことができます。ネットワーク トラフィックの識別と構成は、適切なQoS機能をそのトラフィックに適用するための基礎です。これによって、ネットワーク リソースを割り当て、さまざまなトラフィック タイプに最適なパフォーマンスを実現します。たとえば、高い優先度のネットワーク トラフィックまたはトラフィック マッチング固有の基準は、特別な処理のために分類できます。そのため、最適なアプリケーション パフォーマンスを達成できます。

MQC とネットワーク トラフィックの分類

ネットワーク トラフィックの分類を設定するには、モジュラ QoS コマンドライン インターフェイス（MQC）を使用します。

MQC は、次の作業を完了できる CLI 構造です。

- トラフィック クラスの定義に使用される一致基準を指定します。
- トラフィック ポリシー（ポリシー マップ）を作成します。トラフィック ポリシーには、各トラフィック クラスに実行する QoS ポリシー アクションを定義します。
- **service-policy** コマンドを使用して、インターフェイス、サブインターフェイス、またはATM相手先固定接続（PVC）にポリシーマップに指定されたポリシーアクションを適用します。

ネットワーク トラフィック分類の Match コマンドと一致基準

ネットワーク トラフィック分類を使用すると、トラフィックが 1 つまたは複数の特定基準を満たすかどうかに基づいて、トラフィックをグループ化または分類できます。たとえば、特定の IP precedence を持つネットワーク トラフィックをあるトラフィック クラスに配置し、特定の DSCP 値を持つトラフィックを別のトラフィック クラスに配置できます。そのトラフィック クラス内のネットワーク トラフィックは適切な QoS 処理に渡すことができます。これは、後述のポリシーマップで設定できます。

match コマンドを使用して、トラフィックの分類に使用する基準を指定します。次の表に、使用可能な **match** コマンドと対応する一致基準を示します。

表 *20*：*match* コマンドと対応する一致基準

match コマンド[2]	**一致基準**
matchaccessgroup	アクセス コントロール リスト（ACL）番号
matchany	任意の一致基準
matchatmclp	ATM セル損失率優先度（CLP）

match コマンド[2]	一致基準
matchclass-map	トラフィック クラス名
matchcos	レイヤ 2 サービス クラス（CoS）値
matchdestination-addressmac	MAC address
matchdiscard-class	クラス値の廃棄
matchdscp	DSCP の値
matchfield	Protocol Header Description File（PHDF）に定義されているフィールド
matchfr-de	フレーム リレー廃棄適性（DE）ビット設定
matchfr-dlci	フレームリレー データリンク接続識別子（DLCI）番号
matchinput-interface	入力インターフェイス名
matchiprtp	リアルタイム転送プロトコル（RTP）ポート
matchmplsexperimental	マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値
matchmplsexperimentaltopmost	最上位ラベルの MPLS EXP 値
matchnot	不成功の一致基準として使用する単一の一致基準値
matchpacketlength(class-map)	IP ヘッダーのレイヤ 3 パケット長
matchport-type	ポート タイプ
matchprecedence	IP precedence 値
matchprotocol	プロトコル タイプ
matchprotocol(NBAR)	Network-Based Application Recognition（NBAR）に認識されるプロトコル タイプ
matchprotocolcitrix	Citrix プロトコル
matchprotocolfasttrack	FastTrack ピアツーピア トラフィック

match コマンド[2]	一致基準
matchprotocolgnutella	Gnutella ピアツーピア トラフィック
matchprotocolhttp	Hypertext Transfer Protocol
matchprotocolrtp	RTP トラフィック
matchqos-group	QoS グループ値
matchsource-addressmac	ソース メディア アクセス コントロール（MAC）アドレス
matchstart	データグラム ヘッダー（レイヤ 2）またはネットワーク ヘッダー（レイヤ 3）
matchtag(class-map)	クラス マップのタグ タイプ
matchvlan(QoS)	レイヤ 2 の仮想ローカル エリア ネットワーク（VLAN）識別番号

[2] シスコ match コマンドは、リリースとプラットフォームによって異なります。詳細については、お使いのシスコ リリースとプラットフォームのコマンド マニュアルを参照してください。

トラフィックの分類とトラフィック マーキングの比較

トラフィックの分類とトラフィック マーキングには密接に関係があり、併用できます。トラフィック マーキングは、トラフィック クラスで実行される、ポリシー マップに指定された追加アクションとして表示できます。

トラフィックの分類を使用すると、トラフィックが特定の基準に一致するかどうかに基づいて、トラフィック クラスを構成できます。たとえば、CoS 値 2 を持つすべてのトラフィックを 1 つのクラスにグループ分けし、DSCP 値 3 を持つトラフィックを別のクラスにグループ分けします。一致基準はユーザ定義です。

トラフィックをトラフィック クラスに構成した後は、トラフィック マーキングを使用して、そのクラスに属するトラフィックの属性にマーク（つまり、設定または変更）できます。たとえば、CoS 値を 2 から 1 に変更したり、DSCP 値を 3 から 2 に変更したりできます。

トラフィックの分類に使用される一致基準は、クラス マップに **match** コマンドを設定して指定します。トラフィック マーキングによって実行するマーキング アクションは、ポリシー マップで **set** コマンドを設定して指定します。これらのクラス マップとポリシー マップは、MQC を使用して設定されます。

次の表に、トラフィック分類とトラフィック マーキングの機能の比較を示します。

表 *21*：トラフィックの分類とトラフィック マーキングの比較

機能	トラフィック分類	トラフィック マーキング
目標	トラフィックがユーザ定義の基準に一致するかどうかに基づいて、ネットワーク トラフィックを特定のトラフィック クラスにグループ化します。	ネットワーク トラフィックをトラフィック クラスにグループ化した後に、特定のトラフィック クラスのトラフィックの属性を変更します。
設定メカニズム	MQC でクラス マップとポリシー マップを使用します。	MQC でクラス マップとポリシー マップを使用します。
CLI	クラス マップでは、**match** コマンド（たとえば、**matchcos**）を使用して、トラフィック一致基準を定義します。	トラフィックの分類によって指定されたトラフィック クラスと一致基準を使用します。 さらに、ポリシー マップに **set** コマンドを使用して（たとえば **setcos**）、ネットワーク トラフィックの属性を変更します。

ネットワーク トラフィックの分類方法

ネットワーク トラフィックの分類のためのクラス マップの作成

（注） 次のタスクでは、手順4に **matchfr-dlci** コマンドを示します。**matchfr-dlci** コマンドは、フレーム リレー DLCI 番号に基づいてトラフィックを照合します。**matchfr-dlci** コマンドは、使用できる **match** コマンドの単なる一例です。その他の **match** コマンドのリストについては、「ネットワーク トラフィック分類の Match コマンドと一致基準」の項を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map***class-map-name* [**match-all**| **match-any**]
4. **matchfr-dlci***dlci-number*
5. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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-map-name* [**match-all**|**match-any**] 例： `Router(config)# class-map class1`	トラフィックを指定したクラスにマッチングするために使用するクラスマップを作成し、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。 • クラス マップ名を入力します。
ステップ 4	**matchfr-dlci***dlci-number* 例： `Router(config-cmap)# match fr-dlci 500`	（任意）クラス マップに一致基準を指定します。 （注） **matchfr-dlci** コマンドは、フレーム リレー DLCI 番号に基づいてトラフィックを分類します。**matchfr-dlci** コマンドは、使用できる **match** コマンドの単なる一例です。その他の **match** コマンドのリストについては、「ネットワーク トラフィック分類の match コマンドと一致基準」の項を参照してください。
ステップ 5	**end** 例： `Router(config-cmap)# end`	（任意）特権 EXEC モードに戻ります。

QoS機能をネットワーク トラフィックに適用するためのポリシーマップの作成

（注） 次のタスクでは、QoS 機能をネットワーク トラフィックに適用するためのポリシー マップの作成に **bandwidth** コマンドを示します。**bandwidth** コマンドは、QoS 機能の Class-Based Weighted Fair Queuing（CBWFQ）を設定します。CBWFQ は、設定できる QoS 機能の単なる一例です。使用する QoS 機能に適したコマンドを使用してください。

（注） class-default クラスを含むポリシーに基づく帯域幅設定は、ギガビット イーサネット（GigE）、シリアル、モバイル ロケーション プロトコル（MLP）、およびマルチリンク フレームリレー（MFR）などの物理インターフェイスでサポートされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps*| **remainingpercent***percentage*| **percent***percentage*}
6. **end**
7. **showpolicy-map**
8.
9. **showpolicy-map***policy-map***class***class-name*
10. Router# show policy-map
11.
12. Router# show policy-map policy1 class class1
13. **exit**

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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map policy1`	作成されるポリシー マップの名前を指定し、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。 • ポリシー マップ名を入力します。
ステップ 4	**class** {*class-name* | **class-default**} 例： `Router(config-pmap)# class class1`	クラスの名前を指定し、policy-map class コンフィギュレーションモードを開始します。このクラスは、以前に作成したクラス マップと関連付けられます。 • クラス名を入力するか、**class-default** キーワードを入力します。
ステップ 5	**bandwidth** {*bandwidth-kbps*| **remainingpercent***percentage*| **percent***percentage*} 例： `Router(config-pmap-c)# bandwidth percent 50`	（任意）ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。 • kbps の数値、帯域幅の相対的な割合、または帯域幅合計の絶対値として、帯域幅の合計を入力します。 （注） **bandwidth** コマンドは、QoS 機能の Class-Based Weighted Fair Queuing（CBWFQ）を設定します。CBWFQ は、設定できる QoS 機能の単なる一例です。使用する QoS 機能に適したコマンドを使用してください。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showpolicy-map**	（任意）すべての設定済みポリシー マップを表示します。
ステップ 8		または
ステップ 9	**showpolicy-map***policy-map***class***class-name* 例：	（任意）指定したポリシーマップの指定したクラスの設定を表示します。 • ポリシー マップ名とクラス名を入力します。
ステップ 10	Router# show policy-map	

	コマンドまたはアクション	目的
ステップ 11		
ステップ 12	Router# show policy-map policy1 class class1	
ステップ 13	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

次の作業

実際のネットワークの必要に応じて任意の数を作成および設定します。追加のポリシー マップを作成して設定するには、「QoS機能をネットワーク トラフィックに適用するためのポリシーマップの作成」の手順を繰り返します。その後、「ポリシー マップのインターフェイスへの適用」の手順に従ってポリシー マップを適切なインターフェイスに適用します。

ポリシー マップのインターフェイスへの接続

（注） ネットワークの必要に応じて、ポリシーマップをインターフェイス、サブインターフェイス、または ATM PVC に適用できます。

（注） コマンドの **match fr-dlic** を含むポリシーは、ポイントツーポイント接続を使用したフレームリレー メイン インターフェイスにしか適用できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber* [**name-tag**]
4. **pvc** [*name*] *vpi*/*vci* [**ilmi**|**qsaal**|**smds**| **l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**}*policy-map-name*
7. **end**
8. **showpolicy-mapinterface***typenumber*
9. **exit**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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***typenumber* [**name-tag**] 例： `Router(config)# interface serial4/0/0`	インターフェイス タイプを設定し、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。 • インターフェイス タイプと番号を入力します。
ステップ 4	**pvc** [*name*] *vpi*/*vci* [**ilmi**|**qsaal**|**smds**|**l2transport**] 例： `Router(config-if)# pvc cisco 0/16`	（任意）名前を ATM PVC に作成または割り当て、ATM PVC でカプセル化を指定し、ATM 仮想回線コンフィギュレーション モードを開始します。 • PVC 名、ATM ネットワーク仮想パス ID、およびネットワーク仮想チャンネル ID を入力します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。ポリシー マップを ATM PVC に適用しない場合は、ポリシーマップのインターフェイスへの接続 に進みます。
ステップ 5	**exit** 例： `Router(config-atm-vc)# exit`	（任意）インターフェイス コンフィギュレーション モードに戻ります。 （注） この手順は、ポリシー マップを ATM PVC に適用しており、ポリシーマップのインターフェイスへの接続を完了している場合にのみ必要です。ポリシー マップを ATM PVC に適用しない場合は、ポリシー マップのインターフェイスへの接続 に進みます。
ステップ 6	**service-policy** {**input** | **output**}*policy-map-name* 例： `Router(config-if)# service-policy input policy1`	ポリシーマップを入力または出力インターフェイスに適用します。 • ポリシー マップ名を入力します。

	コマンドまたはアクション	目的
		（注） ポリシーマップは、入力または出力ルータで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシーマップを適用する方向（入力または出力）とルータ（入力または出力）は、ネットワーク構成に従って変わります。**service-policy** コマンドを使用してポリシーマップをインターフェイスに適用する場合、ネットワーク構成に適したルータおよびインターフェイスの方向を選択してください。
ステップ **7**	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

ステップ **8**	**showpolicy-mapinterface***typenumber*
	
	例：
	`Router#`
	`show policy-map interface`
	`serial4/0/0`
		（任意）指定されたインターフェイスまたはサブインターフェイスとインターフェイス上の特定の PVC のどちらかで、すべてのサービス ポリシーに設定されたすべてのトラフィック クラスのトラフィック統計情報を表示します。
		• タイプと番号を入力します。

ステップ **9**	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

ネットワーク トラフィックを分類するための設定例

ネットワーク トラフィックの分類のためのクラス マップの作成例

次に、トラフィックの分類に使用するクラス マップの作成例を示します。この例では、class1 という名前のトラフィック クラスが作成されます。500 というフレームリレー DLCI 値を持つトラフィックは、このトラフィック クラスに配置されます。

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
Router(config-cmap)# end
```

（注） この例では、**matchfr-dlci** コマンドが使用されます。**matchfr-dlci** コマンドは、使用できる **match** コマンドの単なる一例です。その他の **match** コマンドのリストについては、「ネットワーク トラフィック分類の Match コマンドと一致基準」を参照してください。

match fr-dlic を含むポリシーは、ポイントツーポイント接続を使用したフレーム リレー メイン インターフェイスにしか適用できません。

QoS機能をネットワーク トラフィックに適用するためのポリシーマップの作成例

次に、トラフィックの分類に使用するポリシー マップの作成例を示します。この例では、policy1 というポリシーマップが作成され、class1 用に **bandwidth** コマンドが設定されました。**bandwidth** コマンドは、QoS 機能の CBWFQ を設定します。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
Router#
show policy-map policy1 class class1
Router# exit
```

（注） この例では、**bandwidth** コマンドを使用します。**bandwidth** コマンドは、QoS 機能の Class-Based Weighted Fair Queuing（CBWFQ）を設定します。CBWFQ は、設定できる QoS 機能の単なる一例です。使用する QoS 機能に適したコマンドを使用してください。

ポリシー マップをインターフェイスに適用する例

次に、ポリシーマップをインターフェイスに適用する例を示します。この例では、policy1 というポリシー マップが、シリアル インターフェイス 4/0 の入力方向に適用されました。

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0/0
Router(config-if)# service-policy input policy1
Router(config-if)# end
Router#
show policy-map interface serial4/0/0
Router# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
MQC	「Applying QoS Features Using the MQC」モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール
IPsec と VPN	『Configuring Security for VPNs with IPsec』モジュール
NBAR	『Classifying Network Traffic Using NBAR』モジュール
IPv6 QoS	『IPv6 Quality of Service』モジュール

関連項目	マニュアル タイトル
IPv6 MQC パケット分類	『IPv6 QoS: MQC Packet Classification』モジュール

標準

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
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 XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、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
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

ネットワーク トラフィックの分類の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *22*：ネットワーク トラフィックの分類の機能情報

機能名	リリース	機能情報
フレームリレー DLCI 番号を使用したパケットの分類	12.2(13)T Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.12	フレームリレー DLCI 番号機能を使用したパケットの分類を使用すると、パケットに関連付けられたフレームリレー データ リンク接続識別子（DLCI）番号に基づいて、トラフィックをマッチングおよび分類できます。この新しい一致基準は、IP precedence、Diffserv コード ポイント（DSCP）値、サービス クラス（CoS）などの現在使用可能な一致基準に対する追加です。 **matchfr-dlci** コマンドが追加または変更されています。

機能名	リリース	機能情報
QoS：Local Traffic Matching Through MQC	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
QoS：Match ATM CLP	Cisco IOS XE Release 2.3	QoS：Match ATM CLP 機能を使用すれば、ATM セル損失率優先度（CLP）値に基づいてトラフィックを分類することができます。 **matchatm-clp** コマンドが導入または変更されています。
QoS：MPLS EXP Bit Traffic Classification	Cisco IOS XE Release 2.3	QoS：MPLS EXP Bit Traffic Classification 機能を使用すれば、マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）値に基づいてトラフィックを分類することができます。 **matchmplsexperimental** コマンドが導入または変更されています。

第 8 章

クラスベース イーサネット CoS マッチングおよびマーキング

クラスベース イーサネット CoS マッチングおよびマーキング（802.1p と ISL CoS）機能を使用すれば、サービス クラス（CoS）値を使用してパケットをマーキングしてマッチングすることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

クラスベース イーサネット CoS マッチングおよびマーキングの前提条件

この機能を設定する場合は、先に、モジュラ QoS コマンドライン インターフェイス（CLI）（MQC）を使用してポリシー マップ（サービス ポリシーまたはトラフィック ポリシーと呼ばれることもある）を作成する必要があります。そのため、MQC を使用してポリシーを作成するための手順に精通しておく必要があります。

MQC を使用したポリシー マップ（トラフィック ポリシー）の作成方法については、『Applying QoS Features Using the MQC』モジュールを参照してください。

クラスベース イーサネット CoS マッチングおよびマーキングに関する情報

レイヤ 2 CoS 値

レイヤ 2（L2）サービス クラス（CoS）値は IEEE 802.1Q タイプとスイッチ間リンク（ISL）タイプのフレームに関係します。クラスベース イーサネット CoS マッチングおよびマーキング機能は、パケットの CoS 値を検査して、そのパケットをユーザ定義の CoS 値でマーキングすることにより、パケットを照合するようにシスコ ソフトウェアの機能を拡張します。この機能は L2 CoS から L3 Terms of Service（TOS）へのマッピングに使用できます。CoS マッチングおよびマーキングは、シスコ モジュラ QoS CLI フレームワーク経由で設定できます。

クラスベース イーサネット CoS マッチングおよびマーキングの設定方法

クラスベース イーサネット CoS マッチングの設定

次の作業では、CoS 値に基づいてトラフィックを分類するために、voice と video-and-data という名前のクラスを作成します。クラスは CoS ベース処理ポリシー マップ内で設定され、サービス ポリシーがギガビット イーサネット インターフェイス 1/0/1 から出るすべてのパケットに適用されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map***class-map-name*
4. **matchcos** *cos-value*
5. **exit**
6. **class-map***class-map-name*
7. **matchcos** *cos-value*
8. **exit**
9. **policy-map***policy-map-name*
10. **class** {*class-name* | **class-default**}
11. **prioritylevel***level*
12. **exit**
13. **class** {*class-name* | **class-default**}
14. **bandwidthremainingpercent***percentage*
15. **exit**
16. **exit**
17. **interface***typenumber*
18. **service-policy** {**input**| **output**} *policy-map-name*
19. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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-map-name* 例： `Device(config)# class-map voice`	作成するクラス マップの名前を指定し、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。

	コマンドまたはアクション	目的
ステップ 4	**matchcos** *cos-value* 例： `Device(config-cmap)# match cos 7`	CoS 値に基づいてトラフィックを照合するようにクラスマップを設定します。
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	（任意）クラスマップ コンフィギュレーション モードを終了します。
ステップ 6	**class-map***class-map-name* 例： `Device(config)# class-map video-and-data`	作成するクラス マップの名前を指定し、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。 • クラス マップ名を入力します。
ステップ 7	**matchcos** *cos-value* 例： `Device(config-cmap)# match cos 5`	CoS 値に基づいてトラフィックを照合するようにクラスマップを設定します。
ステップ 8	**exit** 例： `Device(config-cmap)# exit`	（任意）クラスマップ コンフィギュレーション モードを終了します。
ステップ 9	**policy-map***policy-map-name* 例： `Device(config)# policy-map cos-based-treatment`	事前に作成したポリシーマップの名前を指定して、ポリシーマップ コンフィギュレーション モードに入ります。
ステップ 10	**class** {*class-name* | **class-default**} 例： `Device(config-pmap)# class voice`	作成するポリシーのクラス名を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。このクラスは、以前に作成したクラスマップと関連付けられます。
ステップ 11	**prioritylevel***level* 例： `Device(config-pmap-c)# priority level 1`	プライオリティ サービスのレベルを指定します。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	（任意）ポリシー マップ クラス コンフィギュレーション モードを終了します。
ステップ 13	**class** {*class-name* | **class-default**} 例： `Device(config-pmap)# class video-and-data`	作成するポリシーのクラス名を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。このクラスは、以前に作成したクラスマップと関連付けられます。
ステップ 14	**bandwidthremainingpercent***percentage* 例： `Device(config-pmap-c)# bandwidth remaining percent 20`	クラスに割り当てる帯域幅の量を指定します。
ステップ 15	**exit** 例： `Device(config-pmap-c)# exit`	（任意）ポリシー マップ クラス コンフィギュレーション モードを終了します。
ステップ 16	**exit** 例： `Device(config-pmap)# exit`	（任意）ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 17	**interface***typenumber* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス（サブインターフェイス）タイプを設定し、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 18	**service-policy** {**input**| **output**} *policy-map-name* 例： `Device(config-if)# service-policy output cos-based-treatment`	インターフェイスの入力または出力方向のいずれかに適用するポリシー マップの名前を指定します。

	コマンドまたはアクション	目的
		（注） ポリシー マップは、入力デバイスまたは出力デバイスで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシー マップを適用する方向（入力または出力）とデバイス（入力または出力）は、ネットワーク構成によって異なります。**service-policy** コマンドを使用してポリシー マップをインターフェイスに適用する場合は、ネットワーク構成に適したデバイスおよびインターフェイスの方向を選択してください。
ステップ 19	**end** 例： `Device(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

クラスベース イーサネット CoS マーキングの設定

次の作業では、トラフィックのタイプごとに別々の CoS 値を割り当てる、cos-set という名前のポリシー マップを作成します。

（注） この作業では、voice と video-and-data という名前のクラス マップがすでに作成されているものとします。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **setcos***cos-value*
6. **exit**
7. **class** {*class-name* | **class-default**}
8. **setcos***cos-value*
9. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**policy-map***policy-map-name* 例： `Device(config)# policy-map cos-set`	事前に作成したポリシー マップの名前を指定して、ポリシー マップ コンフィギュレーション モードに入ります。
ステップ 4	**class** {*class-name* | **class-default**} 例： `Device(config-pmap)# class voice`	作成するポリシーのクラス名を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。このクラスは、以前に作成したクラス マップと関連付けられます。
ステップ 5	**setcos***cos-value* 例： `Device(config-pmap-c)# set cos 1`	パケットの CoS 値を設定します。
ステップ 6	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 7	**class** {*class-name* | **class-default**} 例： `Device(config-pmap)# class video-and-data`	作成するポリシーのクラス名を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。このクラスは、以前に作成したクラス マップと関連付けられます。
ステップ 8	**setcos***cos-value* 例： `Device(config-pmap-c)# set cos 2`	パケットの CoS 値を設定します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-pmap-c)# end`	（任意）ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

クラスベース イーサネット CoS マッチングおよびマーキングの設定例

例：クラスベース イーサネット CoS マッチングの設定

この例では、CoS 値に基づいてトラフィックを分類するために 2 つのクラス（voice と video-and-data）を作成します。CoS ベース処理ポリシー マップは、クラスのプライオリティ値と帯域幅値の設定に使用されます。サービス ポリシーは、インターフェイス ギガビット イーサネット 1/0/1 を出るすべてのパケットに適用されます。

（注） サービス ポリシーは、サービス ポリシーをサポートする任意のインターフェイスにアタッチできます。

```
Device(config)# class-map voice
Device(config-cmap)# match cos 7
Device(config-cmap)# exit
Device(config)# class-map video-and-data
Device(config-cmap)# match cos 5
Device(config-cmap)# exit
Device(config)# policy-map cos-based-treatment
Device(config-pmap)# class voice
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# exit
Device(config-pmap)# class video-and-data
Device(config-pmap-c)# bandwidth remaining percent 20
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)#  interface gigabitethernet1/0/1
Device(config-if)# service-policy output cos-based-treatment
```

例：クラスベース イーサネット CoS マーキング

```
Device(config)# policy-map cos-set
Device(config-pmap)# class voice
Device(config-pmap-c)# set cos 1
Device(config-pmap-c)# exit
```

```
Device(config-pmap)# class video-and-data
Device(config-pmap-c)# set cos 2
Device(config-pmap-c)# end
```

クラスベース イーサネット CoS マッチングおよびマーキングに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco コマンド	『Cisco IOS Master Command List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
ネットワーク トラフィックの分類	「Classifying Network Traffic」モジュール
MQC	「Applying QoS Features Using the MQC」モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

クラスベース イーサネット CoS マッチングおよびマーキングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *23*：クラスベース イーサネット *CoS* マッチングおよびマーキングの機能情報

機能名	リリース	機能情報
クラスベース イーサネット CoS マッチングおよびマーキング	12.2(5)T 15.0(1)S Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2SE	この機能を使用すれば、サービス クラス（CoS）値を使用してパケットをマーキングして照合することができます。 **match cos** コマンドと **set cos** コマンドが導入または変更されています。
ワイヤレス展開用のユーザ プライオリティ ベース QoS マーキング	Cisco IOS XE Release 3.2SE	この機能を使用すれば、ユーザ プライオリティ（CoS）値を使用してワイヤレス展開でパケットをマーキングして照合できます。

第 9 章

分類とマーキングのための QoS グループの照合と設定

この機能は、QoS グループ値に基づいてトラフィックを照合して分類できるようにします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

分類とマッチングのための QoS グループの照合と設定の前提条件

この機能を設定する場合は、先に、モジュラ QoS CLI（MQC）を使用してポリシー マップ（サービス ポリシーまたはトラフィック ポリシーと呼ばれることもある）を作成する必要があります。そのため、MQC を使用してポリシーを作成するための手順に精通しておく必要があります。MQC を使用したポリシー マップ（トラフィック ポリシー）の作成方法については、『Applying QoS Features Using the MQC』モジュールを参照してください。

分類とマーキングのための QoS グループの照合と設定の制約事項

set qos-group コマンドを含むポリシー マップは、入力トラフィック ポリシーとしてのみ適用できます。デバイスを出るトラフィックには QoS グループ値を使用できません。

分類とマーキングのための QoS グループの照合と設定に関する情報

QoS グループ値

QoS グループ値は、**set qos-group** コマンドを使用して設定される 0 ～ 99 の数値です。グループ値を使用すると、プレフィクス、自律システム、およびコミュニティ ストリングに基づいて、パケットを QoS グループに分類できます。パケットは、デバイス内で処理されている間だけ、QoS グループ値でマーク付けされます。パケットが出力インターフェイスを介して送信されるとき、QoS グループ値はパケットのヘッダーに含まれません。ただし、QoS グループ値を使用すると、パケットのヘッダーに含まれるレイヤ 2 またはレイヤ 3 フィールド（MPLS EXP、CoS、DSCP フィールドなど）の値を設定できます。

MQC と QoS グループ値に基づくトラフィックの分類とマーキング

QoS グループ値に基づいてパケットの分類とマーキングをイネーブルにするには、MQC を使用します。MQC は、トラフィック クラスおよびポリシーを作成し、QoS 機能（パケット分類など）をイネーブルにし、それらのポリシーをインターフェイスに適用するための CLI です。

MQC では、トラフィックの分類（とその後のトラフィック ポリシーとの関連付け）に使用されるトラフィック クラスを定義するために、**class-map** コマンドが使用されます。

MQC は、次の 3 つのプロセスで構成されます。

- **class-map** コマンドを使用した、トラフィック クラスの定義。
- トラフィック クラスを 1 つまたは複数の QoS 機能と関連付けてトラフィック ポリシーを作成（**policy-map** コマンドを使用）
- **service-policy** コマンドを使用してトラフィック ポリシーをインターフェイスに適用

トラフィック クラスに含まれる 3 つの主な要素は、名前、1 つ以上の **match** コマンド、そしてトラフィック クラスに複数の **match** コマンドが存在する場合に **match** コマンドを評価する方法です。トラフィック クラスの名前は、**class-map** コマンド ラインで指定します。たとえば、CLI でトラフィック クラスを設定するときに **class-mapcisco** コマンドを入力すると、トラフィック クラスの名前は「cisco」になります。

match コマンドは、パケット分類のためのさまざまな基準を指定するために使用します。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。

ポリシー マップも次の 3 つの主要素で構成されます。1 つの名前、1 つ以上の QoS 機能に関連付けるトラフィック クラス、およびネットワーク トラフィックをマーキングするために使用する個別の **set** コマンドです。

分類とマーキングのための QoS グループの照合と設定の設定方法

QoS グループ値に基づいて照合するためのクラス マップの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map***class-map-name*
4. **matchqos-group** *qos-group-value*
5. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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-map-name* 例： `Device(config)# class-map class1`	作成するクラスマップの名前を指定し、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	**matchqos-group** *qos-group-value* 例： `Device(config-cmap)# match qos-group 30`	QoS グループ値に基づいてトラフィックを照合するようにクラス マップを設定します。 • QoS グループ値の識別に使用される 0 ～ 99 の正確な値を入力します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	（任意）クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

QoS グループ値を使用したポリシー マップの作成

次に、事前設定済みのクラス（class1）を使用してポリシー マップ（policy1）を作成する例とパケットのオリジナルの 802.1P CoS 値に基づいて QoS グループ値を設定する例を示します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **setqos-groupcos**
6. **end**
7. **showpolicy-map**
8. **showpolicy-map***policy-map***class***class-name*
9. **exit**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**policy-map***policy-map-name* 例： `Device(config)# policy-map policy1`	事前に作成したポリシーマップの名前を指定して、ポリシーマップ コンフィギュレーション モードに入ります。
ステップ 4	**class** {*class-name* | **class-default**} 例： `Device(config-pmap)# class class1`	作成するポリシーのクラス名を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。このクラスは、以前に作成したクラスマップと関連付けられます。 • クラス名を入力するか、**class-default** キーワードを入力します。
ステップ 5	**setqos-groupcos** 例： `Device(config-pmap-c)# set qos-group cos`	パケットのオリジナルの 802.1P CoS 値に基づいて QoS グループ値を設定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showpolicy-map** 例： `Device# show policy-map`	（任意）すべての設定済みポリシー マップを表示します。
ステップ 8	**showpolicy-map***policy-map***class***class-name* 例： `Device# show policy-map policy1 class class1`	（任意）指定したポリシーマップの指定したクラスの設定を表示します。
ステップ 9	**exit** 例： `Device# exit`	（任意）特権 EXEC モードを終了します。

ポリシー マップのインターフェイスへの接続

はじめる前に

ポリシー マップをインターフェイスに適用する前に、MQC を使用してポリシー マップを作成する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input**| **output**} *policy-map-name*
6. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface serial4/0/0`	インターフェイス（またはサブインターフェイス）タイプを設定し、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	**pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds**] 例： `Device(config-if)# pvc cisco 0/16 ilmi`	（任意）ATM PVC の名前を作成するか、名前を割り当てて、ATM PVC 上のカプセル化タイプを指定し、ATM VC コンフィギュレーション モードを開始します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。ポリシー マップを ATM PVC に適用しない場合は、この手順を省略します。

ステップ 5	**service-policy** {**input**| **output**} *policy-map-name*
	例：
	`Device(config-if)# service-policy input policy1`
	例：
	`Device(config-if-atm-vc)# service-policy input policy1`
		インターフェイスの入力または出力方向のいずれかに適用するポリシー マップの名前を指定します。
		（注） ポリシーマップは、入力デバイスまたは出力デバイスで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシーマップを適用する方向（入力または出力）とデバイス（入力または出力）は、ネットワーク構成によって異なります。**service-policy** コマンドを使用してポリシーマップをインターフェイスに適用する場合は、ネットワーク構成に適したデバイスおよびインターフェイスの方向を選択してください。

ステップ 6	**end** 例： `Device(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードまたは ATM VC コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	例： `Device(config-if-atm-vc)# end`	

分類とマーキングのための QoS グループの照合と設定の設定例

例：分類とマーキングのための QoS グループの照合と設定

次に、QoS グループ値用のクラスマップとポリシーマップを作成し、ポリシーをインターフェイスに適用する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# class-map class1
Device(config-cmap)# match qos-group 30
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set qos-group cos
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface serial4/0/0
Device(config-if)# service-policy input policy1
Device(config-if)# end
```

分類とマーキングのための QoS グループの照合と設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco コマンド	『Cisco IOS Master Command List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』

関連項目	マニュアル タイトル
ネットワーク トラフィックの分類	「Classifying Network Traffic」モジュール
MQC	「Applying QoS Features Using the MQC」モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

分類とマーキングのための QoS グループの照合と設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *24*：分類とマーキングのための *QoS* グループの照合と設定の機能情報

機能名	リリース	機能情報
分類とマーキングのための QoS グループの照合と設定	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2SE	この機能は、QoS グループ値に基づいてトラフィックを照合して分類できるようにします。 **match qos-group** コマンドと **set qos-group** コマンドが導入または変更されています。

第 10 章

VPN 用 Quality of Service

VPN 用 QoS 機能には、インターフェイス上で Cisco IOS QoS サービスがトンネリングおよび暗号化と連携して動作するためのソリューションが用意されています。Cisco IOS ソフトウェアでパケットを分類し、適切な QoS サービスを適用してから、データを暗号化およびトンネリングできます。VPN 用 QoS 機能を使用すると、元のポート番号とソースおよび宛先 IP アドレスに基づいてパケットの分類を実行できるように、パケット内を確認できます。サービス プロバイダーはこの機能を使用して、ネットワーク内の重要なサービスまたはマルチサービスのトラフィックを高い優先度で処理できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

バーチャルプライベートネットワーク用QualityofServiceに関する情報

VPN 用 QoS

VPN 用 QoS 機能には、インターフェイス上で Cisco IOS QoS サービスがトンネリングおよび暗号化と連携して動作するためのソリューションが用意されています。Cisco IOS ソフトウェアでパケットを分類し、適切な QoS サービスを適用してから、データを暗号化およびトンネリングできます。VPN 用 QoS 機能を使用すると、元のポート番号とソースおよび宛先 IP アドレスに基づいてパケットの分類を実行できるように、パケット内を確認できます。サービス プロバイダーはこの機能を使用して、ネットワーク内の重要なサービスまたはマルチサービスのトラフィックを高い優先度で処理できます。

VPN 用 QoS の設定方法

IPsec VPN を使用した場合の QoS の設定

この作業では **qospre-classify** コマンドを使用して、パケットの QoS 事前分類をイネーブルにします。QoS 事前分類は、すべてのフラグメント化されたパケットではサポートされません。パケットがフラグメント化される場合、各フラグメントは異なる事前分類を受信できます。

（注） この作業が必要なのは、IPsec バーチャル プライベート ネットワーク（VPN）を使用している場合のみです。それ以外の場合、この作業は不要です。IPsec VPN については、『Configuring Security for VPNs with IPsec』モジュールを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptomap***map-nameseq-num*
4. **exit**
5. **interface***typenumber* [**name-tag**]
6. **qospre-classify**
7. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**cryptomap***map-nameseq-num* 例： `Router(config)# crypto map mymap 10`	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップ エントリを作成または変更します。 • クリプト マップとシーケンス番号を入力します。
ステップ 4	**exit** 例： `Router(config-crypto-map)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface***typenumber* [**name-tag**] 例： `Router(config)# interface serial4/0/0`	インターフェイス タイプを設定し、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。 • インターフェイス タイプと番号を入力します。
ステップ 6	**qospre-classify** 例： `Router(config-if)# qos pre-classify`	QoS 事前分類をイネーブルにします。
ステップ 7	**end** 例： `Router(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VPN 用 QoS の設定例

IPsec VPN を使用した場合の QoS の設定例

次に、IPsec VPN を使用する場合の QoS の設定例を示します。この例では、**crypto map** コマンドで IPsec クリプト マップ（mymap 10）を指定します。このクリプト マップには、**qos pre-classify** コマンドが適用されます。

```
Router> enable
Router# configure terminal
Router(config)# crypto map mymap 10

Router(config-crypto-map)# qos pre-classify
Router(config-crypto-map)# exit
```

VPN 用 QoS に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco コマンド	『Cisco IOS Master Command List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
ネットワーク トラフィックの分類	「Classifying Network Traffic」モジュール
MQC	「Applying QoS Features Using the MQC」モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

VPN 用 QoS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *25*：*VPN* 用 *QoS* の機能情報

機能名	リリース	機能情報
バーチャル プライベート ネットワーク用 Quality of Service	12.2(2)T Cisco IOS XE Release 3.9S	VPN 用 QoS 機能には、インターフェイス上で Cisco IOS QoS サービスがトンネリングおよび暗号化と連携して動作するためのソリューションが用意されています。Cisco IOS ソフトウェアでパケットを分類し、適切な QoS サービスを適用してから、データを暗号化およびトンネリングできます。VPN 用 QoS 機能を使用すると、元のポート番号とソースおよび宛先 IP アドレスに基づいてパケットの分類を実行できるように、パケット内を確認できます。サービス プロバイダーはこの機能を使用して、ネットワーク内の重要なサービスまたはマルチサービスのトラフィックを高い優先度で処理できます。
QoS：Traffic Pre-classification	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

第 11 章

QoS Match VLAN

QoS：Match VLAN 機能を使用すると、レイヤ 2 仮想ローカル エリア ネットワーク（VLAN）識別番号に基づいてネットワーク トラフィックを分類できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Match VLAN に関する情報

QoS Match VLAN

QoS：Match VLAN 機能を使用すると、レイヤ 2 仮想ローカル エリア ネットワーク（VLAN）識別番号に基づいてネットワーク トラフィックを分類できます。VLAN 識別番号に基づいてネットワーク トラフィックを分類するには、クラス マップを作成し、**match vlan** コマンドを使用して一致基準を指定します。その後、クラスをポリシー マップに適用し、インターフェイスに適用されたサービス ポリシー内でそのポリシー マップを使用します。

Match VLAN の設定方法

VLAN 単位のネットワーク トラフィックの分類

VLAN ベースでネットワーク トラフィックを分類するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** {**match-any** | **match-all**} *class-map-name*
4. **match vlan***vlan-id-number*
5. **exit**
6. **policy-map***policy-map-name*
7. **class***class-map-name*
8. **bandwidthpercent***percent*
9. **exit**
10. **exit**
11. **policy-map***policy-map-name*
12. **class***class-map-name*
13. **shape** {**average** | **peak**} *cir*
14. **service-policy** {**input** | **output**} *policy-map-name*
15. **exit**
16. **exit**
17. **interface***typenumber* [**name-tag**]
18. **service-policy** {**input** | **output**} *policy-map-name*
19. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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** {**match-any** | **match-all**} *class-map-name* 例： `Router(config)# class-map match-any Blue_VRF`	クラスマップを作成し、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 vlan***vlan-id-number* 例： `Router(config-cmap)# match vlan 101`	指定されたVLAN識別番号の範囲に基づいてトラフィックを照合します。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	グローバルコンフィギュレーションモードに戻ります。
ステップ 6	**policy-map***policy-map-name* 例： `Router(config)# policy-map Shared_QoS`	インターフェイスに適用可能なポリシー マップを作成し、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 7	**class***class-map-name* 例： `Router(config-pmap)# class Blue_VRF`	作成するポリシーのクラス名を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**bandwidthpercent***percent* 例： `Router(config-pmap-c)# bandwidth percent 30`	ポリシーマップに属しているクラスに割り当てる帯域幅を指定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Router(config-pmap-c)# exit`	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `Router(config-pmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**policy-map***policy-map-name* 例： `Router(config)# policy-map COS-OUT-SHAPED`	インターフェイスに適用可能なポリシー マップを作成し、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 12	**class***class-map-name* 例： `Router(config-pmap)# class FROM_WAN`	作成するポリシーのクラス名を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 13	**shape** {**average** | **peak**} *cir* 例： `Router(config-pmap-c)# shape average 9000000000`	平均レート トラフィック シェーピングを指定します。 • 認定情報レート（CIR）はビット/秒（bps）単位で指定します。
ステップ 14	**service-policy** {**input** | **output**} *policy-map-name* 例： `Router(config-pmap-c)# service-policy Shared_QoS`	QoS ポリシーとして使用される事前定義済みのポリシーマップの名前を指定します。
ステップ 15	**exit** 例： `Router(config-pmap-c)# exit`	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 16	**exit** 例： `Router(config-pmap)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 17	**interface***typenumber* [**name-tag**] 例： `Router(config)# interface FastEthernet 0/0.1`	インターフェイス タイプを設定し、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。 • インターフェイス タイプと番号を入力します。
ステップ 18	**service-policy** {**input** | **output**} *policy-map-name* 例： `Router(config-if)# service-policy output COS-OUT-SHAPED`	ポリシー マップを入力インターフェイス、仮想回線（VC）、出力インターフェイス、またはインターフェイスのサービス ポリシーとして使用される VC に適用します。
ステップ 19	**end** 例： `Router(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Match VLAN の設定例

例：VLAN 単位のネットワーク トラフィックの分類

次の例は、VLAN ベースでネットワーク トラフィックを分類する方法を示しています。VLAN 分類トラフィックは FastEthernet 0/0.1 サブインターフェイスに適用されます。

```
interface FastEthernet0/0.1
service-policy output COS-OUT-SHAPED
policy-map COS-OUT-SHAPED
      class ADMIN
      class FROM_WAN
               shape average 900000000
               service-policy Shared_QoS
policy-map Shared_QoS
      ! description -- Bandwidth sharing between VRF --
      class Blue_VRF
               bandwidth percent 3
class-map match-any Blue_VRF
      ! description -- traffic belonging to the VRF Blue --
      match vlan  101
```

QoS for Match VLAN に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco コマンド	『Cisco IOS Master Command List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
ネットワーク トラフィックの分類	「Classifying Network Traffic」モジュール
MQC	「Applying QoS Features Using the MQC」モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

QoS for Match VLAN の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *26*：*QoS for Match VLAN* の機能情報

機能名	リリース	機能情報
QoS：Match VLAN	12.2(31)SB2 Cisco IOS XE Release 2.1 15.0(1)S	QoS：Match VLAN 機能を使用すると、レイヤ 2 仮想ローカル エリア ネットワーク（VLAN）識別番号に基づいてネットワーク トラフィックを分類できます。**match vlan**（QoS）コマンドと **show policy-map interface** コマンドがこの機能よって導入または変更されています。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

第 12 章

dVTI 用インバウンド ポリシー マーキング

このマニュアルでは、ダイナミック仮想トンネル インターフェイス用インバウンド ポリシー マーキング機能の使用に関する概念情報と作業について説明します。この機能を使用すれば、マーキング指示が受信パケットに適用されるようにポリシー マップを dVTI に適用できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

dVTI 用インバウンド ポリシー マーキングの前提条件

- ポリシー マップ

dVTI 用インバウンド ポリシー マーキングの制約事項

次はサポートされていません。

- ポリシング
- Network Based Application Recognition（NBAR）ベースの分類
- Queuing
- アウトバウンド ポリシー マーキング

入力 QoS ポリシーだけがサポートされます。入力ポリシーに対して、マーキング機能だけがサポートされます。他の QoS 設定はブロックされない可能性もありますが、サポートがされることはありません。

dVTI 用インバウンド ポリシー マーキングに関する情報

インバウンド ポリシー マーキング

マーキングとは、パケットに関連した QoS 情報の設定です。dVTI 用インバウンド ポリシー マーキング機能では、マーキング指示が受信パケットに適用されるようにポリシー マップを dVTI に適用できます。

ダイナミック仮想トンネル インターフェイスの概要

DVTI によって、リモートアクセス VPN 用接続のセキュリティ保護とスケーラビリティが向上します。dVTI テクノロジーは、ダイナミック クリプト マップとトンネルを確立するためのダイナミック ハブアンドスポーク方式にとって代わるものです。

DVTI は、サーバと、リモート設定の両方に対して使用可能です。トンネルにより、各 VPN セッションに対して、仮想アクセス インターフェイスがオンデマンドで個別に提供されます。仮想アクセス インターフェイス設定は、仮想テンプレート設定からコピーされます。このコピーには、IPsec 設定と、QoS、NetFlow、ACL といった、仮想テンプレート インターフェイス上で設定されたすべての Cisco IOS XE ソフトウェア機能が含まれています。

DVTIは、他の現実のインターフェイスと同様に機能するので、トンネルがアクティブになるのと同時に、QoS、ファイアウォール、およびその他セキュリティ サービスを適用できます。QoS 機能を使用して、ネットワーク上の各種アプリケーションのパフォーマンスを向上させることが可

能です。Cisco IOS XE ソフトウェア内で提供される各種 QoS 機能の組み合わせを使用して、音声、ビデオ、またはデータ アプリケーションをサポートできます。

DVTI によって、IP アドレスを効率的に使用できるようになり、また、セキュアな接続を実現できます。DVTI によって、動的にダウンロード可能な、グループごとおよびユーザごとのポリシーを RADIUS サーバ上で設定できます。グループごとまたはユーザごとの定義を、拡張認証（Xauth）User または Unity グループを使用して作成するか、証明書から取得できます。DVTI は、標準ベースです。そのため、複数のベンダー環境における相互運用性がサポートされます。IPsec dVTI を使用すれば、リモート アクセス VPN 用のセキュリティ保護が強化された接続を作成できます。また、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）と組み合わせて、IP ネットワーク経由で集約された音声、ビデオ、およびデータを転送できます。dVTI は VPN ルーティングおよび転送（VRF）対応 IPsec の導入を容易にします。VRF は、インターフェイス上で設定されます。

dVTI には、ルータ上での最小限の設定が必要です。単一の仮想テンプレートを設定およびコピーできます。

dVTI によって、IPsec セッション用のインターフェイスが作成され、ダイナミック IPsec VTI の動的なインスタンス化および管理のための仮想テンプレート インフラストラクチャが使用されます。仮想テンプレート インフラストラクチャは、ダイナミック仮想アクセス トンネル インターフェイスを作成するために拡張されます。DVTI は、ハブアンドスポーク設定で使用されます。

Cisco IOS XE Release 3.4S で、次のサポートが追加されました。

- QoS が適用された最大 2000 のダイナミック トンネル
- 最大 4000 のダイナミック トンネル（QoS ありの 2000 と QoS なしの 2000）
- オーバーヘッドアカウンティングとキューイングを使用した高速アクセス出力シェーピング用 dVTI LLQ QoS

セキュリティ アソシエーションと dVTI

セキュリティ アソシエーション（SA）は、セキュリティ ポリシー インスタンスであり、データフローに適用される鍵素材です。IPsec SA は単方向で、セキュリティ プロトコルごとに一意です。保護されたデータ パイプには、複数の SA が必要です（プロトコルと方向ごとに 1 つずつ）。dVTI 用インバウンド ポリシー マーキング機能はマルチ SA を使用します。この機能を使用すると、複数の個別 SA が 1 つの dVTI トンネルにリンクできます。

dVTI 用インバウンド ポリシー マーキングの使用方法

dVTI 用インバウンド ポリシー マーキング機能を使用するには、先にポリシー マップを作成します。ポリシー マップを作成したら、それをインターフェイスに適用します。

ポリシー マップの作成

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class{class-name|class-default}**
5. **setipdscp***ip-dscp-value*
6. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map p-map`	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、サービス ポリシーを指定するために 1 つ以上のインターフェイスに適用可能なポリシー マップを作成します。
ステップ 4	**class{class-name|class-default}** 例： `Router(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 5	**setipdscp***ip-dscp-value* 例： `Router(config-pmap-c)# set ip dscp af21`	タイプ オブ サービス（ToS）バイトに IP DiffServ コードポイント（DSCP）値を設定することによってパケットをマーキングします。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	特権 EXEC モードに戻ります。

ポリシー マップの dVTI への適用

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacevirtual-template***number*
4. **policy-map**[**type** {**control** | **service**}] *policy-map-name*
5. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1 type tunnel`	仮想アクセス インターフェイスの作成時にダイナミックに設定および適用される仮想テンプレート インターフェイスを作成します。

	コマンドまたはアクション	目的
ステップ 4	**policy-map**[**type** {**control** | **service**}] *policy-map-name* 例： `Router(config)# policy-map input policy1`	QoS ポリシーマップ コンフィギュレーション モードを開始して、このポリシー マップをインターフェイスに適用します。
ステップ 5	**end** 例： `Router(config-pmap-c)# end`	特権 EXEC モードに戻ります。

dVTI 用インバウンド ポリシー マーキングの設定例

例 1

```
class-map match-any RT
  match ip dscp cs5  ef
!
class-map match-any DATA
  match ip dscp cs1 cs2 af21 af22
!
policy-map CHILD
  class RT
    priority
    police 200000
      conform-action transmit exceed-action drop violate-action drop
  class DATA
    bandwidth remaining percent 100
!
policy-map PARENT
  class class-default
   shape average 1000000 account user-defined xx
   service-policy CHILD
!
interface Virtual-Template 1 type tunnel
  ip vrf forwarding Customer1
  service-policy output PARENT
```

例 2：入力ポリシー マーキングの設定

dVTI のハブ側の設定例を示します。

```
aaa new-model
!
aaa authentication login default local
aaa authorization network default local
```

```
!
aaa session-id common
!
policy-map pm1
class class-default
  shape average 1280000
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp key cisco123 address 192.0.2.1
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
  key cisco
  dns 198.51.100.1
  wins 203.0.113.1
  domain cisco.com
  pool dpool
  acl 101
!
crypto isakmp profile vi
   match identity group cisco
   isakmp authorization list default
   client configuration address respond
   virtual-template 1
!
crypto ipsec transform-set trans-set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
  set transform-set trans-set
  set isakmp-profile vi
!
interface FastEthernet0/0
  ip address 203.0.113.254 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 203.0.113.255 255.255.255.0
  duplex auto
  speed 100
!
interface Virtual-Template1 type tunnel
  ip unnumbered FastEthernet0/0
  tunnel source FastEthernet0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vi
  service-policy output pm1
!
router eigrp 1
  network 192.168.1.0
  network 1.0.0.0
  no auto-summary
!
ip local pool dpool 192.0.2.1 192.0.2.254
ip route 198.51.100.1 198.51.100.254
!
access-list 101 permit ip 192.168.1.0 255.255.255.0 any
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
ネットワーク トラフィックの分類	「Classifying Network Traffic」モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

標準および RFC

標準/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 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

dVTI用インバウンドポリシーマーキングの使用に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *27* : *dVTI* 用インバウンド ポリシー マーキングの機能情報

機能名	リリース	機能情報
dVTI 用インバウンド ポリシー マーキング	Cisco IOS XE Release 3.2S	dVTI 用インバウンド ポリシー マーキング機能を使用すれば、マーキング指示が受信パケットに適用されるようにポリシー マップを dVTI に適用できます。 Cisco IOS XE Release 3.2S で、Cisco ASR 10000 のサポートが追加されました。 Cisco IOS XE Release 3.4S で、次のサポートが追加されました。 • QoS が適用された最大 2000 のダイナミック トンネル • 最大 4000 のダイナミック トンネル（QoS ありの 2000 と QoS なしの 2000） • オーバーヘッド アカウンティングとキューイングを使用した高速アクセス出力シェーピング用 dVTI LLQ QoS 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。

第 13 章

GRE トンネルの QoS トンネル マーキング

GRE トンネル用の QoS トンネル マーキング機能を使用すると、サービス プロバイダー ネットワーク内のプロバイダー エッジ（PE）ルータ上で、受信カスタマー トラフィックと送信カスタマー トラフィックの両方に関する Quality of Service（QoS）を定義して制御できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GRE トンネルの QoS トンネル マーキングの前提条件

- 受信トラフィックと送信トラフィックをマーキングするように設定するトポロジとインターフェイスを決定する必要があります。

GRE トンネルの QoS トンネル マーキングの制約事項

- GRE トンネル マーキングは、次のパスではサポートされません。
  - IPsec トンネル
  - 総称ルーティング カプセル化経由のマルチプロトコル ラベル スイッチング（MPLSoGRE）
  - レイヤ 2 トンネリング プロトコル（L2TP）

GRE トンネルの QoS トンネル マーキングに関する情報

GRE の定義

シスコが開発したトンネリング プロトコルの Generic Routing Encapsulation（GRE）は、多種多様なプロトコル パケットを IP トンネル内にカプセル化でき、リモート地点にあるシスコ ルータへの仮想ポイントツーポイント リンクを IP インターネットワークを介して構築します。

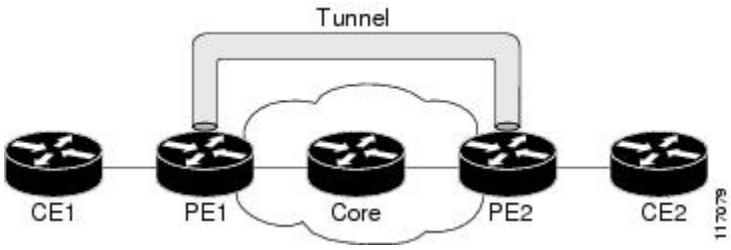
GRE トンネル マーキングの概要

GRE トンネルの QoS トンネル マーキング機能を使用すれば、サービス プロバイダー（SP）ネットワーク内の PE ルータ上で、受信カスタマー トラフィックと送信カスタマー トラフィック用の QoS を定義して制御できます。この機能を使用すると、GRE でトンネリングされたパケットのヘッダー内の IP precedence 値または DiffServ コード ポイント（DSCP）値を設定（マーク）できます。GRE トンネル マーキングは、**setip** {**dscp** | **precedence**} [**tunnel**] などの QoS マーキング コマンドを使用して実装でき、QoS トラフィック ポリシングでも実装できます。この機能を使用すると、PE ルータのトンネル インターフェイス上で GRE トンネル ヘッダーをマーキングすることによって、これまでカスタマー帯域を制御するために必要だった管理オーバーヘッドが軽減されます。

（注） **setip** {**dscp** | **precedence**} [**tunnel**] コマンドは、**set** {**dscp** | **precedence**} [**tunnel**] コマンドと同等です。

下の図は、トンネル マーキングを実行する PE1 ルータ上の着信インターフェイスを介して CE1 ルータから受信されるトラフィックを示しています。トラフィックはカプセル化（トンネリング）され、トンネル ヘッダーはルータ PE1 上でマークされます。マークされたパケットは、コアを通過し（トンネリングされ）、ルータ PE2 の出力インターフェイス上で自動的にカプセル化が解除されます。この機能は、カスタマーエッジ（CE）トラフィックの分類を単純化するために設計され、サービス プロバイダー ネットワークでのみ設定されます。このプロセスは、カスタマー サイトに透過的です。CE1 ルータと CE2 ルータは 1 つのネットワークとして存在します。

図 *2*：トンネル マーキング



GRE トンネル マーキングと MQC

GRE トンネルのトンネル マーキングを設定するには、クラス マップとポリシー マップを設定してから、そのポリシー マップを適切なインターフェイスに適用する必要があります。これら 3 つの作業は MQC を使用して実現できます。

MQC の使用方法については、『Applying QoS Features Using the MQC』モジュールを参照してください。

GRE トンネル マーキングと DSCP 値または IP precedence 値

GRE トンネル マーキングは、**setipprecedencetunnel** コマンドまたは **setipdscptunnel** コマンドで、カスタマー サイトからの受信トラフィックを伝送する PE ルータで設定します。GRE トンネル マーキングを使用すると、DSCP 値を 0 ～ 63 に設定するか、IP precedence 値を 0 ～ 7 に設定することで、GRE トンネルのヘッダーをマークし、GRE トンネル トラフィックの帯域幅と優先度を制御できます。

GRE トラフィックは、**police** コマンドの **set-dscp-tunnel-transmit** アクションおよび **set-prec-tunnel-transmit** アクション（またはキーワード）を使用して、トラフィック ポリシングに基づいてマーキングすることもできます。トンネル マーキング値は、**set-dscp-tunnel-transmit** アクションでは 0 ～ 63、**set-prec-tunnel-transmit** コマンドでは 0 ～ 7 です。トラフィック ポリシングに基づくトンネル マーキングは、conform、exceed、および violate アクション文を使用して適用できます。これを使用すれば、予想トラフィック レートに適合しないトラフィックに対して自動的に別の値を適用できます。

トンネル ヘッダーがマークされた後、GRE トラフィックはトンネルを通じてサービス プロバイダー ネットワーク内を伝送されます。このトラフィックは、出力トラフィックを他のカスタマー

サイトに伝送するPEルータのインターフェイス上でカプセル化解除されます。GREトンネルマーキングの設定はカスタマー サイトに透過的です。すべての内部設定は保持されます。

setipprecedence および **setipdscp** コマンドと **setipprecedencetunnel** および **setipdscptunnel** コマンドには違いがあります。

- **setipprecedence** コマンドと **setipdscp** コマンドは、IP パケットのヘッダー内の IP precedence 値または DSCP 値を設定するために使用します。
- **setipprecedencetunnel** および **setipdscptunnel** コマンドは、GRE トラフィックをカプセル化するトンネル ヘッダー内の IP precedence 値または DSCP 値を設定（マーク）します。
- **setipprecedencetunnel** コマンドと **setipdscptunnel** コマンドは、GRE トンネル内でカプセル化されていない出力トラフィックに影響しません。

GRE トンネル マーキングの利点

GRE トンネル マーキングは、カスタマー GRE トラフィックの帯域幅を制御するための単純なメカニズムを提供します。raffic.GRE トンネルの QoS トンネル マーキング機能のすべては、サービス プロバイダー ネットワーク内と、PE ルータ上で受信トラフィックと送信トラフィックを伝送するインターフェイス上で設定します。

GRE トンネル マーキングとトラフィック ポリシング

トラフィック ポリシングでは、インターフェイス上で送受信するトラフィックの最大レートを制御し、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）に区切ります。ネットワークでトラフィック ポリシングを使用する場合は、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 **police** コマンドの **set-dscp-tunnel-transmit** または **set-prec-tunnel-transmit** アクション（またはキーワード）を使用して、GREトンネルマーキング機能を実装することもできます。トラフィック ポリシングに基づくトンネル マーキングは、conform、exceed、および violate アクション文を使用して適用できます。これを使用すれば、予想トラフィック レートに適合しないトラフィックに対して自動的に別の値を適用できます。

GRE トンネル マーキングの値

setipdscptunnel コマンドと **set-dscp-tunnel-transmit** コマンドのトンネル マーキング値の範囲は、0 ～ 63 です。**setipprecedencetunnel** および **set-prec-tunnel-transmit** コマンドの値の範囲は、0 ～ 7 です。

GRE トンネルのトンネル マーキングの設定方法

クラス マップの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **matchip precedence***precedence-value*
5. **exit**
6. **class-map** [**match-all** | **match-any**] *class-map-name*
7. **matchip dscp***dscp-value*
8. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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** [**match-all**	**match-any**] *class-map-name* 例： `Router(config)# class-map match-any MATCH_PREC`	作成するクラス マップの名前を指定し、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。 • クラス マップは、トラフィックを差別化するために使用する条件を定義します。たとえば、クラスマップを使用して、**match** コマンドを使用して定義した一連の一致基準に基づき、音声トラフィックをデータ トラフィックから差別化できます。 （注） **match-all** または **match-any** キーワードを指定しない場合、トラフィックがそのトラフィック クラスに分類されるためには、すべての一致基準を満たさなければなりません。

	コマンドまたはアクション	目的
ステップ 4	**matchip precedence***precedence-value* 例： `Router(config-cmap)# match ip precedence 0`	指定する IP precedence 値に基づくパケット照合をイネーブルにします。 （注） 数字の省略形（0 ～ 7）または基準名（critical、flash など）で、単一の match 文で最大 4 つの一致基準を入力できます。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Router(config)# class-map match-any MATCH_DSCP`	作成するクラス マップの名前を指定し、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 7	**matchip dscp***dscp-value* 例： `Router(config-cmap)# match ip dscp 0`	ユーザが指定した DSCP 値に基づいて一致するパケットをイネーブルにします。 • このコマンドはクラス マップで使用され、パケット上の特定の DSCP 値マーキングを識別します。 • これらのマーキングされたパケットの扱いは、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、QoS ポリシーの設定を使用してユーザが定義します。
ステップ 8	**end** 例： `Router(config-cmap)# end`	（任意）特権 EXEC モードに戻ります。

ポリシー マップの作成

トンネル マーキング ポリシー マップを作成し、そのマップを特定のインターフェイスに適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **setipprecedencetunnel***precedence-value*
6. **exit**
7. **class** {*class-name* | **class-default**}
8. **setipdscptunnel***dscp-value*
9. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map TUNNEL_MARKING`	サービス ポリシーを指定するために 1 つ以上のインターフェイスに適用可能なポリシー マップを作成または修正し、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 4	**class** {*class-name*	**class-default**} 例： `Router(config-pmap)# class MATCH_PREC`	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。 • ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**setipprecedencetunnel***precedence-value* 例： `Router(config-pmap-c)# set ip precedence tunnel 3`	入力インターフェイス上で、GRE でトンネリングされるパケットのトンネル ヘッダー内の IP precedence 値を設定します。トンネル マーキング値は IP precedence が設定されている場合は 0 ～ 7 の数字になります。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-pmap-c)# exit`	QoS ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 7	**class** {*class-name* | **class-default**} 例： `Router(config-pmap)# class MATCH_DSCP`	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。 • ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**setipdscptunnel***dscp-value* 例： `Router(config-pmap-c)# set ip dscp tunnel 3`	入力インターフェイス上で、GRE でトンネリングされるパケットのトンネル ヘッダーの DiffServ コードポイント（DSCP）値を設定します。トンネル マーキング値は DSCP が設定されている場合は 0 ～ 63 の数字になります。
ステップ 9	**end** 例： `Router(config-pmap-c)# end`	（任意）特権 EXEC モードに戻ります。

インターフェイスまたは VC へのポリシー マップのアタッチ

ポリシー マップは、メイン インターフェイス、サブインターフェイス、または ATM 相手先固定接続（PVC）にアタッチできます。ポリシー マップをインターフェイスに適用するには、**service-policy** コマンドを使用し、**input** キーワードまたは **output** キーワードを指定して、インターフェイスの方向を示します。

（注） トンネル マーキング ポリシーは入力方向または出力方向に適用することができます。また、トンネル マーキング ポリシーは、サービス プロバイダー エッジ（SPE）ルータの入力物理インターフェイス上の入力ポリシーとして、または、トンネル インターフェイス上のイーグレス ポリシーとして適用できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **service-policy** {**input** | **output**}*policy-map-name*
5. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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***typenumber* 例： `Router(config)# interface GigabitEthernet 0/0/1`	インターフェイス タイプを設定し、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	**service-policy** {**input** | **output**}*policy-map-name* 例： `Router(config-if)# service-policy input TUNNEL_MARKING`	インターフェイスの入力方向または出力方向にアタッチするポリシー マップの名前を指定します。 • ポリシーマップは、入力または出力ルータで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシーマップを適用する方向（入力または出力）とルータ（入力または出力）は、ネットワーク構成に従って変わります。
ステップ 5	**end** 例： `Router(config-if)# end`	（任意）特権 EXEC モードに戻ります。

GRE トンネルのトンネル マーキングの設定の確認

GRE トンネル マーキング設定を表示するには、この手順に従って **show** コマンドを使用します。**show** コマンドは任意であり、これらのコマンドを任意の順序で入力できます。

手順の概要

1. **enable**
2. **showpolicy-mapinterface***interface-name*
3. **showpolicy-map***policy-map*
4. **exit**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**showpolicy-mapinterface***interface-name* 例： `Router# show policy-map interface GigabitEthernet0/0/1`	（任意）指定されたインターフェイスまたはサブインターフェイスですべてのサービスポリシーに関して設定されたすべてのクラスのパケット統計情報を表示します。
ステップ 3	**showpolicy-map***policy-map* 例： `Router# show policy-map TUNNEL_MARKING`	（任意）指定したサービスポリシーマップの全クラスの設定、またはすべての既存ポリシーマップに関する全クラスの設定を表示します。
ステップ 4	**exit** 例： `Router# exit`	（任意）ユーザ EXEC モードに戻ります。

トラブルシューティングのヒント

設定が想定どおりに機能していない場合は、設定の問題を修正するために次の操作を実行します。

- **showrunning-config** コマンドを使用して、コマンドの出力を分析します。

- ポリシー マップが **showrunning-config** コマンドの出力に表示されない場合は、**loggingconsole** コマンドをイネーブルにします。
- ポリシー マップをインターフェイスに再度アタッチします。

GRE トンネルの QoS トンネル マーキングの設定例

例：GRE トンネルのトンネル マーキングの設定

次に示すのは、GRE トンネル マーキングの設定例です。この例では、「MATCH_PREC」という名前のクラス マップが、DSCP 値に基づいてトラフィックを照合するように設定されています。

```
Router> enable
Router# configure terminal
Router(config)# class-map MATCH_DSCP
Router(config-cmap)# match ip dscp 0
Router(config-cmap)# end
```

設定例のこの部分では、「TUNNEL_MARKING」という名前のポリシーマップが作成され、ポリシー マップで **setipdscptunnel** コマンドが設定されています。ネットワークで DSCP を使用しない場合は、**setipdscptunnel** コマンドの代わりに **setipprecedencetunnel** コマンドを使用できます。

```
Router(config)# policy-map TUNNEL_MARKING
Router(config-pmap)# class MATCH_DSCP
Router(config-pmap-c)# set ip dscp tunnel 3
Router(config-pmap-c)# end
```

（注） **setipdscptunnel** コマンドまたは **setipprecedencetunnel** コマンドを使用して GRE トンネル マーキングをイネーブルにする場合には、この機能を設定するために設定例の次の部分は必要ありません。この例は、トラフィック ポリシングの下で GRE トンネル マーキングをイネーブルにする方法を示しています。

設定例の次の部分では、「TUNNEL_MARKING」という名前のポリシーマップが作成され、**police** コマンドを使用して適切なポリシングアクションを指定することでトラフィック ポリシングが設定されています。ネットワークで DSCP を使用する場合は、**set-prec-tunnel-transmit** コマンドの代わりに **set-dscp-tunnel-transmit** コマンドを使用できます。

```
Router(config)# policy-map TUNNEL_MARKING
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 8000 conform-action set-prec-tunnel-transmit 4 exceed-action
 set-prec-tunnel-transmit 0
Router(config-pmap-c)# end
```

設定例の次の部分では、**service-policy** コマンドの **input** キーワードを指定することで、GigabitEthernet インターフェイス 0/0/1 の着信（入力）方向にポリシー マップが適用されます。

```
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# service-policy input TUNNEL_MARKING
Router(config-if)# end
```

設定例の最後の部分では、**service-policy** コマンドの **output** キーワードを使用して、トンネル インターフェイス 0 の発信（出力）方向にポリシー マップが適用されます。

```
Router(config)# interface Tunnel 0
Router(config-if)# service-policy output TUNNEL_MARKING
Router(config-if)# end
```

例：GRE トンネルのトンネル マーキング設定の確認

ここでは、**showpolicy-mapinterface** コマンドおよび **showpolicy-map** コマンドの出力例を示します。これらのコマンドの出力は、ネットワーク上の機能設定の確認およびモニタに使用できます。

次は、**showpolicy-mapinterface** コマンドのサンプル出力です。このサンプル出力において以下の点に注意してください。

- 文字列「ip dscp tunnel 3」は、GRE トンネリングされたパケットのヘッダー内の DSCP 値を設定するように GRE トンネル マーキングが設定されていることを示します。
- 文字列「ip precedence tunnel 3」は、GRE トンネリングされたパケットのヘッダー内の precedence 値を設定するように GRE トンネル マーキングが設定されていることを示します。

```
show policy-map interface GigabitEthernet0/0/1
Service-policy input: TUNNEL_MARKING

   Class-map: MATCH_PREC (match-any)
     22 packets, 7722 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: ip precedence 0
     QoS Set
       ip precedence tunnel 3
         Marker statistics: Disabled

   Class-map: MATCH_DSCP (match-any)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: ip dscp default (0)
     QoS Set
       ip dscp tunnel 3
         Marker statistics: Disabled

   Class-map: class-default (match-any)
     107 packets, 8658 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: any
```

次は、**showpolicy-map** コマンドのサンプル出力です。このサンプル出力で、文字列「ip precedence tunnel 3」は、GRE トンネリングされたパケットのヘッダー内の IP precedence 値を設定するように GRE トンネル マーキング機能が設定されていることを示します。

```
show policy-map

Policy Map TUNNEL_MARKING
    Class MATCH_PREC
      set ip precedence tunnel 3
    Class MATCH_DSCP
      set ip dscp tunnel 3
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
MQC	「Applying QoS Features Using the MQC」モジュール
Layer 2 Tunnel Protocol Version 3（L2TPv3）トンネル用のトンネル マーキング	「QoS: Tunnel Marking for L2TPv3 Tunnels」モジュール
DSCP	「Overview of DiffServ for Quality of Service」モジュール

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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、およびフィーチャ セットに関する MIB を探してダウンロードするには、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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

GRE トンネルの QoS トンネル マーキングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *28*：*GRE* トンネルの *QoS* トンネル マーキングの機能情報

機能名	リリース	機能情報
GRE トンネルの QoS トンネル マーキング	Cisco IOS XE Release 3.5S	Generic Routing Encapsulation（GRE）トンネルの QoS トンネル マーキング機能により、サービス プロバイダー ネットワーク内の PE ルータで受信カスタマー トラフィックの QoS を定義および制御する機能が導入されます。 **matchatm-clp**、**matchcos**、**matchfr-de**、**police**、**police(tworates)**、**setipdscptunnel**、**setipprecedencetunnel**、**showpolicy-map**、および **showpolicy-mapinterface** コマンドが導入または変更されています。

第 14 章

QoS for dVTI

このモジュールでは、Dynamic Virtual Tunnel Interface（dVTI）で出力 QoS を使用するための概念的情報を示します。QoS for dVTI を使用すると、単一の dVTI トンネル テンプレートを設定できます。このテンプレートが複製され、リモート エンドポイントへの接続が提供されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

QoS dVTI の制約事項

- 階層型イーグレス ポリシーマップを使用する場合は、最上位ポリシーに class-default しか含まれません。

- プライオリティ、帯域幅、およびフェアキューは、キューイング機能を含むポリシーマップ階層の最下位レベルでのみ設定できます。
- 2000 の dVTI トンネルにしか QoS を設定できません
- 出力 QoS は dVTI トンネル テンプレートと物理出力の両方で設定することはできません。

QoS for dVTI に関する情報

1 つの dVTI テンプレートで、静的な VTI（sVTI）設定がされたルータからの複数の接続をサポートできます。通常、dVTI テンプレート設定はハブ ルータ上に保存されます。リモート スポーク ルータには常にハブ ルータを指している sVTI 設定が保存されます。QoS for dVTI は次をサポートしています。

- dVTI トンネル テンプレートからの QoS を使用した最大 4000 のダイナミック トンネル
- dVTI トンネル テンプレートに基づく QoS を使用しない新しい 2000 のダイナミック トンネルのスケーラビリティ
- dVTI トンネル テンプレートに基づく低遅延出力キューイング
- dVTI トンネル テンプレートに基づく出力シェーピング（オーバーヘッド アカウンティングありとなし）

QoS for dVTI の設定例

dVTI 用の 2 レイヤ レート LLQ の例

この例では、以下を指定する仮想トンネルインターフェイス上での 2 レイヤイーグレス ポリシーマップの設定方法を示します。

- 特定のトラフィックの ToS 固有のレート LLQ
- トンネル単位の全体レート制限
- 親シェーパーで shape コマンドの account ディレクティブを使用して、追加のオーバーヘッドを考慮

```
class-map match-any real_time
  match ip dscp cs5  ef
!
class-map match-any generic_data
  match ip dscp cs1 cs2 af21 af22
  match ip dscp default
!
policy-map child
class real_time
  police cir 200000
   conform-action transmit
   exceed-action drop
   violate-action drop
```

```
  priority
class generic_data
  bandwidth remaining percent 100
!
policy-map parent
  class class-default
  shape average 1000000 account user-defined 30
  service-policy child
!
interface Virtual-Template 1 type tunnel
  service-policy output parent
```

dVTI 用の帯域幅保証付き 2 レイヤ レート LLQ の例

この例では、以下を指定する仮想トンネルインターフェイス上での 2 レイヤイーグレス ポリシーマップの設定方法を示します。

- 特定のトラフィックの ToS 固有のレート LLQ
- その他のトラフィックの帯域幅保証
- トンネル単位の全体レート制限

```
class-map match-any real_time
match ip precedence 5
!
class-map match-any higher_data_1
match ip precedence 2
!
class-map match-any higher_data_2
match ip precedence 3
!
policy-map child
  class real_time priority
    police 5000000 conform-action transmit exceed-action drop violate-action drop
  class higher_data_1
    bandwidth remaining percent 50
  class higher_data_2
    bandwidth remaining percent 40
  class class-default
    shape average 10000000
  bandwidth remaining percent 5
!
policy-map parent
  class class-default shape average 15000000
  service-policy child
!
interface Virtual-Template 1 type tunnel
service-policy output parent
```

3 レイヤ QoS for dVTI の例

```
policy-map parent
  Class class-default
       Shape average 50000000
       Bandwidth remaining ratio 1
       Service-policy child
!
policy-map child
    Class Red
      Shape average percent 80
      Bandwidth remaining ratio 9
      Service-policy grandchild
    Class Green
```

```
      Shape average percent 80
      Bandwidth remaining ratio 2
      Service-policy grandchild
!
policy-map grandchild
  Class voice
    Priority level 1
  Class video
    Priority level 2
  Class data_gold
    Bandwidth remaining ratio 100
  Class class-default
    Random-detect dscp-based
!

interface virtual-template101 type tunnel
ip unnumbered looback101
tunnel source GigabitEthernet0/3/0
service-policy output parent
```

その他の参考資料

関連資料

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

標準および RFC

標準/RFC	タイトル

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

QoS for dVTI の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *29*：*QoS for dVTI* の機能情報

機能名	リリース	機能情報
QoS for dVTI	Cisco IOS XE Release 2.1	QoS for dVTI は単一の dVTI トンネル テンプレートを設定します。

第 15 章

MPLS EXP の分類とマーキング

QoS EXP Matching 機能を使用すれば、IP パケットのマルチプロトコル ラベル スイッチング（MPLS）Experimental ビット（EXP ビット）フィールドを変更して、ネットワーク トラフィックを分類してマーキングすることができます。このモジュールでは、MPLS EXP フィールドを使用してネットワーク トラフィックを分類してマーキングするための概念情報と設定作業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 リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

MPLS EXP の分類とマーキングの前提条件

- ルータは MPLS プロバイダー エッジ（PE）またはプロバイダー（P）ルータとして設定する必要があります。この設定には、有効なラベル プロトコルと基礎となる IP ルーティング プロトコルの設定を含めることができます。

MPLS EXP の分類とマーキングの制約事項

- MPLS の分類とマーキングは、運用可能な MPLS ネットワーク内でのみ実行できます。
- MPLS EXP の分類とマーキングは、MPLS パケット スイッチングとインポジション（簡易 IP インポジションと Ethernet over MPLS（EoMPLS）インポジション）についてはメイン ルータ インターフェイスで、EoMPLS インポジションについてはイーサネット仮想回線（EVC）またはイーサネット フロー ポイント（EFP）でサポートされます。
- EVC または EFP 上のブリッジド MPLS パケットの MPLS EXP の分類とマーキングはサポートされません。
- MPLS EXP マーキングは入力方向でのみサポートされます。
- パケットが入力で IP タイプ オブ サービス（ToS）またはサービス クラス（CoS）によって分類された場合は、出力で MPLS EXP によって再分類できません（インポジション ケース）。ただし、パケットが入力で MPLS によって分類された場合は、出力で IP ToS、CoS、または Quality of Service（QoS）グループによって再分類できます（ディスポジション ケース）。
- パケットが MPLS でカプセル化されている場合は、IP などの他のプロトコルの MPLS ペイロードをチェックして分類またはマーキングすることはできません。MPLS EXP マーキングのみが MPLS によってカプセル化されたパケットに影響します。

MPLS EXP の分類とマーキングに関する情報

MPLS EXP の分類とマーキングの概要

QoS EXP Matching 機能を使用すれば、MPLS パケットの MPLS EXP フィールドに値を設定することによってネットワーク トラフィックを整理できます。MPLS EXP フィールドで異なった値を選択することにより、輻輳時にパケットが必要なプライオリティを持つようパケットをマーキングすることができます。MPLS EXP 値の設定によって次のことが可能になります。

- トラフィックの分類
  分類プロセスでマーキングするトラフィックが選択されます。分類は、トラフィックを複数の優先順位レベル、つまり、サービス クラスに分割することによりこのプロセスを実施しま

す。トラフィック分類は、クラス ベースの QoS プロビジョニングのプライマリ コンポーネントです。詳細については、『Classifying Network Traffic』モジュールを参照してください。

- トラフィックのポリシングとマーキング
  ポリシングでは、設定されたレートを上回るトラフィックが廃棄されるか、別のドロップ レベルにマーキングされます。トラフィックのマーキングは、パケット フローを特定してそれらを区別する方法です。パケット マーキングを利用すれば、ネットワークを複数の優先プライオリティ レベルまたはサービス クラスに分割することができます。詳細については、『Marking Network Traffic』モジュールを参照してください。

MPLS 実験フィールド

MPLS Experimental ビット（EXP）フィールドは、ノードからパケットに付加される QoS 処理（Per-Hop Behavior）を定義するために使用可能な MPLS ヘッダー内の 3 ビット フィールドです。IP ネットワークでは、DiffServ コード ポイント（DSCP）（6 ビット フィールド）でクラスとドロップ優先順位が定義されます。EXP ビットは、IP DSCP でエンコードされた情報の一部を伝達するためにも、ドロップ優先順位をエンコードするためにも使用できます。

デフォルトで、Cisco IOS ソフトウェアは、IP パケットの DSCP または IP precedence の上位 3 ビットを MPLS ヘッダー内の EXP フィールドにコピーします。このアクションは、MPLS ヘッダーが初めて IP パケットに付加されたときに実行されます。ただし、DSCP または IP precedence と EXP ビットとの間のマッピングを定義することによって、EXP フィールドを設定することもできます。このマッピングは、**set mpls experimental** コマンドまたは **police** コマンドを使用して設定します。詳細については、「MPLS EXP の分類とマーキングの方法」を参照してください。

MPLS EXP の分類とマーキングのメリット

ネットワーク経由で伝送されるパケットの IP precedence フィールド値をサービス プロバイダーが変更したくない場合は、MPLS EXP フィールド値を使用して IP パケットを分類してマーキングできます。

MPLS EXP フィールド用の複数の値を選択することにより、ネットワーク輻輳が発生した場合に重大なパケットが優先されるようにそのようなパケットをマーキングすることができます。

MPLS EXP の分類とマーキングの方法

MPLS カプセル化パケットの分類

（注） MPLS EXP 最上位分類は、イーサネット仮想回線（EVC）またはイーサネット フロー ポイント（EFP）上のブリッジド MPLS パケットに対してサポートされません。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match mpls experimental topmost***mpls-exp-value*
5. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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** [**match-all**	**match-any**] *class-map-name* 例： `Router(config)# class-map exp3`	トラフィックを指定したクラスにマッチングするために使用するクラスマップを作成し、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。 • クラス マップ名を入力します。
ステップ 4	**match mpls experimental topmost***mpls-exp-value* 例： `Router(config-cmap)# match mpls experimental topmost 3`	一致基準を指定します。 （注） **match mpls experimental topmost** コマンドは、最上位ラベル ヘッダー内の EXP 値に基づいてトラフィックを分類します。
ステップ 5	**end** 例： `Router(config-cmap)# end`	（任意）特権 EXEC モードに戻ります。

インポーズされたすべてのラベルの MPLS EXP のマーキング

インポーズされたすべてのラベル エントリの MPLS EXP フィールドの値を設定するには、次の作業を実行します。

はじめる前に

ルータは、入力方向だけの MPLS EXP マーキングをサポートしています。

通常の設定では、インポジションでの MPLS パケットのマーキングが IP ToS または CoS フィールドに基づく入力分類で使用されます。ただし、クラスのデフォルト値との汎用マッチングは、**vlan** などのその他の入力属性でサポートされます。

（注） IP インポジション マーキングでは、デフォルトで、IP precedence 値が MPLS EXP 値にコピーされます。

（注） EVC設定では、CoSに基づくマッチングを実行し、EXPインポジション値を設定するポリシーマップを使用して CoS 値を EXP 値にコピーする必要があります。

（注） **set mpls experimental imposition** コマンドは、新しいまたは追加の MPLS ラベルが追加されたパケットに対してのみ機能します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-map-name*
5. **set mpls experimental imposition***mpls-exp-value*
6. **end**

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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map mark-up-exp-2`	作成されるポリシー マップの名前を指定し、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。 • ポリシー マップ名を入力します。
ステップ 4	**class***class-map-name* 例： `Router(config-pmap)# class prec012`	トラフィックを指定したクラスにマッチングするために使用するクラスマップを作成し、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。 • クラス マップ名を入力します。
ステップ 5	**set mpls experimental imposition***mpls-exp-value* 例： `Router(config-pmap-c)# set mpls experimental imposition 2`	インポーズされたすべてのラベル エントリの MPLS EXP フィールドの値を設定します。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	（任意）特権 EXEC モードに戻ります。

ラベル スイッチド パケットでの MPLS EXP のマーキング

ラベル スイッチドパケットでの MPLS EXP フィールドを設定するには、次の作業を実行します。

はじめる前に

（注） **set mpls experimental topmost** コマンドは、すでに MPLS カプセル化されたパケットにのみ作用します。

（注） ルータは入力方向の MPLS EXP マーキングだけをサポートし、MPLS EXP 分類や EVC または EFP に対するブリッジド MPLS パケットのマーキングはサポートしていません。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-map-name*
5. **set mpls experimental topmost***mpls-exp-value*
6. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map mark-up-exp-2`	作成されるポリシー マップの名前を指定し、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。 • ポリシー マップ名を入力します。
ステップ 4	**class***class-map-name* 例： `Router(config-pmap)# class-map exp012`	トラフィックを指定したクラスにマッチングするために使用するクラスマップを作成し、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。 • クラス マップ名を入力します。

	コマンドまたはアクション	目的
ステップ 5	**set mpls experimental topmost***mpls-exp-value* 例： `Router(config-pmap-c)# set mpls experimental topmost 2`	出力インターフェイスの最上位ラベルの MPLS EXP フィールド値を設定します。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	（任意）特権 EXEC モードに戻ります。

条件付きマーキングの設定

すべてのインポーズされたラベルに MPLS EXP フィールドの値を条件付きで設定するには、次の作業を実行します。

はじめる前に

（注） **set-mpls-exp-topmost-transmit** アクションは、MPLS カプセル化パケットにのみ影響します。**set-mpls-exp-imposition-transmit** アクションは、パケットに追加されたすべての新しいラベルに影響します。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-map-name*
5. **police cir***bps***bc pir***bps***be**
6. **conform-action**[**set-mpls-exp-imposition-transmit***mpls-exp-value* | **set-mpls-exp-topmost-transmit***mpls-exp-value*]
7. **exceed-action**[**set-mpls-exp-imposition-transmit***mpls-exp-value* | **set-mpls-exp-topmost-transmit***mpls-exp-value*]
8. **violate-actiondrop**
9. **end**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**policy-map***policy-map-name* 例： `Router(config)# policy-map ip2tag`	作成されるポリシーマップの名前を指定し、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。 • ポリシー マップ名を入力します。
ステップ 4	**class***class-map-name* 例： `Router(config-pmap)# class iptcp`	トラフィックと指定されたクラスを照合するために使用するクラス マップを作成し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 • クラス マップ名を入力します。
ステップ 5	**police cir***bps***bc pir***bps***be** 例： `Router(config-pmap-c)# police cir 1000000 pir 2000000`	分類するトラフィック用のポリサーを定義し、ポリシーマップ クラス ポリシング コンフィギュレーション モードを開始します。
ステップ 6	**conform-action**[**set-mpls-exp-imposition-transmit***mpls-exp-value* | **set-mpls-exp-topmost-transmit***mpls-exp-value*] 例： `Router(config-pmap-c-police)# conform-action set-mpls-exp-imposition-transmit 3`	ポリサーで指定された値に適合するパケットに対して実行するアクションを定義します。 • この例では、パケットが認定情報レート（cir）に適合する場合または適合バースト（bc）サイズ以内の場合に、MPLS EXP フィールドが 3 に設定されます。
ステップ 7	**exceed-action**[**set-mpls-exp-imposition-transmit***mpls-exp-value* | **set-mpls-exp-topmost-transmit***mpls-exp-value*] 例： `Router(config-pmap-c-police)# exceed-action set-mpls-exp-imposition-transmit 2`	ポリサーで指定された値を上回るパケットに対して実行するアクションを定義します。 • この例では、パケットが cir レートと bc サイズを超えているが、ピーク バース

	コマンドまたはアクション	目的
		ト（be）サイズ以内の場合に、MPLS EXP フィールドが 2 に設定されます。
ステップ 8	**violate-actiondrop** 例： `Router(config-pmap-c-police)# violate-action drop`	レートが最大情報レート（pir）を超えており、bc と be の範囲外のパケットに対して実行するアクションを定義します。 • 違反アクションを指定する前に、超過アクションを指定する必要があります。 • この例では、パケット レートが pir レートを超えており、bc と be の範囲外の場合に、パケットがドロップされます。
ステップ 9	**end** 例： `Router(config-pmap-c-police)# end`	（任意）特権 EXEC モードに戻ります。

MPLS EXP の分類とマーキングの設定例

例：MPLS カプセル化パケットの分類

MPLS EXP クラス マップの定義

次に、MPLS 実験値 3 を含むパケットと一致する exp3 という名前のクラス マップを定義する例を示します。

```
Router(config)# class-map exp3
Router(config-cmap)# match mpls experimental topmost 3
Router(config-cmap)# exit
```

ポリシー マップの定義とポリシー マップの入力インターフェイスへの適用

次の例では、上の例でポリシーマップを定義するために作成したクラスマップを使用します。また、この例では、入力トラフィックの物理インターフェイスにポリシー マップを適用します。

```
Router(config)# policy-map change-exp-3-to-2
Router(config-pmap)# class exp3
Router(config-pmap-c)# set mpls experimental topmost 2
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy input change-exp-3-to-2
Router(config-if)# exit
```

ポリシー マップの定義とポリシー マップの出力インターフェイスへの適用

次の例では、上の例でポリシーマップを定義するために作成したクラスマップを使用します。また、この例では、出力トラフィックの物理インターフェイスにポリシー マップを適用します。

```
Router(config)# policy-map WAN-out
Router(config-pmap)# class exp3
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy output WAN-out
Router(config-if)# exit
```

例：インポーズされたすべてのラベルでの MPLS EXP のマーキング.

MPLS EXP インポジション ポリシー マップの定義

次の例では、転送されたパケットの IP precedence 値に基づいて MPLS EXP インポジション値を 2 に設定するポリシー マップを定義します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map prec012
Router(config-cmap)# match ip prec 0 1 2
Router(config-cmap)# exit
Router(config)# policy-map mark-up-exp-2
Router(config-pmap)# class prec012
Router(config-pmap-c)# set mpls experimental imposition 2
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

MPLS EXP インポジション ポリシー マップをメイン インターフェイスに適用する

次に、ポリシー マップをギガビット イーサネット インターフェイス 0/0/0 に適用する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy input mark-up-exp-2
Router(config-if)# exit
```

MPLS EXP インポジション ポリシー マップを EVC に適用する

次に、**service instance** コマンドで指定されたイーサネット仮想接続にポリシー マップを適用する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface GigabitEthernet 0/0/0
Router(config-inf)# service instance 100 ethernet
Router(config-if-srv)# xconnect 100.0.0.1 encapsulation mpls 100
Router(config-if-srv)# service-policy input mark-up-exp-2
Router(config-if-srv)# exit
Router(config-if)# exit
```

例：ラベル スイッチド パケットの MPLS EXP のマーキング

MPLS EXP ラベル スイッチド パケット ポリシー マップの定義

次の例では、転送されたパケットの MPLS EXP 値に基づいて MPLS EXP 最上位値を 2 に設定するポリシー マップを定義します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map exp012
Router(config-cmap)# match mpls experimental topmost 0 1 2
Router(config-cmap)# exit
Router(config-cmap)# policy-map mark-up-exp-2
Router(config-pmap)# class exp012
Router(config-pmap-c)# set mpls experimental topmost 2
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

メイン インターフェイスへの MPLS EXP ラベル スイッチド パケット ポリシー マップの適用

次に、ポリシー マップのメイン インターフェイスへの適用例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy input mark-up-exp-2
Router(config-if)# exit
```

例：条件付きマーキングの設定

この例では、**ip2tag** ポリシーマップに含まれる **iptcp** クラス用のポリサーを作成し、そのポリシーマップをギガビット イーサネット インターフェイスに適用します。

```
Router(config)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# police cir 1000000 pir 2000000
Router(config-pmap-c-police)# conform-action set-mpls-exp-imposition-transmit 3
Router(config-pmap-c-police)# exceed-action set-mpls-exp-imposition-transmit 2
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# service-policy input ip2tag
```

その他の参考資料

関連資料

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

関連項目	マニュアル タイトル
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』
ネットワーク トラフィックの分類	「Classifying Network Traffic」モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール

標準および RFC

標準/RFC	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	

MIB

MIB	MIB のリンク
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 ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

MPLS EXP の分類とマーキングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *30*：*MPLS EXP* の分類とマーキングの機能情報

機能名	リリース	機能情報
QoS EXP マッチング	Cisco IOS XE Release 3.5S	QoS EXP マッチングを使用すれば、MPLS EXP フィールドを使用してパケットを分類してマーキングできます。 Cisco IOS XE Release 3.5S では、この機能が Cisco ASR 903 シリーズ ルータで導入されました。