Cisco ASR 9000 シリーズ アグリゲーション サービス ルーター モジュラ QoS サービス コンフィギュレーション ガイド リリース 4.3.x

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/

Text Part Number: OL-28380-01-J

【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

はじめに

このマニュアルでは、IOS XR QoS 設定について説明します。『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide*』の「はじめに」で説明する内容は、次のとおりです。

- マニュアルの変更履歴，xiii ページ
- マニュアルの入手方法およびテクニカル サポート，xiii ページ

マニュアルの変更履歴

表 1 に、初版後、このマニュアルに加えられた技術的な変更の履歴を示します。

表 *1*：マニュアルの変更履歴

リビジョン	日付	変更点
OL-28380-01-J	2012 年 12 月	このマニュアルの初版

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

新機能および変更された機能に関する情報

この表では、『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide*』のリリース 4.3.0 の新機能および変更情報の概要を示します。

新機能および変更された機能に関する情報

機能	説明	このリリースで導入/変更された機能	参照先
ECN サポート	この機能が導入されました。	リリース 4.3.0	明示的輻輳通知について，（76 ページ） Ecn コマンドについては、『*Cisco ASR 9000* シリーズアグリゲーション サービス ルータ モジュラ *QoS* コマンド リファレンス』の「Congestion Management」の章を参照してください。
IRB（BVI）に対する QoS	この機能が導入されました。	リリース 4.3.0	ブリッジ グループ仮想インターフェイスの QoS，（78 ページ）
衛星通信の QoS	この機能が変更されました。	リリース 4.3.0	衛星システム上の QoS，（130 ページ）

新機能および変更された機能に関する情報

機能	説明	このリリースで導入/変更された機能	参照先
疑似配線ヘッド エンドの QoS	この機能が導入されました。	リリース 4.3.0	PWHE 上の QoS, （132 ページ）

第 2 章

モジュラ QoS の概要

Quality of Service（QoS）は、トラフィック フローの優先順位付けを行い、高プライオリティ パケットの優先的な転送を実現するための技術です。 ネットワークに QoS を実装する基本的な理由は、より優れたサービスを特定のトラフィック フローに提供することです。 トラフィック フローは、送信元アドレスと宛先アドレス、送信元ソケット番号と宛先ソケット番号、およびセッション ID の組み合わせとして定義できます。 より広い意味では、トラフィック フローは、発信インターフェイスを宛先として送信された、着信インターフェイスから移動しているパケットとして説明できます。 エンドツーエンドの QoS 提供を実現するためには、トラフィック フローをすべてのルータ上で識別、分類、および優先順位付けし、ネットワーク全体のデータ転送パス上でトラフィック フローを転送する必要があります。 このモジュールでは、トラフィック フローとパケットの用語が同義的に使用されています。

ネットワーク上に QoS を実装するには、帯域幅割り当てのサポート、損失特性の向上、ネットワークの輻輳回避/管理、ネットワーク トラフィックの測定、またはネットワーク全体でのトラフィック フローのプライオリティ設定により、より優れた予測可能なネットワーク サービスを提供する QoS 機能を設定する必要があります。

ここでは、サービス プロバイダー ネットワーク内のモジュラ QoS 機能の概要について説明します。

モジュラ QoS の概要について

ネットワーク上のモジュラ QoS を設定する前に、次の概念を理解する必要があります。

- 「Cisco IOS XR ソフトウェアのディファレンシエーテッド サービス モデル」（QC-4 ページ）
- 「Access Node Control Protocol」（QC-5 ページ）
- 「Cisco IOS XR の QoS でサポートされるその他の機能」（QC-5 ページ）

Cisco IOS XR QoS 機能の利点

Cisco IOS XR の QoS 機能を使用すると、ネットワークは、さまざまなネットワーク アプリケーションとトラフィック タイプを制御し、予測どおりにサービスを提供できるようになります。ネットワーク内に Cisco IOS XR QoS を実装することにより、次の利点が得られます。

- リソースの制御。 使用するリソース（帯域幅、機器、ワイドエリア ファシリティなど）を制御できます。 たとえば、FTP転送によって消費されるバックボーン リンクの帯域幅を制限したり、重要なデータベース アクセスを優先させたりすることができます。
- 特別仕立てのサービス。 インターネット サービス プロバイダー（ISP）にとっては、QoS によって提供される制御と可視性により、慎重に調整を行った、サービス等級の差別化を顧客に提供できます。
- ミッションクリティカル アプリケーションの共存。 Cisco IOS XR の QoS 機能により、次の条件を確認できます。
  - ビジネスにとって最も重要なミッションクリティカル アプリケーションによって WAN が効率的に使用されます。
  - 時間に敏感なマルチメディアおよび音声アプリケーションで必要な帯域幅と最小遅延が利用できます。
  - リンクを使用している他のアプリケーションは、ミッションクリティカルなトラフィックに影響を与えることなく、公平なサービスを受けます。

QoS 技術

Cisco IOS XR ソフトウェア上の QoS は、次の技術に依存して、異種ネットワーク全体にエンドツーエンドの QoS を提供しています。

- パケットの分類とマーキング
- 輻輳管理
- 輻輳回避

すべての技術が使用するネットワーク環境に適しているわけではないため、これらの技術の QoS 機能を実装する前に、ネットワークのトラフィック特性を識別し、評価する必要があります。

パケットの分類とマーキング

パケットの分類/マーキング技術では、トラフィック フローを識別して、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 クラスに区切ることができます。 分類が完了すると 、他の任意の QoS アクションを実行できます。

トラフィック フローの識別は、単一のルータ内で複数の方法（アクセス コントロール リスト（ACL）、プロトコル一致、IP precedence、IP DiffServ コード ポイント（DSCP）、MPLS EXP ビット、サービス クラス（CoS））を使用して行えます。

トラフィックのマーキングは、次により実行されます。

- タイプ オブ サービス（ToS）バイトに IP precedence ビットまたは DSCP ビットを設定する。
- レイヤ 2 ヘッダー内に CoS ビットを設定する。
- インポーズされた、または最上位のマルチプロトコル ラベル スイッチング（MPLS）ラベル内に EXP ビットを設定する。
- qos-group ビットおよび discard-class ビットを設定する。

マーキングは次のように実行できます。

- 無条件：クラスアクションの一部として。
- 条件付き：ポリサーアクションの一部として。
- 条件付きと無条件の組み合わせ。

パケット マーキングの詳細な概念および設定情報に関して、無条件マーキングについては、このマニュアルの 「モジュラ QoS パケットの分類の設定（Cisco ASR 9000 シリーズ ルータ）」の に関するモジュール、および条件付きマーキングについては、このマニュアルの「モジュラ QoS の輻輳管理の設定（Cisco ASR 9000 シリーズ ルータ）」の に関するモジュールを参照してください。

デフォルトのマーキング動作

入力インターフェイスまたは出力インターフェイスが VLAN タグまたは MPLS ラベルを追加する際には、これらのタグおよびラベルに入力する CoS 値および EXP 値のデフォルト値が必要です。デフォルト値は、ポリシー マップに基づいて上書きできます。 CoS および EXP のデフォルト値は、システムに入る時点のパケット内の信頼フィールドに基づいています。 ルータは、パケット タイプおよび入力インターフェイスの転送タイプ（レイヤ 2 またはレイヤ 3）に基づいて、特定のフィールドの暗黙的な信頼を実装します。

デフォルトでは、ルータは設定されているポリシーマップなしでは IP precedence または DSCP を変更しません。 デフォルトの動作の説明は、次のとおりです。

xconnect やブリッジドメインなどの入力レイヤ 2 インターフェイスまたは出力レイヤ 2 インターフェイス上では、入力インターフェイスで追加されるすべてのフィールドに最も外側の CoS 値が使用されます。 レイヤ 2 リライトが原因で追加された VLAN タグがある場合は、新しい VLAN

タグに最も外側の着信 CoS 値が使用されます。 MPLS ラベルが追加された場合は、MPLS タグの EXP ビットに CoS 値が使用されます。

（IPv4 パケットまたは IPv6 パケットに対してルーティングされた、またはラベルにより重み付けされた）入力レイヤ 3 インターフェイスまたは出力レイヤ 3 インターフェイス上では、3 つの DSCP ビットおよび precedence ビットが着信パケット内で識別されます。 MPLS パケットの場合は、最も外側のラベルの EXP ビットが識別され、この値は、入力インターフェイスで追加されるすべての新しいフィールドに使用されます。 MPLS ラベルが追加された場合は、識別された precedence 値、DSCP 値、または MPLS EXP 値が、新たに追加された MPLS タグの EXP ビットに使用されます。

プロバイダー バックボーン ブリッジ（PBB）の設定

PBB 設定では、パケットが PBB カプセル化を使用して顧客ネットワークからサービス プロバイダー ネットワークに入る際に、バックボーン VLAN タグ（B タグ）で使用されるサービス クラス（CoS）と廃棄適性インジケータ（DEI）、および PBB ヘッダーのサービス インスタンス タグ（I タグ）が、デフォルトでは着信パケットの最上位タグの CoS および DEI になります。

パケットがサービス プロバイダーから顧客ネットワークに移動すると、PBB ヘッダーが削除され、顧客インターフェイス上でインポーズされるすべてのタグにおいて、I タグの CoS および DEI がデフォルトで使用されます。 デフォルトのマーキングはインポーズされたタグに対してのみ実行され、既存のタグまたは変換されたタグには実行されません。

輻輳管理

輻輳管理技術は、発生した後に輻輳を制御します。 ネットワーク要素が着信したトラフィックのオーバーフローを処理するための 1 つの方法は、キューイング アルゴリズムを使用してトラフィックを並べ替え、それを出力リンク上で優先順位付けする何らかのサービス手段を決定することです。

Cisco IOS XR ソフトウェアにより、ストリクト プライオリティ キューイング（PQ）を Modified Deficit Round Robin（MDRR）スケジューリング メカニズムに提供する低遅延キューイング（LLQ）機能が実装されます。 LLQ とストリクト PQ では、音声などの遅延に影響されやすいデータを、他のキューのパケットをキューから取り出す前にキューから取り出して送信できます。

Cisco IOS XR ソフトウェアには、クラスベースのシェーピングだけではなく、クラス単位で使用可能なトラフィック ポリシング機能が含まれています。

トラフィック ポリシング機能では、ユーザ定義の基準に基づいてトラフィック クラスの入力または出力の伝送レートを制限し、IP precedence、QoS グループ、DSCP 値などの設定値によりパケットをマーキングできます。

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

Cisco IOS XR ソフトウェアでは、パラメータがクラス単位で適用される CLI メカニズムを使用したクラスベースのトラフィック シェーピング方式がサポートされます。

輻輳管理に関する詳細な概念および設定情報については、Cisco ASR 9000 シリーズ ルータでのモジュラ QoS の輻輳管理の設定に関するモジュールを参照してください。

輻輳回避

輻輳回避技術では、トラフィック フローをモニタすることにより、問題が発生する前に、共通ネットワークおよびインターネットワークのボトルネックでの輻輳を予測し回避します。 これらの技術は、輻輳状況下においてリアルタイム クリティカルとして分類されているトラフィック（ビデオ ストリームなど）の優先的な処理を実現すると同時に、ネットワーク スループ ットおよびキャパシティ使用率を最大化しつつ、パケットの損失や遅延を最小限に抑えるよう設計されています。 Cisco IOS XR ソフトウェアでは、ランダム早期検出（RED）、重み付け RED（WRED）、およびテール ドロップによる QoS 輻輳回避機能がサポートされます。

輻輳管理に関する詳細な概念および設定情報については、このガイドの Cisco ASR 9000 シリーズ ルータでのモジュラ QoS の輻輳管理の設定に関するモジュールを参照してください。

Cisco IOS XR ソフトウェアのディファレンシエーテッド サービス モデル

Cisco IOS XR ソフトウェアでは、異なる QoS 要件を満たすことが可能な複数サービス モデルであるディファレンシエーテッド サービスがサポートされます。 しかし、統合サービス モデルと異なり、ディファレンシエーテッド サービスを使用するアプリケーションは、データを送信する前に明示的にルータにシグナリングを行いません。

差別化サービスでは、ネットワークは各パケットによって指定された QoS に基づいて特定の種類のサービスを提供しようとします。 この指定はさまざまな方法で行われます。たとえば、IP パケット内の IP precedence ビットの設定や、送信元アドレスと宛先アドレスが使用されます。 ネットワークでは、この QoS 仕様に基づいてトラフィックのマーキング、形成、およびポリシングを行い、インテリジェント キューイングを実行します。

ディファレンシエーテッド サービス モデルは、いくつかのミッションクリティカル アプリケーションで使用されたり、エンドツーエンド QoS を提供するために使用されます。 一般に、このサービス モデルでは、比較的粗いレベルのトラフィック分類が行われるため、集約フローに適しています。

Access Node Control Protocol

Access Node Control Protocol（ANCP）は、QoS 関連、サービス関連、加入者関連の操作を実行するために、サービス指向の集約デバイスとアクセス ノード（AN）間のコントロール プレーン（DSLAM など）を作成します。 ANCP ネットワーク アクセス サーバ（NAS）は、ANCP 隣接（ANCP ネイバーとのセッション）を受け入れて維持し、ANCP メッセージの送受信を行います。

ANCP を使用すると、AN ポートと VLAN サブ インターフェイス間でのスタティック マッピングを行うことができ、これにより、ANCP サーバが受信した特定の加入者の DSL レートの更新を、その加入者に対応する QoS 設定に適用できます。 ANCP 経由で受信した DSL トレイン レートは、

ルータの加入者側インターフェイスとサブインターフェイスのシェーピング レートを変更するために使用されます。

Cisco IOS XR の QoS でサポートされるその他の機能

ここでは、Cisco IOS XR ソフトウェア上での QoS 実装において重要な役割を担う、その他の機能について説明します。

モジュラ QoS コマンドライン インターフェイス（MQC）

Cisco IOS XR ソフトウェアでは、モジュラ QoS コマンドライン インターフェイス（MQC）機能を介して QoS 機能を使用します。 *MQC* はコマンドライン インターフェイス（CLI）構造を採用しています。これを使用すると、ポリシーを作成し、作成したポリシーをインターフェイスにアタッチできます。 1 つのトラフィック ポリシーには、1 つのトラフィック クラスと 1 つ以上の QoS 機能が含まれます。トラフィック クラスは、トラフィックの分類に使用されます。これに対して、トラフィック ポリシーの QoS 機能は、分類されたトラフィックの処理方法を決定します。MQC の主な目的の 1 つは、プラットフォームに依存しないインターフェイスを提供することにより、シスコ プラットフォーム全体の QoS を設定することです。

MQC 機能に関する詳細な概念および設定情報については、このマニュアルの Cisco ASR 9000 シリーズ ルータでのモジュラ QoS パケットの分類の設定に関するモジュールを参照してください。

ファブリック QoS

ファブリック QoS 向けの個別の設定はありません。ファブリックのプライオリティは、入力サービス ポリシーのプライオリティ アクションから取得されます。

次の作業

トラフィック フローの識別およびマーキングを含むパケット分類機能を設定するには、このマニュアルの Cisco ASR 9000 シリーズ ルータでのモジュラ QoS パケットの分類の設定に関するモジュールを参照してください。

キューイング、スケジューリング、ポリシング、およびシェーピング機能を設定するには、このマニュアルの Cisco ASR 9000 シリーズ ルータでのモジュラ QoS の輻輳管理の設定に関するモジュールを参照してください。

WRED および RED 機能を設定するには、このマニュアルの「Configuring Modular QoS Congestion Avoidance on Cisco ASR 9000 Series Routers」モジュールを参照してください。

Access Node Control Protocol（ANCP）機能を設定するには、このマニュアルの「Configuring Access Node Control Protocol on Cisco ASR 9000 Series Routers」モジュールを参照してください。

その他の関連資料

ここでは、QoS の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
初期システム起動と設定	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
マスター コマンド リファレンス	『*Cisco ASR 9000 Series Aggregation Services Router Master Command Listing*』
QoS コマンド	『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』
ユーザ グループとタスク ID	『Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide』の「Configuring AAA Services on Cisco ASR 9000 Series Router」モジュール

標準

標準	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 リンク
CISCO-CLASS-BASED-QOS-MIB	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

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
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

第 3 章

Access Node Control Protocol の設定

Access Node Control Protocol（ANCP）は、QoS 関連、サービス関連、加入者関連の操作を実行するために、サービス指向の集約デバイスとアクセス ノード（AN）間のコントロール プレーン（DSLAM など）を作成します。 ANCP サーバは ANCP 隣接（ANCP ネイバーとのセッション）、ANCP メッセージの送信と受信を受け入れ、維持します。 ANCP では、ANCP サーバが受信した、特定の加入者の DSL レート更新がその加入者に対応する QoS 設定に適用されるように ANCP ポートと VLAN サブインターフェイスの間でスタティック マッピングできます。 ANCP 経由で受信した DSL トレイン レートは、ルータの加入者側インターフェイスとサブインターフェイスのシェーピング レートを変更するために使用されます。 ANCP はルート プロセッサ（RP）の 1 つのプロセスとして動作します。

このモジュールでは、ANCP の実装に関する概念的および設定情報を提供します。

ラインカード、SIP および SPA のサポート

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
Access Node Control Protocol	yes	no

Cisco ASR 9000 シリーズ ルータ上でのアクセス ノード プロトコルの設定に関する機能の履歴

リリース	変更内容
リリース 3.7.2	Access Node Control Protocol 機能が導入されました。
リリース 3.9.0	イーサネット バンドル上の VLAN インターフェイスへの ANCP ポート マッピングが追加されました。
リリース 4.0.0	マルチシャーシ リンク集約上の ANCP が導入されました。

- ANCP の設定の前提条件，12 ページ

ANCP の設定の前提条件

ANCP の設定に関する制約事項

次の制限は、ネットワークの ANCP の設定時に適用されます。

- Cisco IOS XR Release 3.7.2 では、レート アダプティブ モードだけがサポートされます。
- VPN ルーティングおよび転送（VRF）認識は、Cisco IOS XR リリース 3.7.2 ではサポートされません。 ANCP のトラフィックを受信するすべての IP インターフェイスはデフォルトの VRF にある必要があります。
- IPv6 を介した ANCP は Cisco IOS XR Release 3.7.2 ではサポートされません。
- ANCP を使用してイーサネットとイーサネットバンドルポート上の VLAN サブインターフェイスだけを AN ポートにマッピングできます。

ANCP の設定に関する情報

ANCP を実装するには、次の概念について理解する必要があります。

ANCP 隣接

ANCP サーバはアクセス ノードからの TCP 接続を許可します。 ANCP ネイバーは、ANCP サーバとの隣接関係を確立するアクセス ノードです。 ANCP はグローバルに設定され、IP 対応であれば ANCP メッセージが物理インターフェイスまたは論理インターフェイスのどちらで受信されるかは制限されていません。

TCP は各アクセス ノードの個別の接続ソケットを作成します。 アクセス ノードが ANCP メッセージで明示的に識別されていないため、TCP ソケットが ANCP サーバの ANCP 隣接識別子として機能します。

ANCP ネイバー間の TCP 接続が行われると、ANCP 隣接プロトコルはその接続上で ANCP セッションを確立し、ANCP 機能についてネゴシエーションを行います。 ANCP ネイバー 1 つにつき

1 つの ANCP セッションがあります。 ANCP セッション情報は、対応するネイバーの情報のサブセットになります。

ANCP プロトコルはダイナミック ネイバー検出をサポートしているので、アクセス ノードの設定は必要ではありません。 ANCP ネイバーは ANCP サーバに静的に事前設定することもできます。このような場合、アクセス ノードは ID で明示的に識別されます。ID は ANCP 隣接プロトコル メッセージの **sender-name** フィールドと一致する必要があります。

ネイバーとの隣接関係のタイミング

隣接タイマーは、ANCP セッション確立の異なるステージ間の最大遅延および ANCP キープアライブの間隔を定義します。

ANCP 隣接のライフタイムは、隣接プロトコルによって制御されます。 ピア アクセス ノードとの同期が失われると（たとえば隣接のデッド タイマーが切れると）、ANCP サーバによって隣接関係が削除され、ベースとなる TCP 接続が閉じます。

ANCP メッセージ

Port Up と Port Down の 2 つの ANCP メッセージ タイプが、ANCP サーバによって処理されます。Port Up メッセージには、DSL レート情報が含まれます。Port Down メッセージは、対応するアクセス回線が利用できないことを示します。 Port Up メッセージからの DSL レート更新は、QoS サブシステムが使用できます。 Port Down メッセージは ANCP ポートのステートを内部的に追跡するために使用されます。

これらのメッセージは、ANCP 隣接が確立された後でサーバだけで受信できます。 ただし、Port Up メッセージを受信すると、含まれる DSL レート情報は、AN-port-to-interface マッピングがそのポートに設定されている場合、無期限に有効と見なされます。 これは、このポートの別の Port Up メッセージによって上書きされるかまたは手動で削除されるまで AN ポート データベースに保存されます。 隣接の削除または Port Down メッセージの受信は表示およびトラブルシューティングの目的でデータベースに反映されますが、DSL レート情報は無効にはなりません。

ポート マッピング

AN ポートは、VLAN サブインターフェイスにスタティックにマッピングされます（AN-port-to-interface マッピングと呼ばれます）。 これは加入者線に対して設定された、少なくとも 1 つの VLAN サブインターフェイスがあることを示します。 AN ポートにマッピング可能なインターフェイスの数に制限はありません。

AN ポートにマッピングされている VLAN サブインターフェイスを作成または削除できます。マッピングが設定されている場合、VLAN サブインターフェイスは ANCP モジュール内で名前で参照されます。 この名前は、インターフェイスの作成および削除の通知に使用され、DSL レートの更新に使用する情報を提供します。

AN ポート データベースは Port Up メッセージから学習したすべてのポートに対して維持されます。 このデータベースには、AN-port-to-interface マッピング データベースも含まれます。 AN ポー

トの Port Up メッセージが到着して、インターフェイスがそのポートにマッピングされていない場合、レート情報は、AN ポート データベースに保存されますが、パブリッシュされません。 そのポートのマッピングが設定されている場合、マッピングを設定する前にこのポートで受信された ANCP メッセージを識別するために、AN ポート データベースがスキャンされます。 検出された場合は、既知のレートがパブリッシュされます。

比率調整

ANCP では、システムにレート更新をパブリッシュする前に、Port Up メッセージで報告された DSL 回線レートに補正係数を適用できます。 この補正係数または比率調整は、DSL タイプとアクセス カプセル化タイプ（ATM やイーサネット）ごとのグローバル コンフィギュレーション モードで設定可能です。 DSL タイプおよびカプセル化タイプは Port Up メッセージの必須のタイプ、長さ、値（TLV）のデータで提供されます。

（注） デフォルト以外のループ タイプ（イーサネット）の比率調整機能を使用するには、DSLAM はオプションのアクセス ループ カプセル化サブ TLV をサポートする必要があります。

ANCP レート アダプティブ モード情報は、特定の加入者線に使用できる最大帯域幅（シェーピング レート）を決定するために ANCP モジュールによって処理されます。 固定補正係数が、異なる DSL テクノロジーのオーバーヘッドを考慮して、DSL タイプに基づいて ANCP の帯域幅に適用されます。 たとえば、特定の加入者の ANCP 帯域幅が 15 Mbps の場合、DSL テクノロジーのオーバーヘッドが原因で、その加入者の有効な帯域幅は 15 Mbps の 80 % である 12 Mbps に制限されます。 この修正された有効帯域幅は、加入者のトラフィックの最大レートを制限するために QoS モジュールに伝えられます。

（注） ANCP 比率は ANCP 比率が現在設定されている QoS シェーピング レートより大きい場合に限り QoS シェーピング レートとして使用されます。 （QoS で使用される ANCP 比率は、最も近い 128 kbps の単位に切り捨てられます）。

ANCP トラフィックの優先順位

輻輳時には、Cisco ASR 9000 シリーズ ルータは、ネットワーク アクセス サーバ（NAS）とアクセス ノード（AN）間の集約ネットワークで他のトラフィックより ANCP メッセージにプライオリティを設定できるように、ANCP メッセージに高プライオリティとしてマークします。

プロセスの再起動

プロセスの再起動時に、ANCP ネイバーとの TCP 接続は一般的にドロップします。 ANCP サーバがオンラインに戻ると、TCP 接続および ANCP セッションは、ネイバーによって再確立されます。 サーバへの再接続時に、DSLAM はすべてのアクティブなポートの Port Up メッセージを送信

します。 再起動前に受信されたパブリッシュされているレート情報は ANCP 設定に復元されます。 再起動がクラッシュが原因で発生した場合は、パブリッシュされたデータと設定データの間に競合が検出され、パブリッシュされたデータは修正されます。

ANCP および QoS の相互作用

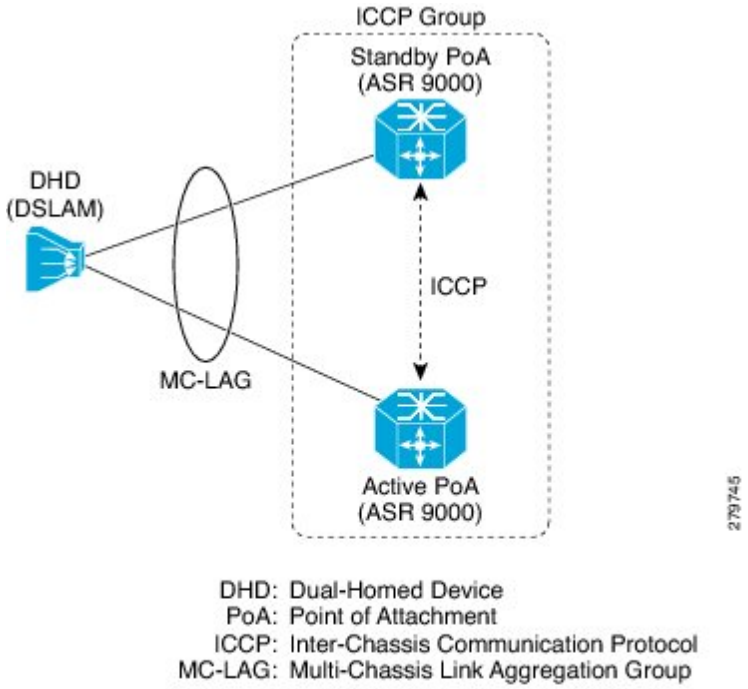
ANCP 値が適切に適用されると、設定された QoS のシェーパー値を上書きします。 誤って適用された ANCP 値の例、および ANCP 値が正しく適用された場合の QoS との相互作用の例については、ANCP および QoS の相互作用：例の項を参照してください。

マルチシャーシ リンク集約

マルチ シャーシのリンク集約（MC-LAG）は、Cisco ASR 9000 シリーズ ルータの接続に Digital Subscriber Line Access Multiplexer（DSLAM）の単純な冗長メカニズムを提供します。 冗長性は、2 台のルータへのデュアルホーム接続を可能にすることによって実現されます。 DSLAM はデュアル ホーム接続を単一の LAG として見なしているため、DSLAM でソフトウェアが複雑になることはありません。 MC-LAG 用語では、DSLAM はデュアルホーム接続デバイス（DHD）と呼ばれ、各ルータは接続ポイント（PoA）と呼ばれます。 MC-LAG の詳細については、『*Cisco ASR*

9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide』を参照してください。

図 *1*：*MC-LAG* による *ASR 9000* シリーズ ルータへの *DSLAM* の接続



MC-LAG 上の ANCP

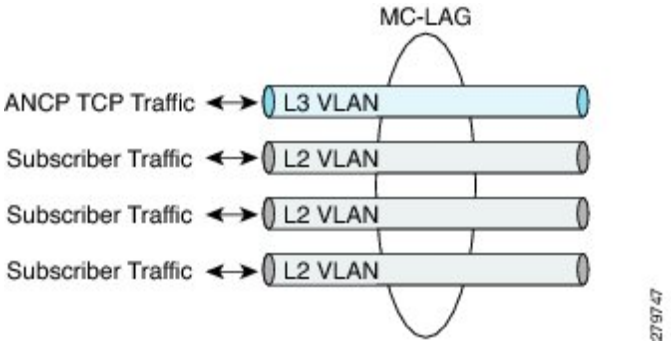
Access Node Control Protocol（ANCP）は DSLAM への MC-LAG 接続を含むネットワーク トポロジをサポートするために必要です。 CPE 回線は DSLAM に接続し、レート アダプティブ DS との信号品質に基づいて回線速度を調整します。 アップリンクは、DSLAM にルータを接続します。 回線速度がアップリンクより低いデータ レートに調整されると、加入者データが DSLAM で失われる可能性があります。 データの損失を防ぐために、DSLAM は ANCP により新しい DSL レートをルータに通知し、アップリンクのデータ レートが CPE 回線のデータ レートを超えないようにダウンストリーム シェーピングをルータに動的に適用します。

ANCP は、加入者回線にマッピングされた MC-LAG VLAN サブインターフェイスに、学習した DSLAM 加入者回線の DSL レート データを適用します。 レートは、QoS のシェーパーに適用されます。 ANCP が MC-LAG VLAN サブインターフェイスに適用した DSL レートは、ICCP（シャーシ間通信プロトコル）を使用して、MC-LAG のスタンバイ PoA で実行している ANCP アプリケーションに MC-LAG のアクティブ PoA 上で実行する ANCP アプリケーションによって配布されます。 MC-LAG のスタンバイ PoA の ANCP は、対応する MC-LAG VLAN サブインターフェイスに DSL レート データを適用します。 MC-LAG のアクティブ ロールをスタンバイ PoA の 1 つが担う原因になるイベントが発生した場合、新しいアクティブ PoA の ANCP アプリケーションはすでに

MC-LAG VLAN サブインターフェイスのシェーパーに DSL レートを適用しているので、この LAG がアクティブになり、輻輳とそれに続くデータの損失が DSLAM に発生しなかった場合に正しい DSL レートが適用されます。

DSLAM は TCP 接続を介してルータとの ANCP 隣接関係を確立します。 DSLAM 加入者回線の DSL レートはこの TCP 接続を介して伝達されます。 DSL レートは加入者回線にマッピングされているレイヤ 2 VLAN サブインターフェイスに適用されます。 MC-LAG のレイヤ 2 VLAN サブインターフェイスの DSL レートの送信に使用する ANCP TCP 接続は、L2VLAN サブインターフェイスと同じ MC-LAG にあるレイヤ 3 VLAN サブインターフェイス上にある必要があります。 この制約は、MC-LAG あたりの DSLAM とルータ間で 1 つの ANCP TCP 接続があることを示していることに注意してください。

図 *2*：*MC-LAG VLAN* サブインターフェイス上の *ANCP*



MC-LAG のアクティブ PoA がスタンバイになると、DSLAM ANCP TCP 接続は終了します。 DSLAM は MC-LAG のアクティブ ロールを担う PoA との ANCP TCP 接続を再確立します。

シスコでの ANCP の設定方法

ここでは、次のタスクの手順を示します。

- ANCP のイネーブル化
- ANCP サーバ送信元名の設定
- ANCP ネイバーの設定
- VLAN サブインターフェイスへの AN ポートのマッピング
- ANCP 比率調整の設定

ANCP のイネーブル化

ANCP をイネーブルにするには、グローバル コンフィギュレーション モードで **ancp** コマンドを使用します。

前提条件

このコマンドを使用するには、ANCP の適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。

手順の概要

1. configure RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)#
2. ancp RP/0/RSP0/CPU0:router(config)# ancp
3. end
4. または **commit**
5. show ancp summary [statistics][detail] RP/0/RSP0/CPU0:router# show ancp summary

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)#	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 2	ancp RP/0/RSP0/CPU0:router(config)# ancp	ANCP をイネーブルにします。
ステップ 3	end	

ステップ 4	または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-ancp)# end`
	または
	`RP/0/RSP0/CPU0:router(config-ancp)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

ステップ 5	show ancp summary [statistics][detail] RP/0/RSP0/CPU0:router# show ancp summary	（任意）ANCP の要約と一般的な設定情報を表示します。

ANCP サーバ送信元名の設定

ANCP サーバ送信元名は DSLAM への隣接プロトコル メッセージで ANCP サーバによって使用されます。

手順の概要

1. configure RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)#
2. ancp server sender-name {H.H.H | A.B.C.D} RP/0/RSP0/CPU0:router(config)# ancp server sender-name 0013.1aff.c2bd
3. end
4. または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)#	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 2	ancp server sender-name {H.H.H | A.B.C.D} RP/0/RSP0/CPU0:router(config)# ancp server sender-name 0013.1aff.c2bd	ローカル送信元の名前を設定します。
ステップ 3	end	

ステップ 4	または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-ancp)# end`
	または
	`RP/0/RSP0/CPU0:router(config-ancp)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。

	コマンドまたはアクション	目的
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

ANCP ネイバーの設定

ネイバーからの TCP 接続はどのインターフェイスでも許可されます。 各 TCP 接続にネイバー設定を一致させるため、ANCP ネイバーは隣接プロトコル メッセージの対応するフィールドと一致する必要のある送信元名によって識別されます。 必要に応じて、システム上の ANCP ネイバーと設定された隣接タイマー間隔を識別するために説明ストリングを使用できます。

手順の概要

1. configure
2. ancp neighbor sender-name {H.H.H | A.B.C.D}[**description** string]
3. ancp neighbor sender-name {*H.H.H* | *A.B.C.D*} [**adjacency-timer** *interval*]
4. **end** または **commit**
5. show ancp neighbor {**description** *description-string*| sender-name {*H.H.H* | *A.B.C.D*}} [statistics][detail] RP/0/RSP0/CPU0:router# show ancp neighbor sender-name 0006.2aaa.281b
6. show ancp neighbor summary [statistics][detail] RP/0/RSP0/CPU0:router# show ancp neighbor summary
7. clear ancp neighbor {all | **description** description-string | sender-name {H.H.H | A.B.C.D}}[state | statistics] RP/0/RSP0/CPU0:router# clear ancp neighbor all
8. clear ancp summary [statistics | detail] RP/0/RSP0/CPU0:router# clear ancp summary statistics
9. show ancp neighbor [all] [statistics] RP/0/RSP0/CPU0:router# show ancp neighbor statistics
10. show ancp neighbor state [none | synsent | synrcvd | estab} [statistics] RP/0/RSP0/CPU0:router# show ancp neighbor none

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	configure
	
	例：
	
	`RP/0/RSP0/CPU0:router# configure`
	`RP/0/RSP0/CPU0:router(config)#`
		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 2	ancp neighbor sender-name {H.H.H | A.B.C.D}[**description** string] 例： `RP/0/RSP0/CPU0:router(config)# ancp neighbor sender-name oo13.1aff.c2bd description vendorA1`	簡単に DSLAM を識別するためにネイバーの description パラメータを設定します。
ステップ 3	ancp neighbor sender-name {*H.H.H* | *A.B.C.D*} [**adjacency-timer** *interval*] 例： `RP/0/RSP0/CPU0:router(config)# ancp neighbor sender-name 0013.1aff.c2bd adjacency-timer 20`	ネイバーの adjacency timer パラメータを設定します。 ネイバー セッションがすでに確立されている場合は、このタイマーが有効になるようにリセットされます。 （注） • 設定されているポートはダウン ステートに置かれ、未設定のポートは解放されます。

ステップ 4	**end** または **commit**
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-ancp)# end`
	または
	
	`RP/0/RSP0/CPU0:router(config-ancp)# commit`
		設定変更を保存します。
		
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		
		Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:
		
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	show ancp neighbor {**description** *description-string*| sender-name {*H.H.H* | *A.B.C.D*}} [statistics][detail] RP/0/RSP0/CPU0:router# show ancp neighbor sender-name 0006.2aaa.281b	（任意）個々の ANCP 隣接または隣接のセットに関連付けられたデータまたはメッセージの統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	show ancp neighbor summary [statistics][detail] RP/0/RSP0/CPU0:router# show ancp neighbor summary	（任意）ステート別に隣接関係の数を表示します。
ステップ 7	clear ancp neighbor {all | **description** description-string | sender-name {H.H.H | A.B.C.D}}[state | statistics] RP/0/RSP0/CPU0:router# clear ancp neighbor all	（任意）ANCP ネイバーをすべてまたは個別に消去します。 設定されているポートをダウン ステートにして、未設定のポートを開放します。 ステートが選択されている場合、隣接は TCP ソケットを消去せずにリセットされます。
ステップ 8	clear ancp summary [statistics | detail] RP/0/RSP0/CPU0:router# clear ancp summary statistics	（任意）集約メッセージの統計情報だけをクリアします。個別のネイバーまたはポートの統計情報は変更しません。
ステップ 9	show ancp neighbor [all] [statistics] RP/0/RSP0/CPU0:router# show ancp neighbor statistics	（任意）ANCP ネイバー情報を表示します。
ステップ 10	show ancp neighbor state [none | synsent | synrcvd | estab} [statistics] RP/0/RSP0/CPU0:router# show ancp neighbor none	（任意）隣接プロトコル ステート情報を表示します。

VLAN サブインターフェイスへの AN ポートのマッピング

ポート マッピングは、VLAN サブインターフェイスと DSLAM アクセス ポートまたは DSLAM の顧客宅内機器（CPE）クライアントを関連付けます。 VLAN は IEEE 802.1Q または QinQ 階層 VLAN にすることができます。 AN ポートを VLAN サブインターフェイスにマッピングするには、グローバル コンフィギュレーション モードで **ancp an-port** コマンドを使用します。

手順の概要

1. configure
2. ancp an-port circuit-id *Access-Loop-Circuit*-ID [**interface** type interface-path-id | **interface Bundle-Ether** *bundle-id*] RP/0/RSP0/CPU0:router(config)# ancp an-port circuit-id circuit1 interface gigabitethernet 2/0/1/1.1
3. **end** または **commit**
4. show ancp an-port {circuit-id *Access-Loop-Circuit-ID* | **interface** type interface-path-id | **interface Bundle-Ether** *bundle-id* | **mapping} [statistics** | detail]
5. show ancp an-port [configured | dynamic-only][statistics]
6. show ancp an-port summary [statistics][detail]
7. clear ancp an-port {all | circuit-id Access-Loop-Circuit-Id | **interface** type interface-path-id | **interface Bundle-Ether** *bundle-id* | neighbor {description string | sender-name {H.H.H | A.B.C.D}}[statistics]
8. **show ancp an-port** {**description** description-string | **sender-name** {*H.H.H* | *A.B.C.D*}}
9. **show ancp an-port state** [**up** | **down** | **none**] [**statistics**]

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	configure
	
	例：
	
	`RP/0/RSP0/CPU0:router# configure`
	`RP/0/RSP0/CPU0:router(config)#`
		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 2	ancp an-port circuit-id *Access-Loop-Circuit*-ID [**interface** type interface-path-id | **interface Bundle-Ether** *bundle-id*] RP/0/RSP0/CPU0:router(config)# ancp an-port circuit-id circuit1 interface gigabitethernet 2/0/1/1.1	一意のアクセス ノード ID を定義します。 この ID 情報は、ANCP Port Up および Port Down メッセージに含まれます。 アクセス ノード ポートの設定をコミットする前に、回線 ID を指定する必要があります。 共有ポリシー インスタンスを ANCP とのサブインターフェイスで使用する場合は、同じ共有ポリシー インスタンスを持つすべてのサブインターフェイスに AN ポート回線 ID をマッピングする必要があります。

ステップ 3	**end** または **commit**
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-ancp)# end`
	または
	
	`RP/0/RSP0/CPU0:router(config-ancp)# commit`
		設定変更を保存します。
		
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		
		Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:
		
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッ

	コマンドまたはアクション	目的
		ションが終了して、ルータが EXEC モードに戻ります。 **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、ルータは現在のコンフィギュレーションセッションで継続されます。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。
ステップ 4	show ancp an-port {circuit-id *Access-Loop-Circuit-ID* | **interface** type interface-path-id | **interface Bundle-Ether** *bundle-id* | **mapping} [statistics** | detail] 例： `RP/0/RSP0/CPU0:router# show ancp an-port gigabitethernet 2/0/1/1.1`	（任意）DSLAM のアクセス ポート（または DSLAM の CPE クライアント）と VLAN サブインターフェイスのアソシエーションに関する情報を表示します。
ステップ 5	show ancp an-port [configured | dynamic-only][statistics] 例： `RP/0/RSP0/CPU0:router# show ancp an-port configured`	（任意）インターフェイスにマッピングされている、またはされていない AN ポートのサマリーデータまたは統計情報を表示します。
ステップ 6	show ancp an-port summary [statistics][detail] 例： `RP/0/RSP0/CPU0:router# show ancp an-port summary`	（任意）ステート別にポートの数を表示します。
ステップ 7	clear ancp an-port {all | circuit-id Access-Loop-Circuit-Id | **interface** type interface-path-id | **interface Bundle-Ether** *bundle-id* | neighbor {description string | sender-name {H.H.H | A.B.C.D}}[statistics] 例： `RP/0/RSP0/CPU0:router# clear ancp an-port all`	（任意）個別に、またはグループで、動的データまたは統計情報の AN ポートをクリアします。パブリッシュされた情報がクリアされ、DSLAM から学習した情報がクリアされます。

	コマンドまたはアクション	目的
ステップ 8	**show ancp an-port** {**description** description-string | **sender-name** {*H.H.H* | *A.B.C.D*}} 例： `RP/0/RSP0/CPU0:router# show ancp an-port description vendor3b`	（任意）AN ポート情報を表示します。
ステップ 9	**show ancp an-port state** [**up** | **down** | **none**] [**statistics**] 例： `RP/0/RSP0/CPU0:router# show ancp an-port state up`	（任意）AN ポート ステート情報を表示します。

ANCP 比率調整の設定

シェーパー レートとして適用する前に ANCP 比率の更新に数学的な補正を適用するには、**ancp rate-adjustment** コマンドを使用します。

手順の概要

1. configure RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)#
2. ancp rate-adjustment dsl-type access-loop-type percent-factor factor
3. **end** または **commit**
4. show ancp summary detail RP/0/RSP0/CPU0:router# show ancp summary detail

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)#	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 2	ancp rate-adjustment dsl-type access-loop-type percent-factor factor 例： `RP/0/RSP0/CPU0:router(config)# ancp rate-adjustment adsl2 ethernet percent-factor 90`	ANCP のシェーパー パーセント係数のパラメータを設定します。*dsl-type* および *access-loop-type* は、ANCP Port Up メッセージのオプションの Type-Length Value（TLV）の適切な値と比較され、一致する場合、ANCP の比率は設定されている係数によって調整されます。 • dsl-type：（必須）DSL タイプ コードを設定します。 **adsl1 adsl2 adsl2+ vdsl1 vdsl2 sdsl**

	コマンドまたはアクション	目的
		• *access-loop-type*：（必須）*access-loop-type* を **ATM** または **Ethernet** に設定します。 • **percent-factor** factor：（必須）シェーピング レートとして設定する前に ANCP で報告される比率の更新に適用されるパーセント値。

ステップ 3	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 4	show ancp summary detail RP/0/RSP0/CPU0:router# show ancp summary detail	（任意）比率調整設定情報とともに汎用 ANCP 設定情報を示します。

ANCP の設定例では次の例を紹介します。

- ANCP サーバ送信元名の設定：例
- ANCP ネイバーの設定：例
- VLAN サブインターフェイスへの AN ポートのマッピング：例
- ANCP 比率調整の設定：例
- ANCP および QoS の相互作用：例

• インターフェイス上の QoS ポリシーの不一致：例

ANCP サーバ送信元名の設定：例

ANCP ネイバーの設定：例

次に、ANCP ネイバーのパラメータを設定する例を示します。

```
configure
ancp neighbor sender-name 0001.2222.3333 description VendorA-1
ancp neighbor sender-name 0001.2222.3333 adjacency-timer 20

commit
```

次に、**sender-name** MAC アドレスを使用する特定のネイバーからの出力例を示します。

```
show ancp neighbor sender-name 0006.2aaa.281b

            ANCP Neighbor Data
  ------------------------------------------
  Sender Name               0006.2aaa.281b
  Description               first
  State                     ESTAB
  Capability                Topology Discovery
  Ports:
    State Up                25
    State Down              5
    Total                   30
```

次に、同じコマンドに **detail** キーワードを追加して、ネイバーからレポートされた AN ポートのサマリーを表示する例を示します。

```
show ancp neighbor sender-name 0006.2aaa.281b detail

             ANCP Neighbor Data
  ------------------------------------------
  Sender Name               0006.2aaa.281b
  Description               first
  State                     ESTAB
  Capability                Topology Discovery
  Ports:
    State Up                4
    State Down              0
    Total                   4
Remote IP Addr/TCP Port   209.165.200.225/11126
Local  IP Addr/TCP Port   209.165.200.250/6068
Server Sender Name        0013.1aff.c2bd
Remote Timeout            25500 msec
Local  Timeout            10000 msec
Adjacency Uptime          01:25:20
Time Since Last Port Msg  00:00:04
Remote Port               0
Remote Instance           1
Local Instance            1
Remote Partition ID       0

List of AN port data for neighbor sender name 0006.2aaa.281b
------------------------------ ----- ---------- -------- ----  ------------
                                                  Line     Num   Adjusted DS
Circuit-id                     State Uptime     State    Intf  Rate (kbps)
------------------------------ ----- ---------- -------- ----  ------------
circuit1                       UP    00:27:49   SHOWTIME   3    2250
circuit2                       UP    00:00:49   SHOWTIME   2    2250
```

```
circuit3                        UP    00:00:49  SHOWTIME   2    2250
circuit4                        UP    00:00:49  SHOWTIME   0    2250
```

次に、同じコマンドに **statistics** キーワードを追加して、選択されたネイバーのメッセージ統計情報のサマリーを表示する例を示します。

```
show ancp neighbor sender-name 0006.2aaa.281b statistics

ANCP Neighbor Message Statistics
for Sender-name -, Description 0006.2aaa.281b
-----------------------------------------------
               Sent         Received
SYN            1            2
SNYACK         1            0
ACK            589          238
RSTACK         0            0
Port Up        -            10
Port Down      -            0
Drops          0            0
Total          600          250
```

次に、ANCP 設定に関する基本情報に加えてステート別のネイバー数とポート数を表示する例を示します。

```
show ancp summary

  ANCP Summary Information
 ------------------------------------------------
 Capability:                 Topology Discovery
 Server sender-name:         0013:1aff.c2bd

 Neighbor count by state:
   -                          0
   SYNSENT                    0
   SUNRCVD                    0
   ESTAB                      1
   ---------------------------------
   Total                      1

Port count by state:
  State Up                   1
  State Down                 0
  State Unknown              0
  ---------------------------------
  Total                      1

  No. configured ports       1
  No. mapped sub-interfaces  4
```

次に、前の例で表示した基本情報に加えて比率調整設定情報を表示する例を示します。

```
show ancp summary detail

    ANCP Summary Information
   ------------------------------------------------
   Capability:                 Topology Discovery
   Server sender-name:         0013:1aff.c2bd

Neighbor count by state:
  -                          0
  SYNSENT                    0
  SUNRCVD                    0
  ESTAB                      1
  ---------------------------------
  Total                      1
Port count by state:
  State Up                   1
  State Down                 0
  State Unknown              0
  ---------------------------------
  Total                      1
```

```
  No. configured ports         1
  No. mapped sub-interfaces    4

Rate adjustment configuration:
-----------------------------------------
DSL Type   Loop Type        Percent-Factor
-----------------------------------------
ADSL1      ETHERNET                90
ADSL2      ETHERNET                100
ADSL2PLUS  ETHERNET                100
VDSL1      ETHERNET                100
VDSL2      ETHERNET                100
SDSL       ETHERNET                100
ADSL1      ATM                     100
ADSL2      ATM                     100
ADSL2PLUS  ATM                     100
VDSL1      ATM                     100
VDSL2      ATM                     100
SDSL       ATM                     100
```

次に、ANCP メッセージ統計情報のサマリーを表示する例を示します。

```
show ancp summary statistics
```

```
    ANCP Summary Message Statistics
   -------------------------------------
                Sent          Received
   SYN          3             6
   SYNACK       4             0
   ACK          7105          2819
   RSTACK       2             0
   Port Up      -             6
   Port Down    -             0
   Drops        0             0
   Total        7114          2831
```

次に、すべてのネイバー データと統計情報をクリアする方法の例を示します。

```
clear ancp neighbor all
```

次に、特定のネイバーをクリアする方法の例を示します。

```
clear ancp neighbor description vendor1a
```

次に、集約メッセージ統計情報をクリアする方法の例を示します。

```
clear ancp summary statistics
```

VLAN サブインターフェイスへの AN ポートのマッピング：例

次に、一意のアクセス ノード ID を定義する例を示します。

```
configure
ancp an-port circuit-id  circuit1 interface gigabitethernet 2/0/1/1.1
```

次に、サブインターフェイスで識別されるポートの情報を表示する例を示します。

```
show ancp an-port interface gigabitethernet 0/0/0/37.1
```

```
  AN port circuit-id ccc1:

  State                                                  UP
  UPtime                                                 02:23:45
  Time Since Last Message                                00:00:00
  Encap Type                                             ETHERNET
  DSL type                                               ADSL1
```

```
  DSL Line State                                          SHOWTIME
  Number of Mapped Interfaces                             3
  Neighbor sender-name                                    0006.2aaa.281b
  Neighbor description                                     7200-client
  Configured Rate Adjustment                              90%
  Actual Downstream Data Rate (kbps)                      2500
  Effective Downstream Data Rate (kbps)                   2250
```

次に、**detail** キーワードを使用して、ポート情報とポートにマッピングされたインターフェイスのリストを表示する例を示します。

```
show ancp an-port circuit-id ccc1 detail

  AN port circuit-id ccc1:

  State                                                   UP
  UPtime                                                  02:31:36
  Time Since Last Message                                 00:00:00
  Encap Type                                              ETHERNET
  DSL type                                                ADSL1
  DSL Line State                                          SHOWTIME
  Number of Mapped Interfaces                             3
  Neighbor sender-name                                    0006.2aaa.281b
  Neighbor description                                     7200-client
  Configured Rate Adjustment                              90%
  Actual Downstream Data Rate (kbps)                      2500
  Effective Downstream Data Rate (kbps)                   2250
  Actual Data Rate Upstream/Downstream (kbps)             2500/2500
  Minimum Data Rate Upstream/Downstream (kbps)            0/0
  Attainable Data Rate Upstream/Downstream (kbps)         0/0
  Maximum Data Rate Upstream/Downstream (kbps)            0/0
  Minimum Low Power Data Rate Upstream/Downstream (kbps)  0/0
  Maximum Interleaving delay Upstream/Downstream (ms)     0/0
  Actual Interleaving Delay Upstream/Downstream (ms)      0/0

  Sub-interface Summary: total 3
  ---------------------------------------------
  Sub-interface Name                  ifhandle
  ---------------------------------   ----------
  GigabitEthernet0/0/0/37.1           0x0
  GigabitEthernet0/0/0/37.11          0x0
  GigabitEthernet0/0/0/38.10          0xb80
```

次に、特定の AN ポートのポート メッセージの統計情報を表示するために、**statistics** キーワードを使用する例を示します。

```
show ancp an-port circuit-id ccc1 statistics

  Port message statistics for circuit-id ccc1:

    Port Up       5
    Port Down     0
```

次に、ステート別にポートの数を表示する例を示します。

```
show ancp an-port summary

     AN Port Count Summary
  ------------------------------
  State UP                 4
  State DOWN               0
  Config only ports        0
  Total                    4
  # Configured ports       1
  # Mapped sub-interfaces  4
```

次に、すべての AN ポートのメッセージの統計情報をクリアする例を示します。

```
clear ancp an-port all statistics
```

次に、すべての AN ポートの動的データをクリアする例を示します。

```
clear ancp an-port all
```

次に、特定のインターフェイスの動的データをクリアする方法を示します。

```
clear ancp an-port interface gigabitethernet 0/1/0/10.5
```

ANCP 比率調整の設定：例

ANCP および QoS の相互作用：例

次に、ANCP 値を適用した場合と適用しない場合の階層型 QoS ポリシーの設定例を示します。

```
policy-map child-3play
 class 3play-voip
  priority level 1
  police rate 65 kbps
  !
 !
 class 3play-video
  priority level 2
  police rate 128 kbps
  !
  random-detect cos 3 10 ms 100 ms
  random-detect cos 4 20 ms 200 ms
 !
 class 3play-premium
  bandwidth percent 100
 !
 class class-default
 !
 end-policy-map
!
policy-map parent-3play-subscriber-line
 class class-default
  service-policy child-3play
  shape average 1 mbps
 !
 end policy-map
!
```

ポリシーは、ANCP なしでインターフェイスで適用されます。

```
interface GigabitEthernet 0/1/0/0.1 l2transport
encapsulation dot1q 2
 service-policy output parent-3play-subscriber-line
!
```

show qos コマンドは、ANCP が適用されていないことを確認します（ANCP は 0 Kbps として示されます）。

```
RP/0/RSP0/CPU0:router# show qos interface GigabitEthernet 0/1/0/0.1 out

Interface: GigabitEthernet0_1_0_0.1 output Bandwidth: 1000000 kbps
ANCP: 0 kbps
Policy: parent-3-play-subscriber-line Total number of classes: 5
------------------------------------------------------------------------------
Level: 0 Policy: parent-3-play-subscriber-line Class: class-default
QueueID: N/A
Shape Profile: 1 CIR: 960 kbps CBS: 1024 bytes PIR: 960 kbps PBS: 13312 bytes
WFQ Profile: 1 Committed Weight: 1 Excess Weight: 1
Bandwidth: 0 kbps, BW sum for Level 0: 1000000 kbps, Excess Ratio: 1
```

```
------------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-voip
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 8 (Priority 1)
Queue Limit: 16 kbytes Profile: 3 Scale Profile: 0
Policer Profile: 0 (Single)
Conform: 65 kbps (65 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
------------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-video
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 9 (Priority 2)
Queue Limit: 8 kbytes (11 Unknown) Profile: 4 Scale Profile: 0
Policer Profile: 24 (Single)
Conform: 128 kbps (128 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
WRED Type: COS based Table: 0 Profile: 4 Scale Profile: 0 Curves: 3
Default RED Curve Thresholds Min : 8 kbytes Max: 8 kbytes
WRED Curve: 1 Thresholds Min : 8 kbytes Max: 8kbytes
 Match: 3
WRED Curve: 2 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 4
------------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3-play-premium
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 10 (Priority Normal)
Queue Limit: 16 kbytes Profile: 1 Scale Profile: 1
WFQ Profile: 4 Committed Weight: 100 Excess Weight: 100
Bandwidth: 1000 kbps, BW sum for Level 1: 1000 kbps, Excess Ratio: 1
------------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: class-default
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 11 (Priority Normal)
Queue Limit: 8 kbytes Profile: 1 Scale Profile: 0
WFQ Profile: 5 Committed Weight: 1 Excess Weight: 1
Bandwidth: 0 kbps, BW sum for Level 1: 1000 kbps, Excess Ratio: 1
------------------------------------------------------------------------------
RP/0/RSP0/CPU0:router#
```

ANCP AN-Port-to-Interface マッピングが適用されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ancp an-port circuit-id dslam1_port1 interface GigabitEthernet
 0/1/0/0.1
```

show ancp an-port interface コマンドはインターフェイスの ANCP 比率を示します。

```
RP/0/RSP0/CPU0:router# show ancp an-port interface GigabitEthernet 0/1/0/0.1 detail

   AN port circuit-id dlsam1_port1:

   State                                                UP
   Uptime                                               00:00:32
   Time Since Last Message                              00:00:32
   Encap Type                                           ATM
   DSL Type                                             ADSL1
   DSL Line State                                       SHOWTIME
   Number of Mapped Sub-interfaces                      1
   Neighbor sender-name                                 0000.0000.1bec
   Neighbor description                                 -
   Configured Rate Adjustment                           100%
   Actual Downstream Data Rate (kbps)                   2000
   Effective Downstream Data Rate (kbps)                2000
   Actual Data Rate Upstream/Downstream (kbps)          2000/2000
   Minimum Data Rate Upstream/Downstream (kbps)         0/0
   Attainable Data Rate Upstream/Downstream (kbps)      0/0
   Maximum Data Rate Upstream/Downstream (kbps)         0/0
   Minimum Low Power Data Rate Upstream/Downstream (kbps) 0/0
```

```
   Maximum Interleaving Delay Upstream/Downstream (ms)     0/0
   Actual Interleaving Delay Upstream/Downstream (ms)      0/0

Sub-interface Summary: total 1
-----------------------------------------------------
Sub-interface name                    ifhandle
----------------------------------    ----------
GigabitEthernet0/1/0.1                0x215e042
```

show qos コマンドは、ANCP が適用されていることを確認します（ここでは ANCP は 1920 kbps として示しされます）。

```
RP/0/RSP0/CPU0/router# show qos interface GigabitEthernet 0/1/0.1 out

Interface GigabitEthernet0_1_0_0.1 output Bandwidth: 1000000 kbps
ANCP: 1920 kbps
Policy: parent-3play-subscriber-line Total number of classes: 5
------------------------------------------------------------------------
Level: 0 Policy: parent-3-play-subscriber-line Class: class-default
QueueID: N/A
Shape Profile: 1 CIR: 1920 kbps CBS: 1024 bytes PIR: 1920 kbps PBS: 13312 bytes
WFQ Profile: 1 Committed Weight: 1 Excess Weight: 1
Bandwidth: 0 kbps, BW sum for Level 0: 1000000 kbps, Excess Ratio: 1
------------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-voip
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 8 (Priority 1)
Queue Limit: 16 kbytes Profile: 3 Scale Profile: 0
Policer Profile: 0 (Single)
Conform: 65 kbps (65 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
------------------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-video
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 9 (Priority 2)
Queue Limit: 8 kbytes (11 Unknown) Profile: 4 Scale Profile: 0
Policer Profile: 24 (Single)
Conform: 128 kbps (128 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
WRED Type: COS based Table: 0 Profile: 4 Scale Profile: 0 Curves: 3
Default RED Curve Thresholds Min : 8 kbytes Max: 8 kbytes
WRED Curve: 1 Thresholds Min : 8 kbytes Max: 8kbytes
 Match: 3
WRED Curve: 2 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 4
------------------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3-play-premium
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 10 (Priority Normal)
Queue Limit: 24 kbytes Profile: 1 Scale Profile: 8
WFQ Profile: 4 Committed Weight: 100 Excess Weight: 100
Bandwidth: 1920 kbps, BW sum for Level 1: 1920 kbps, Excess Ratio: 1
------------------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: class-default
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 11 (Priority Normal)
Queue Limit: 8 kbytes Profile: 1 Scale Profile: 0
WFQ Profile: 5 Committed Weight: 1 Excess Weight: 1
Bandwidth: 0 kbps, BW sum for Level 1: 1920 kbps, Excess Ratio: 1
------------------------------------------------------------------------------------
```

インターフェイス上の QoS ポリシーの不一致：例

絶対値またはパーセント値が設定された有効な QoS ポリシーは次の要件を満たす必要があります。

インターフェイス速度 > ANCP 比率 > QoS 親シェーパー レート

正常にインターフェイスに適用されている QoS ポリシーは 2 種類の外部要因により無効になることがあります。 これらの 2 つの要因は、ANCP 比率変更またはポート速度の変更です。

- ANCP 比率変更：ANCP 比率が低下すると、つまり ANCP 比率調整係数により ANCP 比率が最上位の QoS ポリシー マップのシェーパー レートを下回ると、インターフェイス上の QoS ポリシーは無効になります。
- ポート速度の変更：ギガビット イーサネット インターフェイス ポートはデフォルトの 1000 Mbps から 10 Mbps または 100 Mbps モードに設定できます。 この場合、インターフェイス速度は ANCP 比率および QoS 親シェーパー レート未満に低下します。 インターフェイス上の QoS ポリシーが無効になります。

これらの変更のいずれかが発生すると、インターフェイス上の QoS ポリシーは不一致ステートに置かれます。 不一致ステートから回復するには、次のいずれかの作業を行います。

- QoS ポリシーをインターフェイスから削除して、QoS ポリシー値を調整し、インターフェイスに QoS ポリシーを再適用します。
- ANCP の調整レートまたは ANCP 比率が変更された場合、QoS ポリシー レート要件を満たすように ANCP 比率を更新します。
- ポート速度が変更された場合、QoS ポリシー レート要件を満たすように速度を更新します。

次に、ANCP 比率変更およびポート速度の変更のギガビット イーサネット インターフェイス上の次の QoS ポリシーの設定への影響の例を示します。

```
policy-map child-3play
 class 3play-voip
  priority level 1
  police rate 65 kbps
  !
 !
 class 3play-video
  priority level 2
  police rate 128 kbps
  !
   random-detect cos 3 10 ms 100 ms
   random-detect cos 4 20 ms 200 ms
 !
 class 3play-premium
  bandwidth percent 100
 !
 Class class-default
 !
 end-policy-map
!
policy-map parent-3play-subscriber-line
 class class-default
  service-policy child-3play
  bandwidth 200 mbps
  bandwidth remaining percent 100
```

```
  shape average 800 mbps
 !
 end-policy-map
!
```

ANCP レート値が 999936 kbps で、ANCP 比率係数が 100 % の場合、999936 という ANCP レート値がインターフェイスに適用されます。 これは要件を満たします。

インターフェイスの速度（1000000 kbps）> ANCP レート（999936 kbps）> QoS 親シェーパー レート（800000 kbps）

次の **show qos interface** コマンドの出力で示されているように、これはポリシーが正しく適用されています。

```
show qos interface gig0/0/0/11.1 output

Wed Mar 18 18:25:20.140 UTC
Interface: GigabitEthernet0_0_0_11.1 output Bandwidth: 1000000 kbps ANCP: 999936 kbps
Policy: parent-3play-subscriber-line Total number of classes: 5
------------------------------------------------------------------------
Level: 0 Policy: parent-3play-subscriber-line Class: class-default
QueueID: N/A
Shape Profile: 1 CIR: 200000 kbps (200 mbps)
CBS: 100352 bytes PIR: 999936 kbps PBS: 12517376 bytes
WFQ Profile: 1 Committed Weight: 51 Excess Weight: 100
Bandwidth: 200000 kbps, BW sum for Level 0: 1000000 kbps, Excess Ratio: 100
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-voip
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 136 (Priority 1)
Queue Limit: 16 kbytes Profile: 3 Scale Profile: 0
Policer Profile: 0 (Single)
Conform: 65 kbps (65 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-video
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 137 (Priority 2)
Queue Limit: 8 kbytes (11 Unknown) Profile: 4 Scale Profile: 0
Policer Profile: 24 (Single)
Conform: 128 kbps (128 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
WRED Type: COS based Table: 0 Profile: 4 Scale Profile: 0 Curves: 3
Default RED Curve Thresholds Min : 8 kbytes Max: 8 kbytes
WRED Curve: 1 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 3
WRED Curve: 2 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 4
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-premium
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 138 (Priority Normal)
Queue Limit: 2097 kbytes Profile: 2 Scale Profile: 0
WFQ Profile: 6 Committed Weight: 1020 Excess Weight: 1020
Bandwidth: 200000 kbps, BW sum for Level 1: 200000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: class-default
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 139 (Priority Normal)
Queue Limit: 65 kbytes Profile: 1 Scale Profile: 3
WFQ Profile: 0 Committed Weight: 1 Excess Weight: 1020
Bandwidth: 0 kbps, BW sum for Level 1: 200000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
```

ANCP 比率変更

ANCP 比率が QoS 親シェーパー レートより低下し（たとえば、300000 Kbps）、ANCP 比率調整係数が 100 % のままの場合、ANCP 比率は 800000 kbps の QoS 親シェーパー レートを超えません。次の **show qos interface** コマンドの出力で示されているように、これによってインターフェイス上の QoS ポリシーが不一致ステートに置かれます。

```
show qos interface gig0/0/0/11.1 output

Wed Mar 18 18:21:11.180 UTC
Interface: GigabitEthernet0_0_0_11.1 output Bandwidth: 1000000 kbps ANCP: 299904 kbps
 *Inconsistency* :  ANCP - Downstream Rate less than Shaper Rate
Policy: parent-3play-subscriber-line Total number of classes: 5
------------------------------------------------------------------------
Level: 0 Policy: parent-3play-subscriber-line Class: class-default
QueueID: N/A
Shape Profile: 2 CIR: 200000 kbps (200 mbps)
CBS: 100352 bytes PIR: 800000 kbps PBS: 10027008 bytes
WFQ Profile: 1 Committed Weight: 51 Excess Weight: 100
Bandwidth: 200000 kbps, BW sum for Level 0: 1000000 kbps, Excess Ratio: 100
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-voip
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 136 (Priority 1)
Queue Limit: 16 kbytes Profile: 3 Scale Profile: 0
Policer Profile: 0 (Single)
Conform: 65 kbps (65 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-video
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 137 (Priority 2)
Queue Limit: 8 kbytes (11 Unknown) Profile: 4 Scale Profile: 0
Policer Profile: 24 (Single)
Conform: 128 kbps (128 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
WRED Type: COS based Table: 0 Profile: 4 Scale Profile: 0 Curves: 3
Default RED Curve Thresholds Min : 8 kbytes Max: 8 kbytes
WRED Curve: 1 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 3
WRED Curve: 2 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 4
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-premium
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 138 (Priority Normal)
Queue Limit: 2097 kbytes Profile: 2 Scale Profile: 0
WFQ Profile: 6 Committed Weight: 1020 Excess Weight: 1020
Bandwidth: 200000 kbps, BW sum for Level 1: 200000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: class-default
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 139 (Priority Normal)
Queue Limit: 65 kbytes Profile: 1 Scale Profile: 3
WFQ Profile: 0 Committed Weight: 1 Excess Weight: 1020
Bandwidth: 0 kbps, BW sum for Level 1: 200000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
```

ANCP 比率が設定値に戻ると、不一致は自動的にクリアされます。これは **show qos interface** コマンドを実行して確認できます。

（注） ANCP 比率がシェーピング レート未満の値に設定されている場合、不一致は自動的に消去されず、ポリシーを変更し、再度適用する必要があります。 これを防止するには、特定のサービス レベルのすべての ANCP 比率の最小値にポリシー マップ シェーピング レートを設定してください。

ポート速度の変更

ポート速度が QoS 親シェーパー レート未満に設定されている場合（たとえば、100 Mbps（100000 kbps））、要件は、ポート速度が 800000 kbps の QoS 親シェーパー レートより大きくないため、満たされません。

```
RP/0/RSP0/CPU0:ro-node1#conf
RP/0/RSP0/CPU0:ro-node1(config)#int gigabitEthernet 0/0/0/1
RP/0/RSP0/CPU0:ro-node1(config-if)#speed 100
RP/0/RSP0/CPU0:ro-node1(config-if)#commit
LC/0/0/CPU0:Nov  4 05:36:55.041 : qos_ma_ea[197]: %QOS-QOS_EA_MODIFY_FAIL-3-ERROR :
inconsistency detected due to ANCP or Bandwidth modification. Execute show qos inconsistency,
 to obtain information. Policy resolution failure
RP/0/RSP0/CPU0:ro-node1(config-if)#end
```

次の **show qos interface** コマンドの出力で示されているように、これによってインターフェイス上の QoS ポリシーが不一致ステートに置かれます。

```
RP/0/RSP0/CPU0:ro-node1#sh qos int gigabitEthernet 0/0/0/1.1 output
Interface: GigabitEthernet0_0_0_1.1 output Bandwidth: 1000000 kbps ANCP: 0 kbps
 *Inconsistency* :  Port speed modify fails on Policy
Policy: parent-3play-subscriber-line Total number of classes: 5
------------------------------------------------------------------------------
Level: 0 Policy: parent-3play-subscriber-line Class: class-default
QueueID: N/A
Shape Profile: 1 CIR: 200000 kbps (200 mbps)
CBS: 100352 bytes PIR: 800000 kbps PBS: 10027008 bytes
WFQ Profile: 1 Committed Weight: 51 Excess Weight: 100
Bandwidth: 200000 kbps, BW sum for Level 0: 1000000 kbps, Excess Ratio: 100
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-voip
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 640 (Priority 1)
Queue Limit: 16 kbytes Profile: 3 Scale Profile: 0
Policer Profile: 0 (Single)
Conform: 65 kbps (65 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: 3play-video
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 641 (Priority 2)
Queue Limit: 8 kbytes Profile: 4 Scale Profile: 0
Policer Profile: 24 (Single)
Conform: 128 kbps (128 kbps) Burst: 1598 bytes (0 Default)
Child Policer Conform: TX
Child Policer Exceed: DROP
Child Policer Violate: DROP
WRED Type: COS based Table: 2 Profile: 4 Scale Profile: 0 Curves: 3
Default RED Curve Thresholds Min : 8 kbytes Max: 8 kbytes
WRED Curve: 1 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 3
WRED Curve: 2 Thresholds Min : 8 kbytes Max: 8 kbytes
 Match: 4
------------------------------------------------------------------------
```

```
Level: 1 Policy: child-3play Class: 3play-premium
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 642 (Priority Normal)
Queue Limit: 4194 kbytes Profile: 2 Scale Profile: 1
WFQ Profile: 3 Committed Weight: 1020 Excess Weight: 1020
Bandwidth: 200000 kbps, BW sum for Level 1: 200000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
Level: 1 Policy: child-3play Class: class-default
Parent Policy: parent-3play-subscriber-line Class: class-default
QueueID: 643 (Priority Normal)
Queue Limit: 4194 kbytes Profile: 2 Scale Profile: 1
WFQ Profile: 4 Committed Weight: 1 Excess Weight: 1
Bandwidth: 0 kbps, BW sum for Level 1: 200000 kbps, Excess Ratio: 1
------------------------------------------------------------------------
```

この問題を解決するには、**no speed** コマンドを使用してポート速度を 1000 Mbps（1000000 kbps）に戻す必要があります。

```
RP/0/RSP0/CPU0:ro-node1#conf
RP/0/RSP0/CPU0:ro-node1(config)#int gigabitEthernet 0/0/0/1
RP/0/RSP0/CPU0:ro-node1(config-if)#no speed
RP/0/RSP0/CPU0:ro-node1(config-if)#commit
LC/0/0/CPU0:Nov  4 05:37:39.171 : ifmgr[144]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
 on Interface GigabitEthernet0/0/0/1, changed state to Up
```

不一致の消去は、再度 **show qos interface** コマンドを発行することによって確認できます。

show qos inconsistency コマンド：例

show qos interface コマンドに関連するコマンドは、QoS ポリシー不一致に関する追加情報を示します。

```
RP/0/RSP0/CPU0:RO2#show qos inconsistency detail 0 location 0/7/CPU0

Interface Lists with QoS Inconsistency Warning:
========================================================

                     Node 0/7/CPU0
--------------------------------------------------------

Interfaces with QoS Inconsistency:  ANCP - No Shaper at top policymap
=============================================================================
Interface                   Direction  Policy Name             SPI Name
-----------------------------------------------------------------------------
GigabitEthernet0/7/0/1.5     output    parent-none

Interfaces with QoS Inconsistency:  ANCP - Downstream Rate less than Shaper Rate
=============================================================================
Interface                   Direction  Policy Name             SPI Name
-----------------------------------------------------------------------------
GigabitEthernet0/7/0/1       output    parent                   SPI1
GigabitEthernet0/7/0/1.2     output    parent
GigabitEthernet0/7/0/1       output    normal-policy-name      normal-spi-name

RP/0/RSP0/CPU0:RO2#
RP/0/RSP0/CPU0:RO2#show qos inconsistency summary location 0/7/CPU0

Summary Counts of QoS Inconsistency Warnings:
========================================================


                     Node 0/7/CPU0

   Inconsistency Warning Type                  Count
--------------------------------------------------------
ANCP - No Shaper at top policymap:               1
ANCP - Downstream Rate less than Shaper Rate:    4
RP/0/RSP0/CPU0:RO2#
```

その他の関連資料

ここでは、ANCP の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
初期システム起動と設定	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
マスター コマンド リファレンス	『*Cisco ASR 9000 Series Aggregation Services Router Master Command Listing*』
QoS コマンド	『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』
ユーザ グループとタスク ID	『Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide』の「Configuring AAA Services on Cisco ASR 9000 Series Router」モジュール

標準

標準	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
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

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
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

Access Node Control Protocol の設定

Access Node Control Protocol（ANCP）は、QoS 関連、サービス関連、加入者関連の操作を実行するために、サービス指向の集約デバイスとアクセス ノード（AN）間のコントロール プレーン（DSLAM など）を作成します。 ANCP サーバは ANCP 隣接（ANCP ネイバーとのセッション）、ANCP メッセージの送信と受信を受け入れ、維持します。 ANCP では、ANCP サーバが受信した、特定の加入者の DSL レート更新がその加入者に対応する QoS 設定に適用されるように ANCP ポー

トと VLAN サブインターフェイスの間でスタティック マッピングできます。 ANCP 経由で受信したDSL トレイン レートは、ルータの加入者側インターフェイスとサブインターフェイスのシェーピング レートを変更するために使用されます。 ANCP はルート プロセッサ（RP）の 1 つのプロセスとして動作します。

このモジュールでは、ANCP の実装に関する概念的および設定情報を提供します。

ラインカード、SIP および SPA のサポート

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
Access Node Control Protocol	yes	no

Cisco ASR 9000 シリーズ ルータ上でのアクセス ノード プロトコルの設定に関する機能の履歴

リリース	変更内容
リリース 3.7.2	Access Node Control Protocol 機能が導入されました。
リリース 3.9.0	イーサネット バンドル上の VLAN インターフェイスへの ANCP ポート マッピングが追加されました。
リリース 4.0.0	マルチシャーシ リンク集約上の ANCP が導入されました。

Access Node Control Protocol の設定

第 4 章

モジュラ QoS の輻輳回避の設定

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

輻輳の回避は、パケットのドロップにより行われます。 Cisco IOS XR ソフトウェアは、パケットをドロップする次の Quality of Service（QoS）の輻輳回避技術をサポートします。

- ランダム早期検出（RED
- 重み付けランダム早期検出（WRED）
- テール ドロップ

このモジュールでは、次の輻輳回避技術に関連する概念および作業について説明します。

ラインカード、SIP および SPA のサポート

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
ランダム早期検出	yes	yes
重み付けランダム早期検出	yes	yes
テール ドロップ	yes	yes

Cisco ASR 9000 シリーズ ルータのモジュラ QoS の輻輳回避の設定に関する機能履歴

リリース	変更内容

リリース 3.7.2	輻輳回避機能が ASR 9000 イーサネット ラインカードで導入されました。 ランダム早期検出、重み付けランダム早期検出、およびテール ドロップの各機能が ASR 9000 イーサネット ラインカードで導入されました。
リリース 3.9.0	ランダム早期検出、重み付けランダム早期検出、およびテール ドロップの各機能が ASR 9000 用 SIP 700 でサポートされました。

モジュラ QoS 輻輳回避の設定の前提条件

ネットワークでの QoS 輻輳回避を設定するには、次の前提条件を満たす必要があります。

適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

モジュラ QoS 輻輳回避の設定に関する情報

このマニュアルの QoS 輻輳回避技術を設定するには、次の概念を理解している必要があります。

ランダム早期検出と TCP

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

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

WRED のキュー制限

キュー制限は、各キューに使用可能なバッファ数を微調整するために使用されます。 これはキューイング クラスでのみ使用できます。 デフォルトのキュー制限は、指定されたキューのサービス レートの 100 ms です。 サービス レートは、最小保証帯域幅と特定のクラスに暗黙的または明示的に割り当てられた残存帯域幅の合計です。

キュー制限は、8 KB、16 KB、24 KB、32 KB、48 KB、64 KB、96 KB、128 KB、192 KB、256 KB、384 KB、512 KB、768 KB、1024 KB、1536 KB、2048 KB、3072 KB、4196 KB、8192 KB、16394 KB、32768 KB、65536 KB、131072 KB、262144 KB のいずれかの値に丸められます。

テール ドロップと FIFO キュー

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

Cisco ASR 9000 シリーズ ルータでのモジュラ QoS サービス パケットの分類およびマーキングの設定の「デフォルト トラフィック クラス」の項を参照してください。

ランダム早期検出の設定

この設定作業は WRED で行う場合と同様ですが、**random-detect precedence** コマンドは設定せずに、RED をイネーブルにするために、**default** キーワードを指定した **random-detect** コマンドを使用する必要があります。

制約事項

class-default を含む任意のクラスで **random-detect default** コマンドを設定する場合は、次のいずれかのコマンドを設定する必要があります。

- **shape average**
- **bandwidth**
- **bandwidth remaining**

手順の概要

1. **configure**
2. **policy-map** *policy-map-name*
3. **class** *class-name*
4. **random-detect** {**cos** *value* | **default** | **discard-class** *value* | **dscp** *value* | **exp** *value* | **precedence** *value* | *min-threshold* [*units*] *max-threshold* [*units*] }
5. **bandwidth** {*bandwidth* [*units*] | **percent** *value*} または **bandwidth remaining** [**percent** *value* | **ratio** *ratio-value*
6. **shape average** {**percent** *percentage* | *value* [*units*]}
7. **exit**
8. **exit**
9. **interface** *type interface-path-id*
10. **service-policy** {**input** | **output**} *policy-map*
11. 次のいずれかのコマンドを使用します。
    - **end**
    - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-map-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 4	**random-detect** {**cos** *value* | **default** | **discard-class** *value* | **dscp** *value* | **exp** *value* | **precedence** *value* | *min-threshold* [*units*] *max-threshold* [*units*] } 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# random-detect default`	デフォルトの最小しきい値および最大しきい値を使用した RED をイネーブルにします。

ステップ 5	**bandwidth** {*bandwidth* [*units*] | **percent** *value*} または **bandwidth remaining** [**percent** *value* | **ratio** *ratio-value*
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth percent 30`
	または
	
	`RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 20`
		（任意）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。
		または
		（任意）さまざまなクラスに残りの帯域幅を割り当てる方法を指定します。
		（注）
		• 非デフォルト クラスには、これらの設定のいずれかが必要です。

ステップ 6	**shape average** {**percent** *percentage* | *value* [*units*]} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# shape average percent 50`	（任意）指定されたビット レートまたは使用可能な帯域幅のパーセンテージに従い、トラフィックをシェーピングします。
ステップ 7	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 8	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 9	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/2/0/0`	コンフィギュレーション モードを開始し、インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 10	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシーマップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 11	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ランダム早期検出の設定

手順の概要

1.
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **random-detect** {**cos** *value* | **default** | **discard-class** *value* | **dscp** *value* | **exp** *value* | **precedence** *value* | *min-threshold* [*units*] *max-threshold* [*units*] }
5. **random-detect** {**discard-class** *value* | **dscp** *value* | **exp** *value* | **precedence** *value* | *min-threshold* [*units*] *max-threshold* [*units*] }
6. **bandwidth** {*bandwidth* [*units*] | **percent** *value*}
7. **bandwidth remaining percent** *value*
8. **shape average** {**percent** *percentage* | *value* [*units*]}
9. **exit**
10. **exit**
11. **interface** *type interface-path-id*
12. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	例： `RP/0//CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0//CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0//CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**random-detect** {**cos** *value* | **default** | **discard-class** *value* | **dscp** *value* | **exp** *value* | **precedence** *value* | *min-threshold* [*units*] *max-threshold* [*units*] }	最小および最大のしきい値を持つ RED を有効にします。

	コマンドまたはアクション	目的
	例： `RP/0/RP0/CPU0:router(config-pmap-c)# random-detect default`	
ステップ 5	**random-detect** {**discard-class** *value* | **dscp** *value* | **exp** *value* | **precedence** *value* | *min-threshold* [*units*] *max-threshold* [*units*] } 例： `RP/0/0/CPU0:router(config-pmap-c)# random-detect 1000000 2000000`	デフォルトの最小しきい値および最大しきい値を使用した RED をイネーブルにします。
ステップ 6	**bandwidth** {*bandwidth* [*units*] | **percent** *value*} 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth percent 30`	（任意）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。
ステップ 7	**bandwidth remaining percent** *value* 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth remaining percent 20`	（任意）さまざまなクラスに残りの帯域幅を割り当てる方法を指定します。
ステップ 8	**shape average** {**percent** *percentage* | *value* [*units*]} 例： `RP/0//CPU0:router(config-pmap-c)# shape average percent 50`	（任意）指定されたビット レートまたは使用可能な帯域幅のパーセンテージに従い、トラフィックをシェーピングします。
ステップ 9	**exit** 例： `RP/0//CPU0:router(config-pmap-c)# exit`	ルータをポリシーマップ コンフィギュレーション モードに戻します。
ステップ 10	**exit** 例： `RP/0//CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的

ステップ 11	**interface** *type interface-path-id*
	
	例：
	`RP/0//CPU0:router(config)# interface pos 0/2/0/0`
	
	例：
	`RP/0//CPU0:router(config-if)# service-policy output policy1`
		コンフィギュレーション モードを開始し、インターフェイスを設定します。
		インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシーマップを付加します。
		• この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 12	**end** または **commit**
	
	例：
	`RP/0//CPU0:router(config-cmap)# end`
	または
	`RP/0//CPU0:router(config-cmap)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータがEXECモードに戻ります。
		no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

重み付けランダム早期検出の設定

WREDは、指定した基準に基づいてパケットを選択的にドロップします（CoS、DSCP、EXP、廃棄クラス、優先順位など）。 WREDは、これらの一致基準を使用して、異なるタイプのトラフィックの処理方法を決定します。

random-detect コマンドと異なる CoS、DSCP、EXP、および廃棄クラスの値を使用して、WRED を設定します。 値には、そのフィールドにおいて有効な値の範囲またはリストを指定できます。

また、最小キューしきい値および最大キューしきい値を使用して、ドロップするポイントを決定できます。

パケットが着信すると、次の処理が行われます。

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

制約事項

random-detect dscp コマンドを設定する場合は、**shape average**、**bandwidth**、および **bandwidth remaining** のいずれかのコマンドを設定する必要があります。

クラスごとに 2 つの最小しきい値および最大しきい値（それぞれ異なる一致基準）のみを設定できます。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **random-detect dscp** *dscp-value min-threshold* [*units*] *max-threshold* [*units*]
5. **bandwidth** {*bandwidth* [*units*] | **percent** *value*} or **bandwidth remaining** [**percent** *value* | **ratio** *ratio-value]*
6. **bandwidth** {*bandwidth* [*units*] | **percent** *value*}
7. **bandwidth remaining percent** *value*
8. **shape average** {**percent** *percentage* | *value* [*units*]}
9. queue-limit *value* [*units*] RP/0/RSP0/CPU0:router(config-pmap-c)# queue-limit 50 ms
10. **exit**
11. **interface** *type inteface-path-id*
12. **service-policy** {**input** | **output**} *policy-map*
13. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**random-detect dscp** *dscp-value* *min-threshold* [*units*] *max-threshold* [*units*] 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# random-detect dscp af11 1000000 bytes 2000000 bytes`	DSCP 値の最小および最大パケットしきい値を変更します。 • WRED をイネーブルにします。 • *dscp-value*：DSCP 値を設定する 0～63 の数。 数値の代わりに、予約済みキーワードも指定できます。 • *min-threshold*：指定した単位の最小しきい値。 平均キューの長さが最小しきい値に達すると、WRED では、指定された DSCP の値で一部のパケットがランダムにドロップされます。 • *max-threshold*：指定した単位の最大しきい値。 キューの平均の長さが最大しきい値を超えると、WRED は指定した DSCP 値のすべてのパケットをドロップします。 • *units*：しきい値の単位。 これには、**bytes**、**gbytes**、**kbytes**、**mbytes**、**ms**（ミリ秒）、**packets**、または **us**（マイクロ秒）を指定できます。 デフォルトは **packets** です。 • 次に、DSCP AF11 のパケットで、WRED の最小しきい値が 1,000,000 バイト、最大しきい値が 2,000,000 バイトの場合の例を示します。

ステップ 5	**bandwidth** {*bandwidth* [*units*] | **percent** *value*} or **bandwidth remaining** [**percent** *value* | **ratio** *ratio-value]*
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth percent 30`
	または
	
	`RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 20`
		（任意）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。
		
		または
		
		（任意）さまざまなクラスに残りの帯域幅を割り当てる方法を指定します。
		
		（注） • 非デフォルト クラスには、これらの設定のいずれかが必要です。

	コマンドまたはアクション	目的
ステップ 6	**bandwidth** {*bandwidth* [*units*] | **percent** *value*} 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth percent 30`	（任意）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。 • この例では、class1 クラスへのインターフェイス帯域幅の 30% が保証されます。
ステップ 7	**bandwidth remaining percent** *value* 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth remaining percent 20`	（任意）さまざまなクラスに残りの帯域幅を割り当てる方法を指定します。 • 70 パーセントの残りの帯域幅は、設定済みのすべてのクラスで共有されます。 • この例では、class1 クラスは 70 % の 20 % を受信します。
ステップ 8	**shape average** {**percent** *percentage* | *value* [*units*]} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# shape average percent 50`	（任意）指定されたビット レートまたは使用可能な帯域幅のパーセンテージに従い、トラフィックをシェーピングします。
ステップ 9	queue-limit *value* [*units*] RP/0/RSP0/CPU0:router(config-pmap-c)# queue-limit 50 ms	（任意）キュー制限を変更して、各キューで使用可能なバッファ量を微調整します。 デフォルトのキュー制限は、指定されたキュー クラスのサービス レートの 100 ms です。
ステップ 10	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 11	**interface** *type inteface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0`	コンフィギュレーションモードを開始し、インターフェイスを設定します。
ステップ 12	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシーマップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。 • 入力ポリシーは無効です。**bandwidth** および **bandwidth remaining** コマンドは、入力ポリシーに適用できません。

	コマンドまたはアクション	目的

ステップ 13	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-cmap)# end`
	または
	`RP/0/RSP0/CPU0:router(config-cmap)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

テール ドロップの設定

クラスの一致基準を満たすパケットは、サービスを提供されるまで、クラス用に予約されたキューに蓄積されます。 **queue-limit** コマンドを使用して、クラスの最大しきい値を定義します。 最大しきい値に達したとき、クラス キューへの待機パケットはテール ドロップ（パケット ドロップ）します。

queue-limit の値には、**queue_bandwidth** の基準値として、キューの保証サービス レート（GSR）が使用されます。 クラスに帯域幅の割合が関連付けられている場合、**queue-limit** は、そのクラス用に予約された帯域幅の割合に設定されます。

キューの GSR がゼロの場合は、次を使用してデフォルトの **queue-limit** を計算します。

- 非階層型ポリシー内のキューのインターフェイス帯域幅の 1%。
- 階層型ポリシー内のキューの最小の親シェーピング レートおよびインターフェイス レートの 1%。

デフォルト キュー制限（パケット数）= (200 ms * (キューの帯域幅またはシェーパー比率) / 8) /平均パケット サイズ（250 バイト）

（注） デフォルトの **queue-limit** は、キューの帯域幅の 100 ms のバイトに設定されます。 デフォルトのキュー制限の計算（バイト単位）には、次の式が使用されます。??bytes = (100 ms / 1000 ms) * queue_bandwidth kbps)) / 8

制約事項

- クラス内で **queue-limit** コマンドを設定する場合は、**priority**、**shape average**、**bandwidth**、または **bandwidth remaining** のいずれかのコマンドを設定する必要があります。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **queue-limit** *value* [*units*]
5. **class** *class-name*
6. **bandwidth** {*bandwidth* [*units*] | **percent** *value*}
7. **bandwidth remaining percent** *value*
8. **exit**
9. **exit**
10. **interface** *type interface-path-id*
11. **service-policy** {**input** | **output**} *policy-map*
12. 次のいずれかのコマンドを使用します。
    - **end**
    - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。

	コマンドまたはアクション	目的
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。

ステップ 4	**queue-limit** *value* [*units*]
	
	例：
	`RP/0/RSP0/CPU0:router(config-pmap-c)# queue-limit 1000000 bytes`
	
	例：
	`RP/0//CPU0:router(config-pmap-c)# priority level 1`
	
	例：
	`RP/0//CPU0:router(config-pmap-c)# police rate percent 30`
		ポリシー マップに設定したクラス ポリシー用にキューが保持できる最大値を指定または変更します。 *units* 引数のデフォルト値は **packets** です。
		• この例では、キュー制限が 1,000,000 バイトに到達すると、このクラス キューへの待機パケットはドロップされます。
		
		ポリシー マップに属するトラフィックのクラスにプライオリティを指定します。
		
		トラフィック ポリシングを設定します。

ステップ 5	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class2`	ポリシーを作成または変更するクラスの名前を指定します。 • この例では、class2 が設定されます。
ステップ 6	**bandwidth** {*bandwidth* [*units*] | **percent** *value*} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth percent 30`	（任意）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。 • この例では、クラス class2 へのインターフェイス帯域幅の 30% が保証されます。
ステップ 7	**bandwidth remaining percent** *value* 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth remaining percent 20`	（任意）さまざまなクラスに残りの帯域幅を割り当てる方法を指定します。 • この例では、残りのインターフェイス帯域幅の 20 % を class2 クラスに割り当てます。
ステップ 8	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 10	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface pos 0/2/0/0`	コンフィギュレーション モードを開始し、インターフェイスを設定します。
ステップ 11	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシー マップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 12	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

その他の関連資料

ここでは、QoS 輻輳回避の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
初期システム起動と設定	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
マスター コマンド リファレンス	『*Cisco ASR 9000 Series Aggregation Services Router Master Command Listing*』
QoS コマンド	『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』
ユーザ グループとタスク ID	『Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide』の「Configuring AAA Services on Cisco ASR 9000 Series Router」モジュール

標準

標準	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
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

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
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

第 5 章

モジュラ QoS の輻輳管理の設定

輻輳管理は、ネットワーク上で輻輳が発生した後に輻輳を制御します。 輻輳の管理は、パケットキューイング方式を使用し、トラフィック調整メカニズムを使用してパケットフローをシェーピングすることにより、Cisco IOS XR ソフトウェア上で行われます。

サポートされているトラフィック調整メカニズムのタイプは、次のとおりです。

- トラフィック シェーピングは、次のことを実行します。
  - Modified Deficit Round Robin（MDRR）
  - 低遅延キューイング（LLQ）とストリクト プライオリティ キューイング（PQ）
- トラフィック ポリシングは、次のことを実行します。
  - カラー ブラインド
  - カラーアウェア（入力方向）

ラインカード、SIP および SPA のサポート

次の表に、ASR 9000 イーサネット ラインカードおよび ASR 9000 用 SIP 700 でサポートされる機能を示します。

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
DEI を使用した輻輳管理	no	yes
保証帯域幅および残存帯域幅	yes	yes
低遅延キューイングとストリクト プライオリティ キューイング	yes	yes
トラフィック ポリシング	yes	yes

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
トラフィック シェーピング	yes	yes

Cisco ASR 9000 シリーズ ルータのモジュラ QoS の輻輳管理の設定に関する機能履歴

リリース	変更内容
リリース 3.7.2	輻輳回避機能が ASR 9000 イーサネット ラインカードで導入されました。 保証帯域幅、残存帯域幅、低遅延キューイングとストリクトプライオリティ キューイング、トラフィック ポリシング、およびトラフィック シェーピングの各機能が ASR 9000 イーサネット ラインカードで導入されました。
リリース 3.9.0	保証帯域幅、残存帯域幅、低遅延キューイングとストリクトプライオリティ キューイング、トラフィック ポリシング、およびトラフィック シェーピングの各機能が ASR 9000 用 SIP 700 でサポートされました。
リリース 4.0.0	DEI 機能を使用した輻輳管理が ASR 9000 イーサネット ラインカードで導入されました。
リリース 4.0.1	**police rate** コマンドの更新により、ポリシング レートおよびバースト サイズのパケットベースでの指定が追加されました。
リリース 4.1.0	2 レート 3 カラー ポリサー機能が追加されました（**conform-color** コマンドおよび **exceed-color** コマンドを含む）。 この機能は、SIP 700 ラインカードの入力側に適用されます。
リリース 4.2.1	IPv6ACL 機能に対して設定されたアカウンティングおよび QoS が追加されました。

- QoS 輻輳管理を設定するための前提条件，63 ページ
- 輻輳管理の設定に関する情報，63 ページ
- QoS 輻輳管理の設定方法，80 ページ
- BVI に対するトラフィック ポリシング，106 ページ
- ECN の設定，110 ページ
- 輻輳管理の設定例，112 ページ

• その他の関連資料, 116 ページ

QoS 輻輳管理を設定するための前提条件

ネットワークでの QoS 輻輳管理を設定するには、次の前提条件を満たす必要があります。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。 ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- Cisco IOS XR QoS の設定作業と概念に関する知識が必要です。

輻輳管理の設定に関する情報

輻輳管理を設定するには、次の概念を理解する必要があります。

輻輳管理の概要

輻輳管理機能では、パケットに割り当てられた優先順位に基づいて、トラフィック フロー（またはパケット）がインターフェイスに送信される順番を決定することにより、輻輳を制御できます。輻輳管理は、キューを作成し、そのキューにパケットの分類に基づいてパケットを割り当て、キューにあるパケットの送信をスケジューリングする必要があります。 Cisco IOS XR ソフトウェアの輻輳管理機能を使用すると、異なる番号のキューの作成を指定したり、トラフィックの差別の度合いを大きくまたは小さくしたり、トラフィックが送信される順番を指定したりできます。

トラフィック フロー量が少ない間、つまり輻輳が存在しないときは、パケットは、着信するとすぐにインターフェイスに送信されます。 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。 輻輳管理機能を使用すると、インターフェイスに蓄積しているパケットが、インターフェイスでパケットを送信できるようになるまでキューイングされます。その後、パケットに割り当てられたプライオリティと、インターフェイスに設定されたキューイング方式に従って送信がスケジューリングされます。 ルータで、どのパケットをどのキューに配置するかや、キューをそれぞれどのように処理するかをコントロールすることで、パケット送信の順番が決定されます。

パケットが契約およびサービスに従うようにするには、キューイング方式に加えて、ポリサーやシェーパーなどの Qo S 輻輳管理メカニズムが必要です。 ポリシングとシェーピングの両方のメカニズムでは、パケットのトラフィック記述子を使用します。

ポリサーとシェーパーは、通常はトークンバケットメカニズムを使用した同じ方法でトラフィック記述子違反を識別しますが、違反への対応方法は異なります。 ポリサーは、通常トラフィック フローをドロップします。一方、シェーパーは、バッファまたはキューイング メカニズムを使用して過剰なトラフィック フローを遅らせることにより、トラフィックを保持して後で送信します。

トラフィック シェーピングとトラフィック ポリシングは連携して機能します。 たとえば、優れたトラフィック シェーピング スキームを使用すると、ネットワーク内のノードの異常なフローを簡単に検出できます。

Modified Deficit Round Robin：欠陥修正ラウンド ロビン

MDRRは、最大8個のトラフィック クラスのキューイングが可能なクラスベースの複合スケジューリング メカニズムです。 MDRR はクラスベース重み付け均等化キューイング（CBWFQ）と同様に動作し、顧客の一致基準（アクセスリストなど）に基づくトラフィック クラスの定義が可能になります。ただし、MDRR では重み付け均等化キューイング アルゴリズムは使用されません。

MDRRがキューイング戦略に設定されている場合は、空ではないキューが1つずつ処理されます。キューが処理されるたびに、一定量のデータがキューから取り出されます。 その後に、アルゴリズムは次のキューを処理します。 キューが処理されると、キューから取り出された設定値を超えるデータのバイト数がMDRRに記録されます。 次のパスでは、キューを再び処理するときに、以前に処理された超過データを埋め合わせるために、より少ないデータがキューから取り出されます。 その結果、キュー単位でキューから取り出されるデータの平均量が設定値に近くなります。また、MDRRにより、遅延に影響されやすいトラフィックのストリクト プライオリティ キューが可能になります。

MDRR 内の各キューは 2 つの変数で定義されます。

- 定量値：各ラウンドで処理される平均バイト数。
- 不足カウンタ：各ラウンドでキューから送信されるバイト数。 カウンタは、定量値に合わせて初期化されます。

キューのパケットは不足カウンタがゼロより大きい限り処理されます。 各パケットが処理されると、そのバイト長と同じ値だけ不足カウンタが減少します。 不足カウンタがゼロまたは負になった後には、キューを処理できなくなります。 新しい各ラウンドでは、空ではない各キューの不足カウンタが定量値の分だけインクリメントされます。

低遅延キューイングとストリクト プライオリティ キューイング

LLQ機能により、MDRRスケジューリング メカニズムにおいてストリクト プライオリティ キューイング（PQ）を使用できます。 ストリクト プライオリティ モードの PQ は、場合によっては他のすべてのトラフィックを犠牲にして、1 つのタイプのトラフィックが送信されることを確保します。 PQ では、低プライオリティ キューは悪影響を受けることがあり、最悪の場合、帯域幅の一部が使用可能な場合や、クリティカルなトラフィックの伝送レートが高い場合に、そのパケットが送信できなくなります。

ストリクトPQでは、音声などの遅延に影響されやすいデータを、他のキューのパケットをキューから取り出す前にキューから取り出して送信できます。

LLQ により、MDRR 内の単一のストリクト プライオリティ キューをクラス レベルでイネーブルにし、クラスに属するトラフィックを誘導できます。 ストリクト プライオリティ キューに従ってクラストラフィックをランク付けするには、ポリシーマップの名前が付いたクラスを指定し、

priority コマンドをクラスに設定します。（**priority** コマンドが適用されるクラスは、プライオリティ クラスだと見なされます）。ポリシー マップで、1 つまたは複数の優先ステータスを指定できます。1 つのポリシー マップに複数のクラスがプライオリティ クラスとして設定されている場合、これらのクラスからのトラフィックはすべて、同じ単一の完全プライオリティ キューに入力されます。

priority コマンドを使用すると、トラフィックの指定に使用する有効な一致基準のいずれかにストリクト PQ を割り当てることができます。 クラスへのトラフィックの指定方式には、アクセス リスト、プロトコル、IP precedence、および IP DiffServ コード ポイント（DSCP）値などがあります。 さらに、アクセス リスト内で、IP ヘッダーの IP タイプ オブ サービス（ToS）バイトの最初の 6 ビットを使用して設定した DSCP 値に基づいたトラフィックの一致が可能になるよう指定できます。

設定されているアカウンティング

設定されているアカウンティングは、ポリシングおよびシェーピングのオーバーヘッド（パケット長）を制御します。ポリシーをインターフェイスに適用するときに、サービスポリシーでアカウント オプションを指定できます。 バンドル インターフェイスでは、設定されたアカウンティング オプションは、すべてのメンバ インターフェイスに適用されます。

設定されたアカウンティング オプションはCRS-MSC-140Gでの入力および出力ポリシング、キューイング、および統計情報に使用できます CRS-MSC-40G では、設定されているアカウンティング オプションはキューイングに使用できません。

前提条件および制約事項

- 接続されたインターフェイスで提供される QoS 処理と一致するように、パケット サイズのアカウンティングを調整できます。
- ASR 9000 イーサネット ラインカードおよび Enhanced Ethernet ラインカードでサポートされます。
- サポートされるアカウント値は、-48 ～ +48 です。
- 入力シェーピング アカウンティングはサポートされません（入力および出力ポリシング アカウンティングと出力シェーピング アカウンティングはサポートされます）。
- ポリシー適用後の動的なアカウンティング オーバーヘッドの変更はサポートされません

IPv6 ACL の QoS

Modular Weapon-X ラインカードは、送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル、ToS、ホップ リミット、およびACLベースの分類に基づいてIPv6プロパティの分類をサポートします。

サポートされているインターフェイスを以下に示します。

サポートされているインターフェイス	イーサネット ラインカード	Enhanced Ethernet ラインカード
L3 メイン インターフェイス	yes	yes
L3 サブ インターフェイス	yes	yes
L3 バンドル インターフェイス/サブ インターフェイス	yes	yes
L2 メイン インターフェイス	no	yes
L2 サブ インターフェイス	no	yes
L2 バンドル インターフェイス/サブ インターフェイス	no	yes

トラフィック シェーピング

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

送信元からターゲット インターフェイスへのデータ伝送レートを一致させるには、次のいずれかに合わせてデータ転送を制限できます。

- 特定の設定レート
- 輻輳レベルに基づいて抽出されたレート

転送レートは、トークン バケットを構成する 3 つの要素（バースト サイズ、中間レート、および時間（測定）間隔）に依存します。 中間レートは、バースト サイズを時間間隔で割った商と一致します。

トラフィック シェーピングがイネーブルになっている場合は、インターフェイスのビット レートが、時間間隔の整数倍を超えて、中間レートを上回ることはありません。 つまり、すべての時間間隔で、最大バースト サイズを送信できます。 ただし、時間間隔内の任意の時点で、ビット レートが中間レートを上回ることがあります。

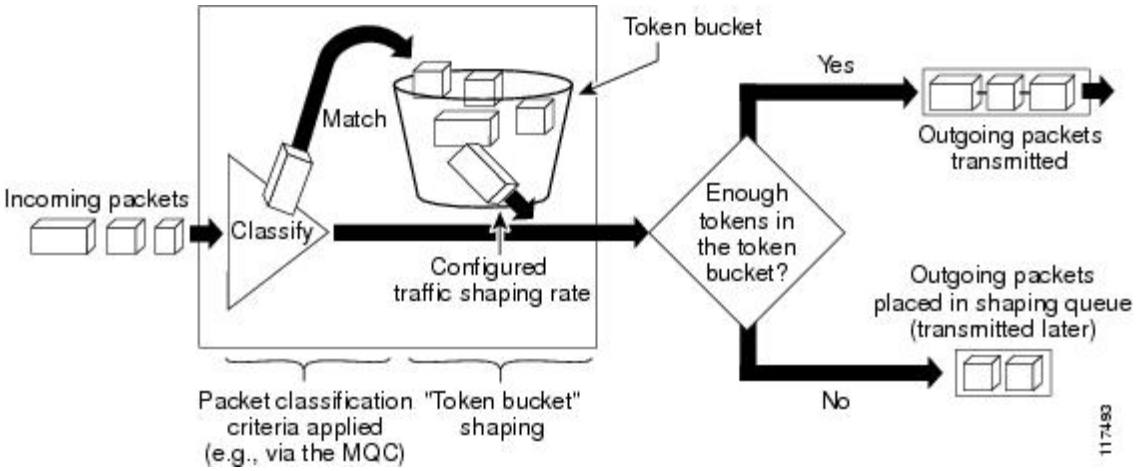
ピーク バースト サイズが 0 の場合は、インターフェイスが時間間隔ごとにバースト サイズしか送信しないため、平均レートが中間レートを超えることはありません。 ただし、ピーク バースト サイズが 0 より大きい場合は、過去に最大量が送信されたことがなければ、インターフェイスは 1 バースト内でバースト サイズとピーク バーストを足したビット数を送信できます。 ある時間間隔中にバースト サイズ未満のビット数が送信された場合は、ピーク バースト サイズを超えない残りのビット数を使用して、次の時間間隔でバースト サイズを超えるビット数を送信できます。

シェーピング メカニズムによるトラフィックの調整

着信パケットがインターフェイスに着信すると、分類技術（アクセス コントロール リスト（ACL）、モジュラ QoS CLI（MQC）による IP precedence ビットの設定など）を使用してパケットが分類されます。パケットが、指定された分類と一致した場合は、トラフィック シェーピング メカニズムが継続されます。 そうでない場合は、それ以上の処理が行われません。

図 1 に、トラフィック シェーピング メカニズムによるトラフィック フローの調整方法を示します。

図 *3*：トラフィック シェーピング メカニズムによるトラフィックの調整方法



指定された条件を満たしているパケットが、トークン バケット内に配置されます。 トークン バケットの最大サイズは、適合バースト（Bc）サイズ＋Be サイズです。 トークン バケットは、Tc ごとに Bc に相当するトークンの固定レートで満たされます。 これは、設定されたトラフィック シェーピング レートです。

トラフィック シェーピング メカニズムがアクティブ（つまり、設定されたトラフィック シェーピング レートを上回るパケットがすでに転送キュー内に存在する）場合は、Tc ごとに、トラフィック シェーパーが、転送キュー内に送信に十分なパケットが存在する（つまり、トラフィックの最大 Bc（または Bc＋Be）に到達している）かどうかをチェックします。

トラフィック シェーパーがアクティブになっていない（つまり、転送キュー内に設定されたトラフィック シェーピングを上回るパケットが存在しない）場合は、トラフィック シェーパーがトークン バケット内のトークンの数をチェックします。 次のどちらかになります。

- トークン バケット内に十分なトークンが存在する場合は、パケットが送信（転送）されます。
- トークンバケット内に十分なトークンが存在しない場合は、パケットが後で転送するためにシェーピング キュー内に配置されます。

トラフィック ポリシング

一般的に、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たり、ネットワークを複数のプライオリティ レベルまたはサービス クラス（CoS）に区切ることができます。

トラフィック ポリシングでは、トークン バケット アルゴリズムを介して、トラフィックの最大レートを管理します。 トークン バケット アルゴリズムでは、ユーザが設定した値を使用して、特定の瞬間にインターフェイス上で許可されるトラフィックの最大レートを決定します。 トークン バケット アルゴリズムは、（トラフィック ポリシングでトラフィック ポリシーが設定された場所により）インターフェイスを出入りするすべてのトラフィックによって影響を受け、複数の大きなパケットが同じトラフィック ストリームで送信される場合に、ネットワーク帯域幅の管理に役立ちます。

トラフィック ポリシングは、多くの場合、ネットワークに出入りするトラフィックのレートを制限するためにネットワークのエッジのインターフェイスで設定されます。最も一般的なトラフィック ポリシングの設定では、CIR に適合したトラフィックは送信され、超過したトラフィックはプライオリティを下げて送信されるかドロップされます。 ユーザはネットワークのニーズに合わせてこれらの設定オプションを変更できます。 トラフィック ポリシングでは、認定情報レート（CIR）のバースト サイズ（Bc）を設定することにより、一定量の帯域幅管理も行えます。 最大情報レート（PIR）がサポートされている場合は、2番めのトークン バケットが有効になり、トラフィック ポリサーは 2 レート ポリサーと呼ばれます。

ポリシング メカニズムによるトラフィックの調整

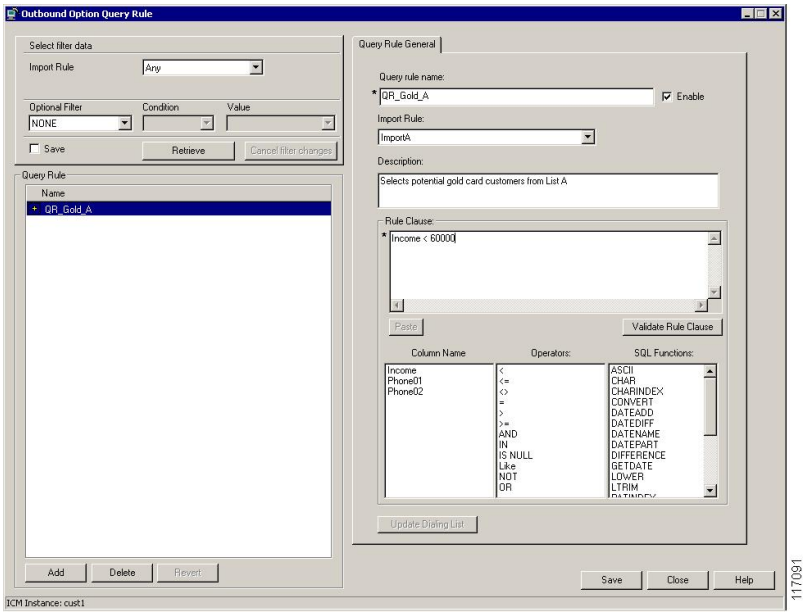
ここでは、シングルレート ポリシング および 2 レート ポリシング メカニズムについて説明します。

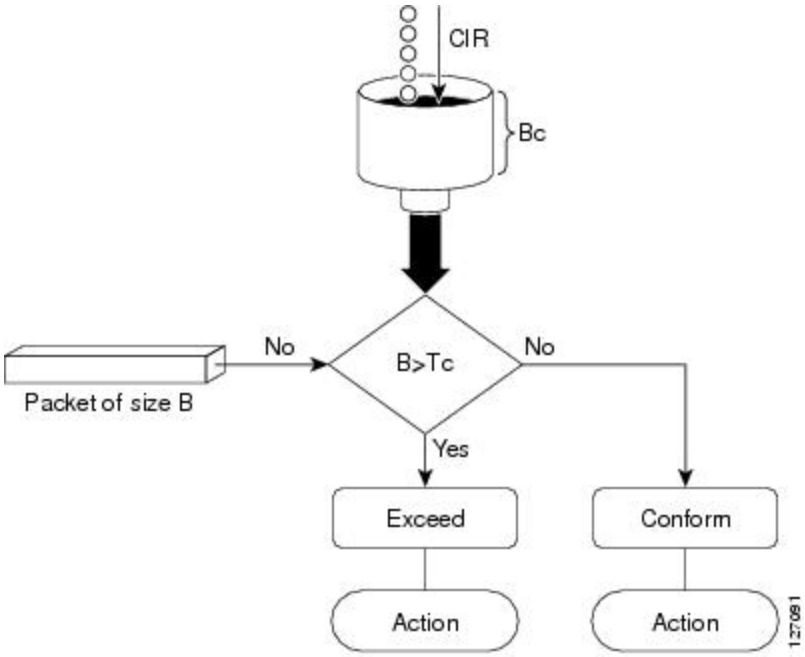
シングルレート ポリサー

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

図 2 に、シングルレートのトークン バケット ポリサーにより、CIR 適合または CIR 超過としてパケットをマーキングし、アクションを割り当てる方法を示します。

図 4：パケットのマーキングおよびアクションの割り当て：シングルレート ポリサー





トークンバケットへのトークン更新の間隔（Tc）は、パケットがトラフィック ポリサーに着信するたびに CIR 値で更新されます。 Tc トークン バケットには Bc 値まで含めることができ、この値には、特定のバイト数または期間を指定できます。 サイズ B のパケットが Tc トークン バケット

を超える場合、パケットはCIR 値を超え、設定されたアクションが実行されます。 サイズ B のパケットが Tc トークン バケット未満の場合、パケットは適合し、設定された異なるアクションが実行されます。

2 つのレートを使用したポリシング機能

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

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

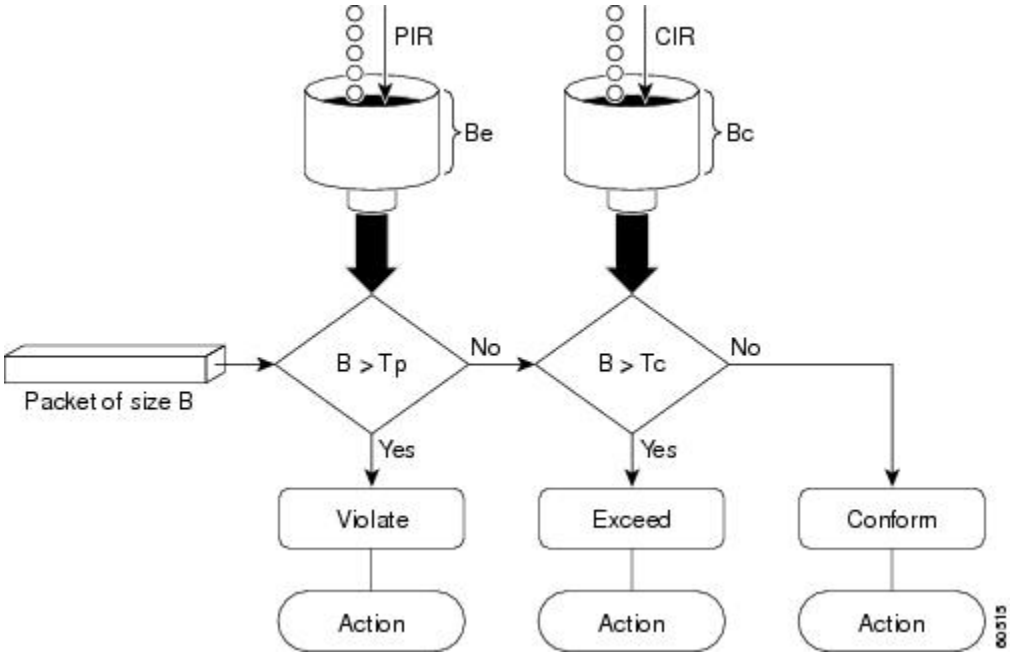
- 一定時間での平均バイト数により認定トークン バケットがオーバーフローしない場合、トラフィック ストリームは適合しています。 この場合、トークン バケット アルゴリズムはトラフィック ストリームを緑色でマーキングします。
- トラフィック ストリームにより認定トークン バケットが最大トークン バケットにオーバーフローした場合、トラフィック ストリームは超過しています。 この場合、トークン バケット アルゴリズムはトラフィック ストリームを黄色でマーキングします。 トラフィックがポリシング レートを超過している間は、最大トークン バケットが満たされた状態になります。

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

デュアルトークン バケット アルゴリズムでは、各パケットに対する 3 つのアクション（conform アクション、exceed アクション、および任意の violate アクション）を使用できます。 2 レート ポリサーを設定した状態でキューに入るトラフィックは、これらのカテゴリのいずれかに配置されます。 これら 3 つのカテゴリ内で、ユーザはパケットの処理を決定できます。 たとえば、適合するパケットは送信されるように設定し、超過するパケットはプライオリティを低くして送信されるように設定し、違反するパケットはドロップされるように設定できます。

図 3 に、2 レート ポリサーを使用してパケットをマーキングする方法、および対応するアクションをパケットに割り当てる方法を示します。

図 *5*：パケットのマーキングおよびアクションの割り当て：*2* レート ポリサー



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

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

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

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

- 着信パケットが CIR を超過した場合、ルータはパケットに対して confirm アクションを実行し、そのパケットのバイト数だけ認定トークン バケットをデクリメントし、パケットのオーバーフロー バイト数だけ最大トークン バケットをデクリメントします。
- 着信パケットが PIR を超過した場合、ルータはパケットに対して違反アクションを実行しますが、最大トークン バケットをデクリメントしません。

認定バーストおよび超過バースト

トラフィック シェーパーとは異なり、トラフィック ポリサーは超過パケットをバッファせず、後で送信します。 代わりに、ポリサーはバッファリングせずに「送信または送信なし」のポリシーを実行します。 輻輳期間中には、超過バースト パラメータを適切に設定することにより、ポリサーによるパケットのドロップを抑えることができます。 したがって、ルータがポリシングが認定（標準）バースト値および超過バースト値を使用して、設定された認定情報レート（CIR）に到達することを確保する仕組みを理解することが重要です。

バースト パラメータは、ルータの一般的なバッファリング ルールに基づいており、ラウンドトリップ時間のビットレートと同じになるようにバッファリングを設定して、輻輳期間中におけるすべての接続の、未処理の TCP ウィンドウに対応することが推奨されます。

ここでは、認定バーストと超過バースト、およびこれらを計算するための推奨される式について説明します。

- 認定バースト
- 超過バースト
- 認定レートに対するパケットの適合または超過の決定

認定バースト

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

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

- パケットが着信したときに、適合トークン バケットに十分なトークンがある場合、メーターはパケットを緑色でマーキングし、パケットのバイト数だけ適合トークン カウントをデクリメントします。
- 適合トークン バケットの使用可能なトークンが不十分な場合は、メーターにより、トラフィック フローは必要なトークンを借りてパケットを送信できます。 メーターはパケットのバイト数の超過トークン バケットをチェックします。 超過トークン バケットに使用可能な十分な数のトークンがある場合、メーターはパケットを次のようにマーキングします。

  緑色：適合トークン カウントを最小値の 0 に達するまでデクリメントします。

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

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

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

デフォルトの認定バースト サイズは、ポリシング レートでの 2 ミリ秒のバイト数、またはネットワークの最大伝送ユニット（MTU）よりも大きくなります。

認定バーストの計算

認定バーストを計算するには、次の式を使用します。

bc = CIR bps * (1 バイト) / (8 ビット) * 1.5 秒

（注） 通常のラウンドトリップ時間は 1.5 秒です。

たとえば、認定情報レートが 512000 bps の場合、認定バーストの式を使用した認定バーストは 96000 バイトになります。

bc = 512000 * 1/8 * 1.5

bc = 64000 * 1.5 = 96000

（注） be 値が 0 になる場合は、出力 bc 値を、入力 bc 値に 1 を足した値以上に設定することを推奨します。 そうしないと、パケット損失が発生する場合があります。 次に例を示します。 be = 0
出力 bc >= 入力 bc + 1

超過バースト

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

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

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

超過バーストの計算

超過バーストを計算するには、次の式を使用します。

be = 2 * 認定バースト

たとえば、4000 バイトの認定バーストを設定した場合、超過バーストの式を使用した超過バーストは 8000 バイトになります。

be = 2 * 4000 = 8000

デフォルトの超過バースト サイズは 0 です。

認定レートに対するパケットの適合または超過の決定

設定された認定情報レート（CIR）に達するように、ポリシングは標準つまり適合バースト（bc）値と超過バースト（be）値を使用します。ポリシングは、設定したバースト値に基づいて、パケットが CIR に適合しているか、または CIR を超過しているかを決定します。次のように、複数の要素がポリサーの決定に影響する可能性があります。

- 低いバースト値：低すぎるバースト値を設定した場合は、達成されるレートが設定されたレートよりかなり低くなる場合があります。
- 一時的なバースト：このようなバーストは、伝送制御プロトコル（TCP）のトラフィックのスループットに重大な悪影響を及ぼすことがあります。

良好なスループットを確保するには、十分高いバースト値を設定することが重要です。適合レートが設定した CIR 未満であるにもかかわらず、ルータがパケットをドロップし、超過したレートを報告する場合は、show interface コマンドを使用して現在のバーストをモニタし、表示された値が一貫して認定バースト（bc）値および超過バースト（be）値に近い値であるか、実際のレート（認定レートおよび超過レート）が設定した認定レートに近い値であるかを確認します。該当しない場合は、バースト値が低すぎる可能性があります。認定バーストの計算および超過バーストの計算の項の推奨計算を使用してバースト レートを再設定してみてください。

2 レート 3 カラー（2R3C）ポリサー

SIP 700 カードでは、入力レイヤ 2 インターフェイスのポリシーマップで 2 レート 3 カラー（2R3C）ポリサーがサポートされます。ポリサーは、以前のネットワーク ノードのポリサーによって設定

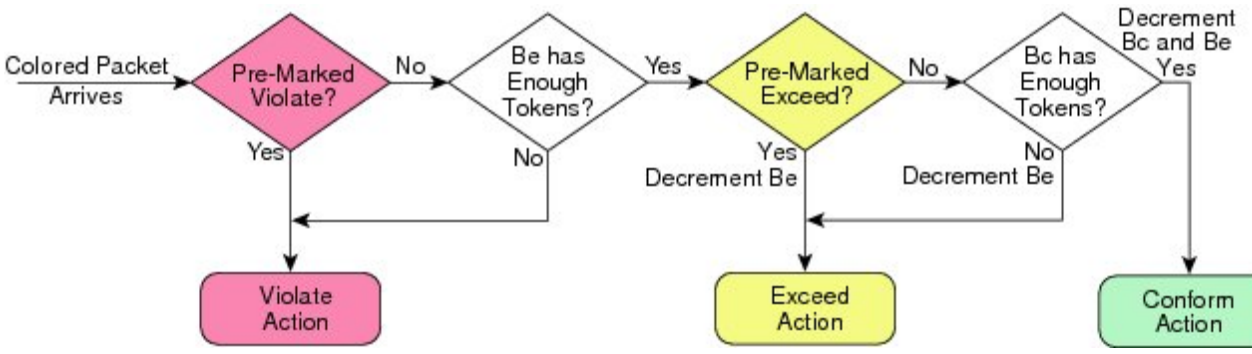
された既存のマーキング（パケット ヘッダーのフレーム リレーの破棄適性（FRDE）ビット）を読み取ります。 デフォルトでは、FRDE ビットは 0 に設定されます。 受信ノードのシステムは、このビットを使用してパケットの適切なカラーアウェア ポリシング アクションを決定します。

- FRDE ビット値 0 を適合カラーとして分類するには、frde=0 パケットの適合カラー クラスマップを作成します。 これにより、パケットが緑色のカラーとして分類され、システムにより conform アクションが適用されます。
- FRDE ビット値 1 を超過カラーとして分類するには、frde=1 パケットの超過カラー クラスマップを作成します。 これにより、パケットが黄色のカラーとして分類され、システムにより exceed アクションが適用されます。

（注） カラーアウェア ポリシングは、階層型 QoS ではサポートされません。

図 4 に、2R3C ポリシング プロセスを示します。

図 *6*：*2R3C* ポリシング プロセスのフローチャート



階層型ポリシング

階層型ポリシング機能は、Cisco ASR 9000 シリーズ ルータ上の入力インターフェイスと出力インターフェイスの両方での階層型ポリシングをサポートする、MQC ベースのソリューションです。

この機能により、着信インターフェイス上で異なる QoS クラスの分類のサブモデルを適用しながら、サービス レベル契約（SLA）を実施できます。

階層型ポリシングは、次の 2 つのレベルでのサポートを提供します。

- 親レベル
- 子レベル

複数アクション設定

set-mpls-exp-imp、set-clp

IP precedence 値、IP DSCP 値、および MPLS EXP 値の設定によるパケット マーキング

レート制限に加えて、トラフィック ポリシングでは、指定したレートにパケットが適合または違反しているかに従って、パケットをマーキング（または分類）できます。パケット マーキングにより、ネットワークを複数のプライオリティ レベルまたは CoS に区切ることもできます。 ポリサーのアクションとしてのパケット マーキングは、条件付きマーキングです。

ネットワークに入るパケットの IP precedence 値、IP DSCP 値、またはマルチプロトコル ラベル スイッチング（MPLS）EXP 値を設定するには、トラフィック ポリサーを使用します。 ネットワーク内にあるネットワーキング デバイスは、この設定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、重み付けランダム早期検出（WRE）機能では、IP precedence 値を使用して、パケットがドロップされる確率を決定します。

トラフィックをマーキングする際に、トラフィック ポリシングを使用しない場合は、パケットの分類を実行する方法について、「クラスベースの無条件パケット マーキングの例」の項を参照してください。

（注） MPLS 対応インターフェイス上で IP フィールドをマーキングすると、特定のインターフェイス上での動作が停止します。

明示的輻輳通知について

モバイル ネットワークでは、基地局コントローラ（BSC）は、特定のセル サイトが特定のリンクのトラフィックによって過負荷になっているかどうかを認識していません。その理由は、BSCは、ASR9000シリーズルータの背後に存在し、リンクに重大な輻輳があっても、トラフィックを送信し続けるためです。 したがって、セル サイトがトラフィックに（明示的輻輳通知）ECN ビットでマーキングして BSC に送信すると、BSC は、ASR9000 シリーズ ルータ向けに ECN ビットのフラグが付けられた輻輳サイトからの影響を受けるセッションにマーキングします。

ECNは、WRED（重み付けランダム早期検出）に対する拡張です。平均キュー長が特定のしきい値を超えた場合、ECNは、それらをドロップする代わりにパケットにマーキングします。設定された場合、ECNは、ルータとエンドホストが、ネットワークが輻輳状態であり、パケットの送信速度が低下しているのを認識できるようにします。 ただし、キュー内のパケット数が最大しきい値を上回っている場合、パケットはドロップ確率に基づいてドロップされます。 これは、ルータ上で ECN を設定せずに WRED が有効化されている場合に、パケットが受けるのと同一の処理です。

制限事項

- ECN は、ASR 9000 SIP-700 ラインカード上でのみサポートされます。

ECN 機能の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide*』を参照してください。

ECN の実装

ECN の実装には、IP ヘッダー内に 2 つのビット（ECN-capable Transport（ECT）ビットと CE（Congestion Experienced）ビット）を持つ ECN 固有のフィールドが必要です。 ECT ビットと CE ビットを使用して、00 から 11 の 4 つの ECN フィールドの組み合わせを作成できます。 最初の数字は ECT ビットで、2 番目の数字は CE ビットです。

ECN ビットの設定

ECT ビット	CE ビット	組み合わせが示す内容
0	0	ECN 非対応。
0	1	転送プロトコルのエンドポイントは ECN 対応です。
1	0	転送プロトコルのエンドポイントは ECN 対応です。
1	1	Congestion Experienced

ECN のフィールドの組み合わせ 00 は、パケットが ECN を使用していないことを示します。 ECN のフィールドの組み合わせ 01 と 10（それぞれ着信側 ECT（1）と ECT（0））は、データの送信側によって設定され、転送プロトコルのエンドポイントが ECN 対応であることを示します。 ルータは、これらの 2 つのフィールドの組み合わせを同様に取り扱います。 データの送信元は、これらの 2 つの組み合わせの 1 つまたは両方を使用できます。 ECN フィールドの組み合わせ 11 は、エンドポイントに対する輻輳を示します。 ルータの満杯のキューに到着するパケットはドロップされます。

ECN がイネーブルの場合のパケット処理

キュー内のパケット数が最小しきい値未満の場合、パケットが送信されます。 これは ECN がイネーブルになっているかどうかに関係なく実行されます。この処理は、ネットワーク上で WRED だけが使用されている場合、パケットが受けるのと同一の処理です。 キュー内のパケット数が最大しきい値を上回っている場合、パケットはドロップ確率に基づいてドロップされます。 これは、ルータ上で ECN を設定せずに WRED が有効化されている場合に、パケットが受けるのと同一の処理です。 キュー内のパケット数が最小しきい値と最大しきい値の間の場合、3 つの異なるシナリオが存在します

- パケットの ECN のフィールドにエンドポイントが ECN 対応であることが示されている（つまり、ECT ビットが 1 および CE ビットが 0 に設定されているか、または ECT ビットが 0 および CE ビットが 1 に設定されている）場合、および WRED アルゴリズムによってパケットが廃棄確率に基づいてドロップされると判断される場合には、パケットの ECT ビットと CE ビットが 1 に変更され、パケットが送信されます。 これは、ECN がイネーブルであり、パケットがドロップされる代わりにマークされているために発生します。
- パケットの ECN のフィールドによって、どちらのエンドポイントも ECN 対応ではないことが示されている（つまり、ECT ビットが 0 設定され、CE ビットが 0 に設定されている）場合、パケットは、WRED 廃棄確率に基づいてドロップされる可能性があります。 これは、

ルータ上で ECN を設定せずに WRED が有効化されている場合に、パケットが受けるのと同一の処理です。

- パケットの ECN のフィールドに、ネットワークで輻輳が発生していることが示されている（つまり、ECT ビットと CE ビットの両方が 1 に設定されている）場合、パケットが送信されます。 これ以上のマーキングは必要ありません。

ブリッジ グループ仮想インターフェイスの QoS

統合ルーティングとブリッジング（IRB）は、ブリッジ グループ仮想インターフェイス（BVI）を使用して、ブリッジ グループとルーテッドのドメイン間でルーティングする機能を提供します。

BVI は、ルータ内の仮想インターフェイスであり、ブリッジングをサポートしないが、ルータ内のルーテッド インターフェイスに相当するブリッジ グループを代表する、正常なルーテッド インターフェイスのように動作します。 BVI のインターフェイス番号は、仮想インターフェイスが代表するブリッジ グループの番号です。 この番号が BVI とブリッジ グループ間のリンクになります。

IRB BVI の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*』を参照してください。

BVI に対する QoS

BVI に対する QoS サポートでは、仮想インターフェイスに対してポリシー マップを直接適用できます。 これにより、仮想インターフェイスの集約ポリシングおよびマーキングが可能になります。 ポリシーは、BVI の入力側または出力側に適用して、ブリッジ ドメインとやり取りするトラフィックにマーキングおよびポリシングすることができます。

制約事項

BVI に対する QoS は、次をサポートしていません。

- イーサネットおよび SIP 700 ラインカード（ASR9000 Enhanced Ethernet ラインカードのみサポート）。
- 双方向フォワーディング検出（BFD）、共有ポリシー インスタンス、L1 オーバーヘッド アカウンティング。
- VLAN タグ、DEI の分類およびマーキング。
- シェーピングと帯域幅を含むキュー QoS。
- 上位レベルの基準ポリサー レートを持たない下位レベルのパーセンテージ ポリサー。
- ボーダー ゲートウェイ プロトコル（BGP）を使用した QoS ポリシー伝搬

（注） キューイングは、qos-group をマーキングし、qos-group に一致するインターフェイス ポリシーを追加することによって実行できます。

制限事項

- スケール制限：2000 BVI（ポリシーごとに 8 クラス）
- ポリ サー制限：8000 ポリサー（ネットワーク プロセッサごと）

BVI の分類とマーキング

次の表に、分類およびマーキングに関して BVI でサポートされる QoS フィールドを示します。

	分類		マーキング	
	入力	出力	入力	出力
Qos-group	yes	yes	yes	yes
廃棄クラス	yes	yes	yes	yes
Prec（DSCP）	yes	yes	yes	yes
vlan	no	no	NA	NA
cos	no	no	no	no
dei	no	no	no	no
src/DST MAC	yes	no	NA	NA
ipv4 L3 フィールド	yes	yes	NA	NA
ipv6 L3 フィールド	yes	yes	NA	NA
QG マーキングによる cos のマーキング/分類	yes inL2/L3 egress	yes in L2/L3 egress	yes in L2/L3 agress	yes in L2/L3 egress

ポリサー粒度とシェーパー粒度

ポリサーの粒度は、入力方向と出力方向で設定できます。 ポリサーの粒度は、ユーザ設定のポリサー レートと、ハードウェアでプログラムされたポリサー レート間の許容パーセンテージ バリエーションとして指定されます。

DEI を使用した輻輳管理

802.1ad フレームと 802.1ah フレームに含まれる Drop Eligible Indicator（DEI）ビットに基づいて輻輳を管理できます。 DEI 値に基づくランダム早期検出は、次における 802.1ad パケットでサポートされます。

- レイヤ 2 サブインターフェイス
- レイヤ 2 メイン インターフェイス
- レイヤ 3 メイン インターフェイス
- 入力および出力

（注） ポリシーにマーキングアクションがある場合、マーキングされた値は、WRED の実行に使用されます。

QoS 輻輳管理の設定方法

ここでは、次のタスクについて説明します。

保証帯域幅および残存帯域幅の設定

bandwidth コマンドでは、トラフィックの特定のクラスに対して割り当てる最小保証帯域幅を指定できます。 MDRR は、スケジューリング アルゴリズムとして実装されます。

bandwidth remaining コマンドでは、MDRR に対するクラスの重みを指定します。 MDRR アルゴリズムは、クラスに割り当てられた残存帯域幅の値から各クラスの重みを取得します。 すべてのクラスに対して **bandwidth remaining** コマンドを設定しない場合、残りの帯域幅は、**bandwidth remaining** が明示的に指定されていないすべてのクラスに均等に割り当てられます。

キューの保証サービス レートは、すべてのキューが輻輳状態である場合にキューが受信する帯域幅として定義されます。 このオブジェクトは次のように定義されています。

保証サービス レート = 最小帯域幅 + キューの超過分

制約事項

設定する帯域幅の量は、レイヤ 2 オーバーヘッドにも対応できるサイズにする必要があります。

bandwidth コマンドは、発信インターフェイスで設定されたポリシーに対してのみサポートされます。

手順の概要

1.
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **bandwidth** {*rate* [*units*]| **percent** *value*}
5. **bandwidth remaining percent** *value*
6. **exit**
7. **class** *class-name*
8. **bandwidth** {*rate* [*units*] | **percent** *value*}
9. **bandwidth remaining percent** *value*
10. **exit**
11. **exit**
12. **interface** *type interface-path-id*
13. **service-policy** {**input** | **output**} *policy-map*
14. **end** または **commit**
15. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	例： `RP/0//CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0//CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RP0/CPU0:router(config-pmap)# class class1`	ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**bandwidth** {*rate* [*units*]| **percent** *value*} 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth percent 50`	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。 • 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
		• この例では、クラス class1 においてインターフェイス帯域幅の 50 % が保証されます。
ステップ 5	**bandwidth remaining percent** *value* 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth remaining percent 20`	残った帯域幅をさまざまなクラスに割り当てる方法を指定します。 • 残っている 40 % の帯域幅は、class1 と class2 クラスに 20:80 の比率で配分され（ステップ 8 と 9 を参照）、class1 クラスは 40 % のうちの 20 % を受け取り、class2 クラスは 40 % のうちの 80 % を受け取ります。
ステップ 6	**exit** 例： `RP/0//CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 7	**class** *class-name* 例： `RP/0//CPU0:router(config-pmap)# class class2`	ポリシーを作成または変更する、別のクラスの名前を指定します。
ステップ 8	**bandwidth** {*rate* [*units*] | **percent** *value*} 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth percent 10`	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。 • この例では、クラス class2 においてインターフェイス帯域幅の 10 % が保証されます。
ステップ 9	**bandwidth remaining percent** *value* 例： `RP/0//CPU0:router(config-pmap-c)# bandwidth remaining percent 80`	残った帯域幅をさまざまなクラスに割り当てる方法を指定します。 • 残っている 40 % の帯域幅は、class1 と class2 クラスに 20:80 の比率で配分され（ステップ 4 と 5 を参照）、class1 クラスは 40 % のうちの 20 % を受け取り、class2 クラスは 40 % のうちの 80 % を受け取ります。
ステップ 10	**exit** 例： `RP/0//CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 11	**exit** 例： `RP/0//CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 12	**interface** *type interface-path-id* 例： `RP/0//CPU0:router(config)# interface POS 0/2/0/0`	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、インターフェイスを設定します。
ステップ 13	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0//CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシー マップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 14	**end** または **commit**
	
	例：
	
	`RP/0//CPU0:router(config-if)# end`
	または
	
	`RP/0//CPU0:router(config-if)# commit`
		設定変更を保存します。
		
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 15	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0//CPU0:router# show policy-map interface POS 0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

保証帯域幅の設定

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **bandwidth** {*rate* [*units*]| **percent** *percentage-value*}
5. **exit**
6. **class** *class-name*
7. **bandwidth** {*rate* [*units*]| **percent** *percentage-value*}
8. **exit**
9. **class** *class-name*
10. **bandwidth** {*rate* [*units*]| **percent** *percentage-value*}
11. **exit**
12. **exit**
13. **interface** *type interface-path-id*
14. **service-policy** {**input** | **output**} *policy-map*
15. **end** または **commit**
16. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**bandwidth** {*rate* [*units*]| **percent** *percentage-value*} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth percent 40`	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。 • 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。 • この例では、クラス class1 においてインターフェイス帯域幅の 40% が保証されます。
ステップ 5	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 6	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class2`	ポリシーを作成または変更するクラスの名前を指定します。
ステップ 7	**bandwidth** {*rate* [*units*]| **percent** *percentage-value*} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth percent 40`	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。 • 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。 • この例では、クラス class2 においてインターフェイス帯域幅の 40% が保証されます。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 9	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class-default`	ポリシーを作成または変更するクラスの名前を指定します。
ステップ 10	**bandwidth** {*rate* [*units*]| **percent** *percentage-value*} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth percent 20`	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。 • 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。 • この例では、クラス class-default においてインターフェイス帯域幅の 20% が保証されます。
ステップ 11	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 12	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 13	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0`	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、インターフェイスを設定します。
ステップ 14	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービスポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシーマップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

	コマンドまたはアクション	目的

ステップ 15	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	
	または
	
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 16	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0/RSP0/CPU0:router# show policy-map interface gigabitethernet 0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

残存帯域幅の設定

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **bandwidth remaining percent** *percentage-value*
5. **exit**
6. **class** *class-name*
7. **bandwidth remaining percent** *percentage-value*
8. **exit**
9. **class** *class-name*
10. **bandwidth remaining percent** *percentage-value*
11. **exit**
12. **exit**
13. **interface** *type interface-path-id*
14. **service-policy** {**input** | **output**} *policy-map*
15. **end** または **commit**
16. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	ポリシーを作成または変更するクラスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 4	**bandwidth remaining percent** *percentage-value* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 40`	クラス class1 に対する残りの帯域幅の割り当て方法を指定します。
ステップ 5	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 6	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class2`	ポリシーを作成または変更するクラスの名前を指定します。
ステップ 7	**bandwidth remaining percent** *percentage-value* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 40`	クラス class2 に対する残りの帯域幅の割り当て方法を指定します。
ステップ 8	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 9	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class-default`	ポリシーを作成または変更するクラスの名前を指定します。
ステップ 10	**bandwidth remaining percent** *percentage-value* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 20`	クラス class-default に対する残りの帯域幅の割り当て方法を指定します。

	コマンドまたはアクション	目的
ステップ 11	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 12	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 13	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0`	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、インターフェイスを設定します。
ステップ 14	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシーマップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 15	**end** または **commit**
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーションセッションで継続されます。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。

	コマンドまたはアクション	目的
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。
ステップ 16	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0/RSP0/CPU0:router# show policy-map interface gigabitethernet 0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

低遅延キューイングとストリクト プライオリティ キューイングの設定

priority コマンドは、低遅延キューイング（LLQ）を設定し、ストリクトプライオリティキューイングを提供します。ストリクトPQでは、音声などの遅延に影響されやすいデータを、他のキューのパケットをキューから取り出す前にキューから取り出して送信できます。**priority** コマンドを使用してクラスがハイプライオリティとしてマーキングされたとき、ポリサーがプライオリティトラフィックを制限するように設定することを推奨します。この設定は、プライオリティトラフィックがラインカード上のその他すべてのトラフィックをスタベーション状態にしないことを保証するため、低プライオリティ トラフィックは、スタベーション状態から保護されます。 **police** コマンドを使用して、ポリサーを明示的に設定します。

（注） 2 つのレベルのプライオリティ（プライオリティ レベル 1 およびプライオリティ レベル 2）がサポートされます。 プライオリティ レベルが設定されていない場合、デフォルトはプライオリティ レベル 1 になります。

制約事項

- ポリシーマップで、1 つまたは複数のクラスにプライオリティ ステータスを指定できます。1 つのポリシーマップに複数のクラスがプライオリティ クラスとして設定されている場合、これらのクラスからのトラフィックはすべて、同じ単一の完全プライオリティ キューにキューイングされます。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **police rate** {*value* [*units*] | **percent** *percentage*} [**burst** *burst-size* [*burst-units*]] [**peak-burst** *peak-burst* [*burst-units*]] [**peak-rate** *value* [*units*]]
5. **exceed-action** *action*
6. priority [**level** *priority-level*] RP/0/RSP0/CPU0:router(config-pmap-c)# priority
7. **exit**
8. **exit**
9. **interface** *type interface-path-id*
10. **service-policy** {**input** | **output**} *policy-map*
11. **end** または **commit**
12. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map voice`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class voice`	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。 • ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**police rate** {*value* [*units*]	**percent** *percentage*} [**burst** *burst-size* [*burst-units*]] [**peak-burst** *peak-burst* [*burst-units*]] [**peak-rate** *value* [*units*]]	トラフィック ポリシングを設定し、ポリシー マップ 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。 • この例では、低遅延キューイングを 250 Kbps に制限して低プライオリティ トラフィックをスタベーション状態から保護し、帯域幅を解放します。

	コマンドまたはアクション	目的
	例： `RP/0/RSP0/CPU0:router(config-pmap-c)# police rate 250`	

ステップ 5	**exceed-action** *action*
	例：
	`RP/0/RSP0/CPU0:router(config-pmap-c-police)# exceed-action drop`
	例：
	`RP/0//CPU0:router(config-pmap-c)# priority`
	例：
	`RP/0/RSP0/CPU0:router(config-pmap-c-police)# exit`
		レート制限を超過したパケットに対して実行するアクションを設定します。
		ポリシーマップに属するトラフィックのクラスにプライオリティを指定します。
		exit
		ルータをポリシー マップ クラス コンフィギュレーション モードに戻します。

ステップ 6	priority [**level** *priority-level*] RP/0/RSP0/CPU0:router(config-pmap-c)# priority	ポリシーマップに属するトラフィックのクラスにプライオリティを指定します。 （注） • プライオリティ レベルが設定されていない場合、デフォルトはプライオリティ 1 になります。
ステップ 7	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 8	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 9	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0`	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、インターフェイスを設定します。
ステップ 10	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシー マップを付加します。

	コマンドまたはアクション	目的
		• この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 11	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーションセッションが終了して、ルータがEXECモードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 12	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0/RSP0/CPU0:router# show policy-map interface gigabitethernet 0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

トラフィック シェーピングの設定

トラフィック シェーピングでは、インターフェイスから出力されるトラフィックを制御して、リモート ターゲット インターフェイスの速度に合わせてトラフィック フローを伝送することにより、指定されているポリシーにトラフィックを適合させることができます。

着信インターフェイスおよび発信インターフェイス上で実行されるシェーピングは、レイヤ 2 レベルで実行され、レート計算にレイヤ 2 ヘッダーが含まれます。

制約事項

bandwidth コマンド、**priority** コマンド、および **shape average** コマンドは、同じクラス内で同時に設定しないでください。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **shape average** {**percent** *value* | *rate* [*units*]}
5. **exit**
6. **exit**
7. **interface** *type interface-path-id*
8. **service-policy** {**input** | **output**} *policy-map*
9. **end** または **commit**
10. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 4	**shape average** {**percent** *value* | *rate* [*units*]} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# shape average percent 50`	指定した単位の平均レート シェーピングに従って、または帯域幅のパーセンテージとして、表示されたビット レートにトラフィックをシェーピングします。
ステップ 5	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシーマップ コンフィギュレーション モードに戻します。
ステップ 6	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 7	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/0`	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、インターフェイスを設定します。
ステップ 8	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシー マップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 9	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	
	または
	
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレー

	コマンドまたはアクション	目的
		ション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。
ステップ 10	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0/RSP0/CPU0:router# show policy-map interface gigabitethernet 0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

トラフィック ポリシングの設定（2 レート カラーブラインド）

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されるトラフィックの最大レートを制御できます。 ここでは、2 レート カラーブラインド トラフィック ポリシングを設定する手順について説明します。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **police rate** {*value* [*units*] | **percent** *percentage*} [**burst** *burst-size* [burst-*units*]] [**peak-burst** *peak-burst* [burst-*units*]] [**peak-rate** *value* [*units*]]
5. **conform-action** *action*
6. **exceed-action** *action*
7. **exit**
8. **exit**
9. **exit**
10. **interface** *type interface-path-id*
11. **service-policy** {**input** | **output**} *policy-map*
12. **end** または **commit**
13. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**police rate** {*value* [*units*] | **percent** *percentage*} [**burst** *burst-size* [burst-*units*]] [**peak-burst** *peak-burst* [burst-*units*]] [**peak-rate** *value* [*units*]] 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# police rate 250000`	トラフィック ポリシングを設定し、ポリシー マップ 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。トラフィック ポリシング機能は、トークン バケット アルゴリズムで動作します。
ステップ 5	**conform-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# conform-action set mpls experimental topmost 3`	レート制限に適合したパケットに対して実行するアクションを設定します。*action* 引数は、次のいずれかのキーワードにより指定します。 • **drop**：パケットをドロップします。 • **set**：次のキーワードおよび引数を使用します。 **discard-class** *value*：廃棄クラスの値を設定します。指定できる範囲は、0 ～ 7 です。 **dscp** ：DiffServ コード ポイント（DSCP）値を設定し、パケットを送信します。 **mpls experimental** {**topmost** | **imposition**} *value*：マルチプロトコル ラベル スイッチング（MPLS）パケットの最上位ラベルまたは付加ラベルの experimental（EXP）値を設定します。 指定できる範囲は、0 ～ 7 です。

	コマンドまたはアクション	目的
		precedence ：IP precedence を設定し、パケットを送信します。 **qos-group**：QoS グループ値を設定します。 指定できる範囲は、0 ～ 63 です。 • **transmit**：パケットを送信します。
ステップ 6	**exceed-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# exceed-action set mpls experimental topmost 4`	レート制限を超過したパケットに対して実行するアクションを設定します。 *action* 引数は、ステップ 5 で指定したいずれかのキーワードにより指定します。
ステップ 7	**exit** 例： RP/0/RSP0/CPU0:router(config-pmap-c-police)# exit	ルータをポリシー マップ クラス コンフィギュレーション モードに戻します。
ステップ 8	**exit** 例： RP/0/RSP0/CPU0:router(config-pmap-c)# exit	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 9	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 10	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/5/0/0`	コンフィギュレーション モードを開始し、インターフェイスを設定します。
ステップ 11	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシー マップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。
ステップ 12	**end** または **commit**	設定変更を保存します。

	コマンドまたはアクション	目的

	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーションセッションが終了して、ルータがEXECモードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

ステップ 13	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0/RSP0/CPU0:router# show policy-map interface gigabitethernet 0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

トラフィック ポリシングの設定（2R3C）

ここでは、2 レート 3 カラー トラフィック ポリシングを設定する手順について説明します。 これは、入力側の SIP 700 ラインカードにのみ適用されます。

手順の概要

1. **configure**
2. **class-map** [**match-all**][**match-any**] *class-map-name*
3. **match [not] fr-de** *fr-de-bit-value*
4. **policy-map** *policy-name*
5. **class** *class-name*
6. **police rate** {*value* [*units*] | **percent** *percentage*} [**burst** *burst-size* [burst-*units*]] [**peak-burst** *peak-burst* [burst-*units*]] [**peak-rate** *value* [*units*]]
7. **conform-color** *class-map-name*
8. **exceed-color** *class-map-name*
9. **conform-action** *action*
10. **exceed-action** *action*
11. **exit**
12. **exit**
13. **exit**
14. **interface** *type interface-path-id*
15. **service-policy** *policy-map*
16. **end** または **commit**
17. **show policy-map interface** *type interface-path-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**class-map** [**match-all**][**match-any**] *class-map-name* 例： `RP/0/RSP0/CPU0:router(config)# class-map match-all match-not-frde`	（SIP 700 ラインカード、入力のみで使用） 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。 • 1 つ以上のインターフェイスに付加できるクラス マップを作成または修正し、一致するポリシーを指定します。
ステップ 3	**match [not] fr-de** *fr-de-bit-value* 例： `RP/0/RSP0/CPU0:router(config)# match not fr-de 1`	（SIP 700 ラインカード、入力のみで使用） 一致条件を指定します。 • 通常、適合カラー パケットの指定には match *not* fr-de 1 を使用します。

	コマンドまたはアクション	目的
		• 通常、超過カラー パケットの指定には match fr-de 1 を使用します。
ステップ 4	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 5	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。
ステップ 6	**police rate** {*value* [*units*] | **percent** *percentage*} [**burst** *burst-size* [burst-*units*]] [**peak-burst** *peak-burst* [burst-*units*]] [**peak-rate** *value* [*units*]] 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# police rate 768000 burst 288000 peak-rate 1536000 peak-burst 576000`	トラフィック ポリシングを設定し、ポリシー マップ 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。トラフィック ポリシング機能は、トークン バケット アルゴリズムで動作します。
ステップ 7	**conform-color** *class-map-name* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# conform-color match-not-frde`	（SIP 700 ラインカード、入力のみで使用） 適合カラー パケットに割り当てるクラスマップ名を設定します。
ステップ 8	**exceed-color** *class-map-name* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# exceed-color match-frde`	（SIP 700 ラインカード、入力のみで使用） 超過カラー パケットに割り当てるクラスマップ名を設定します。
ステップ 9	**conform-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# conform-action set mpls experimental topmost 3`	レート制限に適合したパケットに対して実行するアクションを設定します。 *action* 引数は、次のいずれかのキーワードにより指定します。 • **drop**：パケットをドロップします。 • **set**：次のキーワードおよび引数を使用します。 **discard-class** *value*：廃棄クラスの値を設定します。指定できる範囲は、0 ～ 7 です。

	コマンドまたはアクション	目的
		dscp *value*：DiffServ コードポイント（DSCP）の値を設定し、パケットを送信します。 **mpls experimental** {**topmost** | **imposition**} *value*：マルチプロトコル ラベル スイッチング（MPLS）パケットの最上位ラベルまたは付加ラベルの experimental（EXP）値を設定します。 指定できる範囲は、0 ～ 7 です。 **precedence** *precedence*：IP precedence を設定し、パケットを送信します。 **qos-group**：QoS グループ値を設定します。 指定できる範囲は、0 ～ 63 です。 • **transmit**：パケットを送信します。
ステップ 10	**exceed-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# exceed-action set mpls experimental topmost 4`	レート制限を超過したパケットに対して実行するアクションを設定します。 *action* 引数は、ステップ 5 で指定したいずれかのキーワードにより指定します。
ステップ 11	**exit** 例： RP/0/RSP0/CPU0:router(config-pmap-c-police)# exit	ルータをポリシー マップ クラス コンフィギュレーション モードに戻します。
ステップ 12	**exit** 例： RP/0/RSP0/CPU0:router(config-pmap-c)# exit	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 13	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 14	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface pos 0/5/0/0`	コンフィギュレーションモードを開始し、インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 15	**service-policy** *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy policy1`	インターフェイスのサービス ポリシーとして使用するポリシーマップを入力インターフェイスに付加します。

ステップ 16	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 17	**show policy-map interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router# show policy-map interface POS0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

階層型ポリシングの設定

階層型ポリシングは、次の 2 つのレベルでのサポートを提供します。

- 親レベル
- 子レベル

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **service-policy** *policy-map-name*
5. **police rate percent** *percentage*
6. **conform-action** *action*
7. **exceed-action** *action*
8. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**service-policy** *policy-map-name* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# service-policy child`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシー マップを付加します。
ステップ 5	**police rate percent** *percentage* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# police rate percent 50`	トラフィック ポリシングを設定し、ポリシー マップ 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。

	コマンドまたはアクション	目的
ステップ 6	**conform-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# conform-action transmit`	レート制限に適合したパケットに対して実行するアクションを設定します。 可能なアクションは次のとおりです。 **transmit**：パケットを送信します。
ステップ 7	**exceed-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# exceed-action drop`	レート制限を超過したパケットに対して実行するアクションを設定します。 可能なアクションは次のとおりです。 **drop**：パケットをドロップします。

ステップ 8	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

BVI に対するトラフィック ポリシング

トラフィック ポリシーの設定は、BVI に関して、情報レート、リンク帯域幅のパーセンテージ、およびパケットに対して実行されるアクション（適合/違反/超過）を定義します。 BVI の設定済みポリサー レートは NP 単位で有効です。 1 つの NP に 2 つのインターフェイスがある場合、これら 2 つのインターフェイスからの BVI トラフィックは 1 つのポリサー下になります。 他のイン

ターフェイスからの、または他の NP でのトラフィックは、ポリサーの影響を受けません。 **show controller np ports** コマンドを使用して、特定の NP のインターフェイスがあるか確認できます。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **police rate** {*value* [*units*] | **percent** *percentage*} [**burst** *burst-size* [burst-*units*]] [**peak-burst** *peak-burst* [burst-*units*]] [**peak-rate** *value* [*units*]]
5. **conform-action** *action*
6. **exceed-action** *action*
7. **violate-action** *action*
8. **exit**
9. **exit**
10. **exit**
11. **interface** *type interface-path-id*
12. **service-policy** {**input** | **output**} *policy-map*
13. **end** または **commit**
14. **show policy-map interface** *type interface-path-id* [**input** | **output**]*interface-path-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 4	**police rate** {*value* [*units*] | **percent** *percentage*} [**burst** *burst-size* [burst-*units*]] [**peak-burst** *peak-burst* [burst-*units*]] [**peak-rate** *value* [*units*]] 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# police rate 250000`	トラフィック ポリシングを設定し、ポリシー マップ 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。トラフィック ポリシング機能は、トークン バケット アルゴリズムで動作します。 （注） **police rate** は通常、フラット ポリシー マップにより適しています。親/子ポリシー マップに **police percent** コマンドを使用できます。
ステップ 5	**conform-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# conform-action set prec 1`	レート制限に適合したパケットに対して実行するアクションを設定します。*action* 引数は、次のいずれかのキーワードにより指定します。 • **drop**：パケットをドロップします。 • **set**：次のキーワードおよび引数を使用します。 **discard-class** *value*：廃棄クラスの値を設定します。指定できる範囲は、0 ～ 7 です。 **dscp** ：DiffServ コード ポイント（DSCP）値を設定し、パケットを送信します。 **precedence** ：IP precedence を設定し、パケットを送信します。 **qos-group**：QoS グループ値を設定します。 指定できる範囲は、0 ～ 63 です。 • **transmit**：パケットを送信します。
ステップ 6	**exceed-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# exceed-action drop`	レート制限を超過したパケットに対して実行するアクションを設定します。 *action* 引数は、ステップ 5 で指定したいずれかのキーワードにより指定します。
ステップ 7	**violate-action** *action* 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# violate-action drop`	レート制限を超過したパケットに対して実行するアクションを設定します。 *action* 引数は、ステップ 5 で指定したいずれかのキーワードにより指定します。
ステップ 8	**exit** 例： RP/0/RSP0/CPU0:router(config-pmap-c-police)# exit	ルータをポリシー マップ クラス コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： RP/0/RSP0/CPU0:router(config-pmap-c)# exit	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 10	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 11	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface BVI 10`	QoS ポリシーが付加される BVI を指定します。
ステップ 12	**service-policy** {**input** | **output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力 BVI または出力 BVI にポリシーマップを付加します。 （注） BVI のポリサーは、ネットワーク プロセッサごとに集約されます。 同じ NP の 2 つのインターフェイスの 500M ポリサーでは、NP ごとのポリシング レートが合計で 500M に低下します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 13	**end** または **commit**
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-if)# end`
	または
	
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィ

	コマンドまたはアクション	目的
		ギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。
ステップ 14	**show policy-map interface** *type interface-path-id* [**input** | **output**]*interface-path-id* 例： `RP/0/RSP0/CPU0:router# sh policy-map int BVI 1 input member gig 0/1/0/29`	（任意）指定したインターフェイス（gig 0/1/0/29）が属する NP 上のすべてのサービス ポリシーに対して設定されているすべてのクラスのポリシー設定情報を表示します。

ECN の設定

ECNは、ルータとエンドホストが、ネットワークが輻輳状態であり、パケットの送信速度が低下しているのを認識できるようにします。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **bandwidth** [*percent* |*value*]
5. **random-detect** { **default** | **discard-class** | **dscp** | **precedence** }
6. **random-detect ecn**
7. **exit**
8. **exit**
9. **end** または **commit**
10. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	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。 • ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**bandwidth** [*percent* | *value*] 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth 100`	特定のポリシー マップのクラスに割り当てる帯域幅を指定または変更します。 （注） ECNは、帯域幅、シェーピングなど、特定のキューイング アクションで設定できます。
ステップ 5	**random-detect** { **default** | **discard-class** | **dscp** | **precedence** } 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# random-detect dscp 1 1000 packets 2000 packets`	WRED プロファイルを設定します。 WRED プロファイル エントリは、特定クラスの ECN に適用する必要があります。
ステップ 6	**random-detect ecn** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# random-detect ecn`	ECN をイネーブルにします。
ステップ 7	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。

ステップ 9	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	
	または
	
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 10	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0/RSP0/CPU0:router# show policy-map interface gigabitethernet 0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスの統計情報を表示します。 ECNがイネーブルであると、指定のインターフェイスに ECN マーキング情報が表示されます。

輻輳管理の設定例

輻輳管理対象の例を、次にいくつか示します。

入力インターフェイスのトラフィック シェーピング：例

次に、入力インターフェイス上でポリシー マップを設定する例を示します。

```
policy-map p2
 class voip
 shape average 20 mbps

!
interface GigabitEthernet0/4/0/24
 service-policy input p2
 commit
RP/0/RSP0/CPU0:Jun 8 16:55:11.819 : config[65546]: %MGBL-LIBTARCFG-6-COMMIT : Configuration
 committed by user 'cisco'. Use 'show configuration commit changes 1000006140' to view the
 changes.
```

次に、上記のポリシー マップ設定の表示出力の例を示します。

```
RP/0/RSP0/CPU0:router# show policy-map interface GigabitEthernet 0/4/0/24 input

GigabitEthernet0/4/0/24 input: p2
  Class voip
    Classification statistics                      (packets/bytes)      (rate - kbps)
            Matched       :                              0/0                    0
            Transmitted   :                              0/0                    0
            Total Dropped :                              0/0                    0
Queueing statistics
            Queue ID                                  : 268435978
            High watermark  (Unknown)
            Inst-queue-len  (packets)                 : 0
            Avg-queue-len   (Unknown)
            Taildropped(packets/bytes)                : 0/0
            Queue(confirm)       :                      0/0
            Queue(exceed)        :                      0/0
            RED random drops(packets/bytes)           : 0/0

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

バンドル インターフェイスのトラフィック ポリシング：例

次に、バンドル インターフェイスのポリシー マップを設定する例を示します。

```
policy-map p2
 class voip
 police rate percent 20
 commit
RP/0/RSP0/CPU0:Jun  8 16:51:51.679 : config[65546]: %MGBL-LIBTARCFG-6-COMMIT : Configuration
 committed by user 'cisco'.   Use 'show configuration commit changes 1000006135' to view
the changes.
 exit
exit
interface bundle-ether 1
 service-policy input p2
 commit
RP/0/RSP0/CPU0:Jun  8 16:52:02.650 : config[65546]: %MGBL-LIBTARCFG-6-COMMIT : Configuration
 committed by user 'cisco'.   Use 'show configuration commit changes 1000006136' to view
the changes.
```

次に、ポリシングがパーセンテージで設定されたポリシー マップ設定の表示出力の例を示します。

```
RP/0/RSP0/CPU0:router# show policy-map interface bundle-ether 1

Bundle-ether1 input: p2
  Class voip
    Classification statistics                      (packets/bytes)      (rate - kbps)
            Matched                               : 0/0      0
    Policing statistics                            (packets/bytes)      (rate - kbps)
            Policed(conform)                      : 0/0   0
            Policed(exceed)                       : 0/0   0
            Policed(violate)                      : 0/0   0
            Policed and dropped                   : 0/0
  Class default
    Classification statistics                      (packets/bytes)      (rate - kbps)
            Matched                               : 0/0      0
            Transmitted                           : 0/0      0
            Total Dropped                         : 0/0      0
    Queueing statistics
            Vital           (packets)             : 0
    Queueing statistics
            Queue ID                              : 36
            High watermark  (packets)             : 0
            Inst-queue-len  (bytes)               : 0
            Avg-queue-len   (bytes)               : 0
            TailDrop Threshold(bytes)             : 239616000
            Taildropped(packets/bytes)            : 0/0
```

2R3C トラフィック ポリシング：例

これらのコマンドは、カラーアウェア ポリシーを作成します。

```
!
class-map match-any match-frde-0
 match not fr-de 1
 end-class-map
!
class-map match-any match-frde-1
 match fr-de 1
 end-class-map
!

!
policy-map color-aware-policer
 class class-default
  police rate 1000 kbps peak-rate 2000 kbps
   conform-color match-frde-0
   exceed-color match-frde-1
  conform-action set qos-group 10
  exceed-action set qos-group 20
  violate-action drop
  !
 !
 end-policy-map
!

!
interface POS0/1/0/0
 encapsulation frame-relay
 pos
  crc 32
 !
 frame-relay lmi disable
!
interface POS0/1/0/0.1 l2transport
 pvc 100
```

```
  service-policy input color-aware-policer
 !
!
```

このコマンドは、ポリシーの現在のコンフィギュレーション コマンドを表示します。

```
RP/0/RSP0/CPU0:router# show run policy-map color-aware-policer
Thu Apr 14 09:25:04.752 UTC
policy-map color-aware-policer
 class class-default
  police rate 1000 kbps peak-rate 2000 kbps
   conform-color match-frde-0
   exceed-color match-frde-1
  conform-action set qos-group 10
  exceed-action set qos-group 20
  violate-action drop
  !
 !
 end-policy-map
!
```

このコマンドは、カラーアウェア ポリシーを表示します。

```
/0/RSP0/CPU0:router# show policy-map interface pos 0/1/0/0.1 input
Thu Apr 14 09:24:10.487 UTC

POS0/1/0/0.1 input: color-aware-policer

Class class-default
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            66144900/8201967600           498245
    Transmitted         : N/A
    Total Dropped       :            65879175/8169017700           496245
  Policing statistics                (packets/bytes)     (rate - kbps)
    Policed(conform)    :              132863/16475012             1000
    Policed(exceed)     :              132863/16475012             1000
    Policed(violate)    :            65879175/8169017700           496245
    Policed and dropped :            65879175/8169017700
  Conform Color
    Policed(conform)    :              132863/16475012             1000
    Policed(exceed)     :               51367/6369508              389
    Policed(violate)    :            46186826/5727166424           347907
  Exceed Color
    Policed(exceed)     :               81496/10105504             611
    Policed(violate)    :            19692349/2441851276           148338
  Violate Color
    Policed(violate)    :                   0/0                    0
```

BVI に対するトラフィック ポリシング：例

次に、BVI に対するトラフィック ポリシングを設定する例を示します。

```
policy-map p1
 class c1
   police rate 10
    conform-action set prec 1
    exceed-action drop
   exit
  exit
exit
interface BVI 10
 service-policy output p1
```

L2VPN（サブ インターフェイス）の設定例：

```
interface TE0/2/1/2.1 l2transport
  encapsulation dot1q50
  rewrite ingress tag pop1 symmetric (for dot1q sub)
l2vpn
 bridge group BVI
```

```
 bridge-domain BVI
  interface TE0/2/1/2.1
  !
  routed interface BVI1
 !
!
```

ECN：例

次の例では、**random-detect ecn** コマンドを実行して ECN を設定する例を示します。

```
config
policy-map p1
class c1
bandwidth 100
random-detect dscp 1 1000 packets 2000 packets
random-detect ecn
exit
exit
commit
```

ATM QoS：例

階層型ポリシング：例

その他の関連資料

ここでは、QoS 輻輳管理の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
初期システム起動と設定	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
マスター コマンド リファレンス	『*Cisco ASR 9000 Series Aggregation Services Router Master Command Listing*』
QoS コマンド	『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』
ユーザ グループとタスク ID	『Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide』の「Configuring AAA Services on Cisco ASR 9000 Series Router」モジュール

標準

標準	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
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

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
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

第 6 章

モジュラ QoS サービス パケットの分類の設定

パケット分類は、データ パス上で輻輳管理または輻輳回避を必要とするトラフィック フローを識別し、マーキングします。 モジュラ Quality of Service（QoS）コマンドライン インターフェイス（MQC）は、分類する必要のあるトラフィック フローを定義するために使用します。このとき、各トラフィック フローをサービス クラス、またはクラスと呼びます。 その後、トラフィック ポリシーを作成し、クラスに適用します。 定義されたクラスに該当しないトラフィックは、すべてデフォルト クラスのカテゴリに分類されます。

このモジュールでは、QoS パケット分類の概念および設定情報について説明します。

ラインカード、SIP および SPA のサポート

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
DEI に基づく分類	yes	no
クラスベースの無条件パケット マーキング	yes	yes
In-Place ポリシーの変更	yes	yes
IPv6 QoS	yes	yes
パケットの分類とマーキング	yes	yes
ポリシーの継承	yes	yes
ポート シェーピング ポリシー	yes	no
共有ポリシー インスタンス	yes	no

Cisco ASR 9000 シリーズ ルータでのモジュラ QoS パケット分類とマーキングの設定に関する機能履歴

リリース	変更内容
リリース 3.7.2	クラスベース無条件パケット マーキング機能が、ASR 9000 イーサネット ラインカードに導入されました。 IPv6 QoS 機能が、ASR 9000 イーサネット ラインカードに導入されました。（IPv6 ACL に対する QoS の照合はサポートされていません）。 パケットの分類とマーキング機能が、ASR 9000 イーサネット ラインカードに導入されました。
リリース 3.9.0	クラスベース無条件パケット マーキング機能が、ASR 9000 用 SIP 700 でサポートされました。 パケットの分類とマーキング機能が、ASR 9000 用 SIP 700 でサポートされました。 ポリシーの継承機能が、ASR 9000 イーサネット ラインカードと ASR 9000 用 SIP 700 に導入されました。 共有ポリシー インスタンス機能が、ASR 9000 イーサネット ラインカードに導入されました。
リリース 4.0.0	DEI 機能に基づく分類機能が、ASR 9000 イーサネット ラインカードに導入されました。 In-Place ポリシーの変更機能は、ASR 9000 イーサネット ラインカードと ASR 9000 用 SIP 700 に導入されました。 IPv6 QoS 機能が、ASR 9000 用 SIP 700 でサポートされました。 同じクラスのポリサーアクションの一部として、スタンドアロン マーキング アクションが 3 つ、マーキング アクションが 3 つ、ASR 9000 用 SIP 700 に追加されました。（ASR 9000 イーサネット ラインカードでは、同じクラスのポリサーアクションの一部として、スタンドアロン マーキング アクションを 2 つ、マーキング アクションを 2 つサポートしています）。
リリース 4.0.1	ポート シェーピング ポリシー機能のサポートが、ASR 9000 イーサネット ラインカードに導入されました。
リリース 4.2.1	衛星機能の QoS が追加されました。

- モジュラ QoS パケット分類の設定の前提条件，121 ページ
- モジュラ QoS パケットの分類の設定に関する情報，121 ページ
- モジュラ QoS のパケット分類の設定方法，139 ページ

- モジュラ QoS パケット分類の設定例，163 ページ
- その他の関連資料，170 ページ

モジュラ QoS パケット分類の設定の前提条件

ネットワークでモジュラ QoS パケット分類とマーキングを設定するには、次の前提条件が必要です。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンス ガイドには、各コマンドに必要なタスク ID が含まれます。 ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- Cisco IOS XR QoS の設定作業と概念に関する知識が必要です。

モジュラ QoS パケットの分類の設定に関する情報

このマニュアルの QoS パケット分類機能を設定するには、次の概念を理解している必要があります。

パケット分類の概要

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

トラフィック ポリサーおよびトラフィック シェーパーは、IP precedence などのパケット分類機能を使用して、さまざまなタイプの QoS サービスに対して、ルータを通過するパケット（またはトラフィック フロー）を選択します。 たとえば、IP パケット ヘッダーのタイプ オブ サービス（ToS）フィールドの 3 つの precedence ビットを使用すると、最大 8 種類のトラフィック クラスで構成される限定的な設定にパケットを分類できます。 パケットを分類した後、他の QoS 機能を使用して、輻輳管理、帯域幅割り当て、および遅延限度などの適切なトラフィック処理ポリシーを、各トラフィック クラスに割り当てることができます。

（注） IPv6 ベースの分類は、レイヤ 3 インターフェイスでのみサポートされています。

トラフィック クラスの要素

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

トラフィック クラスに含まれる 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** コマンドで指定します。 たとえば、**class-map** コマンドで *cisco* を使用すると、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。 デフォルト トラフィック クラスを参照してください。

複数の一致基準をトラフィック クラスに指定する場合は、これらの **match** コマンドを評価する方法の説明を指定する必要があります。 評価の説明は、**class-map match-any** コマンドで指定します。 **match-any** オプションを評価の説明として指定した場合、トラフィック クラスによって評価されるトラフィックは、指定した条件のうち少なくとも 1 つを満たす必要があります。 **match-all** オプションを指定した場合、トラフィックはすべての一致基準を満たす必要があります。

これらのコマンドの機能については、『Cisco ASR 9000 Series Aggregation Services Routers Modular Quality of Service Command Reference』でより詳細に説明します。 トラフィック クラスの設定作業については、トラフィック クラスの作成で説明されています。

トラフィック ポリシーの要素

トラフィック ポリシーの目的は、ユーザが指定したトラフィック クラスまたはクラスに分類されたトラフィックに関連付ける QoS 機能を設定することです。 トラフィック ポリシーを作成するには、**policy-map** コマンドを使用します。 トラフィック ポリシーには、名前、トラフィック クラス（**class** コマンドで指定）、および QoS ポリシーという 3 つの要素が含まれます。 トラフィック ポリシーの名前は、ポリシー マップの Modular Quality of Service（MQC）で指定します（たとえば、**policy-map** *policy1* コマンドによって *policy1* という名前のトラフィック ポリシーを作成できます）。 指定したトラフィック ポリシーにトラフィックを分類するために使用するトラフィック クラスは、クラス マップ コンフィギュレーション モードで定義します。 トラフィック ポリシーにトラフィックを分類に使用するトラフィック クラスを選択した後で、この分類されたトラフィックに適用する QoS 機能を入力できます。

MQC では、必ずしも 1 つのトラフィック クラスだけを 1 つのトラフィック ポリシーに関連付ける必要はありません。 パケットが複数の一致基準に一致する場合、1 つのトラフィック ポリシーに 1024 のトラフィック クラスを関連付けることができます。 1024 のクラス マップには、デフォルト クラスと子ポリシーのクラスが含まれます（存在する場合）。

クラスをポリシー マップで設定する順序が重要です。 クラスの一致規則は、クラスをポリシー マップで指定した順序で TCAM にプログラミングされます。 したがって、あるパケットが複数の

クラスと一致する場合は、最初に一致したクラスだけが返され、対応するポリシーが適用されます。

これらのコマンドの機能については、『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』でより詳細に説明します。

トラフィック クラスの設定作業については、トラフィック ポリシーの作成で説明されています。

デフォルト トラフィック クラス

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

ユーザがデフォルト クラスを設定しない場合でも、パケットはデフォルト クラスのメンバとして扱われます。 ただし、デフォルトでは、デフォルト クラスにイネーブルな機能はありません。そのため、機能が設定されていないデフォルト クラスに属するパケットにはQoS機能は適用されません。 この後、これらのパケットは、ファーストイン ファーストアウト（FIFO）キューに配置され、使用可能な下位リンクの帯域幅で決められたレートで転送されます。 このFIFOキューは、テール ドロップと呼ばれる輻輳回避技術で管理されます。 テール ドロップなどの輻輳回避技術の詳細については、このマニュアルの「Configuring Modular QoS Congestion Avoidance on Cisco ASR 9000 Series Routers」モジュールを参照してください。

バンドル トラフィック ポリシー

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

ポリシーは次のものにバインドできます。

- バンドル
- バンドル レイヤ 3 サブインターフェイス
- バンドル レイヤ 2 サブインターフェイス（レイヤ 2 転送）

入力および出力トラフィックの両方がサポートされています。 パーセントベースのポリシーと絶対レートベースのポリシーがサポートされています。 ただし、使いやすさのため、パーセントベースのポリシーを使用することを推奨します。

共有ポリシー インスタンス

トラフィック クラスとトラフィック ポリシーを作成した後、任意で共有ポリシー インスタンス（SPI）を使用して、QoS リソースを 1 つ割り当て、これをサブインターフェイス、複数のイーサネット フローポイント（EFP）、またはバンドル インターフェイスで共有することができます。

SPI を使用して、QoS ポリシーの 1 つのインスタンスを複数のサブインターフェイスで共有し、サブインターフェイスのシェーピングを 1 つのレートに集約できます。 QoS ポリシーのインスタンスを共有するサブインターフェイスは、すべて同じ物理インターフェイスに属する必要があります。 QoS ポリシーのインスタンスを共有するサブインターフェイスの数は、2 からポートのサブインターフェイスの最大数までです。

バンドル インターフェイスの場合、ハードウェア リソースはバンドル メンバごとに複製されます。 共通の共有ポリシー インスタンスを使用し、Link Aggregation Control Protocol（LAG）バンドルで設定されたサブインターフェイスは、すべて同じメンバ リンクにロードバランシングされる必要があります。

バンドル EFP にポリシーが設定されている場合、バンドルのメンバ リンクごとにポリシーのインスタンスが 1 つ設定されます。 同じバンドルの複数のバンドル EFP 間で SPI を使用する場合、バンドルのメンバ リンクごとにポリシーの共有インスタンスが 1 つ設定されます。 デフォルトでは、バンドルのロード バランシング アルゴリズムでは、ハッシュを使用して（バンドル EFP から送信される必要のある）トラフィックをバンドル メンバ間に分散させます。 1 つまたは複数の EFP のトラフィックを、複数のバンドル メンバ間に分散させることができます。 複数の EFP に、SPI を使用して一緒にシェーピングまたはポリシングを実行しなければならないトラフィックがある場合は、同じ共有ポリシーのインスタンスに属するすべての EFP へのトラフィックに対して、バンドル ロード バランシングで同じバンドル メンバを選択する（ハッシュ選択）ように設定する必要があります。 これによって、同じポリシーの共有インスタンスを持つすべての EFP に向かうトラフィックで、同じポリサー/シェーパー インスタンスが使用されます。

これは通常は同じ加入者が多数の EFP を持つ場合（たとえば、各サービス タイプに対して 1 つの EFP を持つなど）や、プロバイダーですべての加入者の EFP に対してシェーピングおよびキューイングを一緒に実装することが求められる場合に使用されます。

ポリシーの継承

ポリシー マップを物理ポートに適用すると、ポリシーは、その物理ポートのすべてのレイヤ 2 およびレイヤ 3 サブインターフェイスに適用されます。

ポート シェーピング ポリシー

ポート シェーピング ポリシーをメイン インターフェイスに適用するときには、個々の通常のサービス ポリシーをそのサブインターフェイスに適用できます。 ポート シェーピング ポリシー マップには、次の制限事項があります。

- class-default が許可された唯一のクラス マップです。
- シェイプ クラス アクションが許可された唯一のクラス アクションです。
- これらは出力方向でだけ設定できます。
- これらのスクリプトは、メイン インターフェイスにのみ適用します。サブインターフェイスには適用できません。

- 2 レベルまたは 3 レベルのポリシーはサポートされていません。 1 レベルまたはフラットなポリシーだけがサポートされています。

上記の制限のいずれかに違反した場合、設定したポリシーマップはポートシェーピング ポリシーではなく、通常のポリシーとして適用されます。

クラスベース無条件パケット マーキングの機能と利点

クラスベースの無条件パケット マーキング機能は、ユーザが指定したマーキングに基づいてパケットを区別できる効率的なパケット マーキング機能です。

クラスベースの無条件パケット マーキングでは、次の作業を行うことができます。

- IP precedence ビットまたは IP DiffServ コード ポイント（DSCP）を IP ToS バイトに設定してパケットをマーキング。
- インポーズされたラベルまたは最上位ラベル内の EXP ビットを設定して、マルチプロトコル ラベル スイッチング（MPLS）パケットをマーキング。
- レイヤ 2 サービス クラス（CoS）値を設定して、パケットをマーキング。
- IEEE 802.1Q トンネリング（QinQ）設定に内部および外部 CoS タグを設定してパケットをマーキング。
- *qos-group* 引数の値を設定してパケットをマーキング。
- *discard-class* 引数の値を設定してパケットをマーキング。

（注） *qos-group* および *discard-class* はルータの内部変数であり、送信されません。

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

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

  たとえば、輻輳回避技術である重み付けランダム早期検出（WRED）を使用すると、パケットがドロップされる確率を判断できます。 さらに、低遅延キューイング（LLQ）を設定して、そのマークのすべてのパケットをプライオリティ キューに送るよう設定できます。

- QoS 無条件パケット マーキングを使用して、パケットを QoS グループに割り当てます。 QoS グループ ID を MPLS パケットに設定するには、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 **set qos-group** コマンドを使用します。

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

- CoS 無条件パケット マーキングを使用して、IEEE 802.1p/ スイッチ間リンク（ISL）パケットのプライオリティ値を設定するパケットを割り当てます。 スイッチ間リンク（ISL）パケット。 ルータでは、CoS 値を使用して、パケットに転送のための優先順位を付ける方法を決定し、このマーキングを使用してレイヤ 2 からレイヤ 3 へのマッピングを行います。 送信パケットのレイヤ 2 CoS 値を設定するには、ポリシー マップ コンフィギュレーション モードで **set cos** コマンドを使用します。

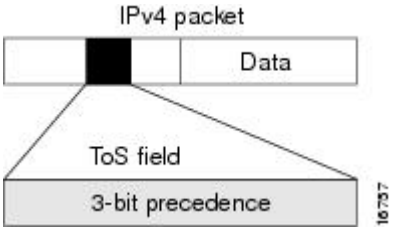
設定作業については、クラスベース無条件パケット マーキングの設定で説明されています。

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

IP precedence によるパケットの CoS の指定

IP precedence を使用すると、パケットの CoS を指定できます。 この目的には、IP Version 4（IPv4）ヘッダーの ToS フィールドの 3 つの precedence ビットを使用します。 図 1 に、ToS フィールドを示します。

図 7：***IPv4*** **パケットのタイプ オブ サービス フィールド**



ToS ビットを使用して、最大 8 つのサービス クラスを定義できます。 その後、ネットワーク全体で設定された他の機能によって、これらのビットを使用して、ToS の付与に関するパケットの処理方法を決定します。 これらの他の QoS 機能では、輻輳管理戦略や帯域幅の割り当てなど適切なトラフィック処理ポリシーを割り当てることができます。 たとえば、などのパケットの IP 優先順位設定を使用してトラフィックのプライオリティを設定できます。

着信トラフィックに precedence レベルを設定し、Cisco IOS XR QoS キューイング機能と一緒に使用することで、ディファレンシエーテッド サービスを作成できます。

後続の各ネットワーク要素が決定されたポリシーに基づいてサービスを提供できるように、できるだけ IP precedence は、通常ネットワークの端または管理ドメインの近くに配置します。 これによって、他のコアまたはバックボーンにおいて、優先順位に基づいて QoS を設定できます。

設定作業については、クラスベース無条件パケット マーキングの設定で説明されています。

パケットの分類に使用する IP precedence ビット

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

歴史的な理由から、各優先度はある名前に対応します。 これらの名前は RFC 791 で定義されています。 表 5 に、重要度のより小さいものから大きいものへの順序で、番号とそれに対応する名前を表示します。

表 *2*：*IP precedence* 値

番号	名前
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

（注） IP precedence ビットの設定 6 と 7 は、ルーティング アップデートなどのネットワーク制御情報用に予約されています。

IP precedence 値の設定

デフォルトでは、Cisco IOS XR ソフトウェアは、IP precedence 値をそのまま残します。 これによって、ヘッダーの precedence 値セットが維持され、すべての内部ネットワーク デバイスが IP precedence

の設定に基づいてサービスを提供できるようになります。 このポリシーは、ネットワークのエッジでネットワーク トラフィックをさまざまなタイプのサービスにソートすること、またこれらのサービス タイプをネットワーク コアで設定することを指定する標準的な方法に従っています。その後、ネットワークのコアにあるルータは、precedence ビットを使用して、送信順やパケットドロップの可能性などを決定できるようになります。

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

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

DEI に基づく分類

802.1ad フレームと 802.1ah フレームに含まれる Drop Eligible Indicator（DEI）ビットに基づいて、トラフィックを分類できます。 デフォルトの DEI マーキングがサポートされています。 ポリシーマップの set dei アクションは、802.1ad パケットで次の項目に対してサポートされています。

- 入力および出力
- レイヤ 2 サブインターフェイス
- レイヤ 2 メイン インターフェイス
- レイヤ 3 メイン インターフェイス

（注） set dei アクションは、802.1ad カプセル化用に設定されていないインターフェイスのトラフィックに対しては無視されます。

デフォルト DEI マーキング

着信パケット		インポーズされた 802.1ad ヘッダーのデフォルト DEI
802.1q パケット	なし	0
802.1ad パケット	なし	着信パケットの最上位タグの DEI

着信パケット		インポーズされた 802.1ad ヘッダーのデフォルト DEI
802.1ad パケットに変換された 802.1q パケット または 802.1ad パケット	set dei {0 | 1}	0 または 1 set アクションの DEI 値に基づく

IP precedence と IP DSCP マーキングの比較

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

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

ボーダー ゲートウェイ プロトコルを使用した QoS ポリシー伝搬

パケット分類は、データ パス上で輻輳管理または輻輳回避を必要とするトラフィック フローを識別し、マーキングします。 ボーダー ゲートウェイ プロトコルを使用した Quality of Service ポリシー伝搬（QPPB）では、アクセス リスト（ACL）、ボーダー ゲートウェイ プロトコル（BGP）コミュニティ リスト、BGP 自律システム（AS）パス、送信元プレフィックス アドレス、または宛先プレフィックス アドレスに基づいて、パケットを QoS グループ ID で分類できます。 パケットを分類しておくと、ポリシングや重み付けランダム早期検出（WRED）などの他の QoS 機能を使用して、ビジネス モデルに適合するようにポリシーを指定し、実行できます。

BGP を使用した QoS ポリシー伝搬（QPPB）では、トラフィック ポリシングの適用に使用できるシスコ エクスプレス フォワーディング（CEF）パラメータに BGP プレフィックスおよび BGP 属性をマッピングできます。 QPPB を使用すると、ネットワークのある場所で設定した BGP ポリシーを、BGP を使用してネットワークの別の場所に伝搬し、そこで適切な QoS ポリシーを作成できます。

QPPB では、次の各点に基づいてパケットを分類できます。

- アクセス リスト
- BGP コミュニティ リスト。 コミュニティ リストを使用すると、ルート ポリシーの match 句で使用するコミュニティ グループを作成できます。 アクセス リストと同様に、一連のコミュニティ リストを作成できます。

- BGP 自律システム パス。 BGP 自律システム パスに基づいて、着信および発信の両方のルーティング アップデートに対してアクセス リストを指定することにより、これらのルーティング アップデートをフィルタリングできます。
- 送信元プレフィックス アドレス。 BGP ネイバーのアドレスから送信されたプレフィックス セットを分類できます。
- 宛先プレフィックス アドレス。 一連の BGP プレフィックスを分類できます。

分類は、トラフィックの送信元または宛先アドレスに基づいて実行できます。 BGP および CEF は、サポートされている QPPB 機能に対して有効にする必要があります。

衛星システム上の QoS

QoS 機能の一貫した展開を自動化する自動 QoS は、衛星システムで有効化されています。 すべてのユーザ設定のレイヤ 2 およびレイヤ 3 機能が ASR9000 で適用され、衛星システムに対する個別の QoS 設定は必要ありません。 自動 QoS は、ICL リンクのオーバーサブスクリプションを処理します。 通常のポート上のその他すべての QoS 機能（ブロードバンド QoS を含む）は、衛星ポートでもサポートされています。 ASR9000 シリーズ ルータと衛星ポート間のシステムの輻輳処理は、プライオリティと保護を維持するように設定されます。 自動 QoS は、ASR9000 シリーズ ルータと衛星間の衛星 ICL で流れるトラフィックの異なるクラス間に対する十分な区別を提供します。

システムは、1G ポート シェーパーに対して、最大 14 個の一意のシェーピング レートをサポートできます。 1G ポートは、トラフィック マネージャ（TM）階層の L0 エンティティを使用して表されます。 ポート シェーパーは、このレベルで適用されます。 衛星ポートで速度が変更された場合、QoS EA は、基本となる衛星ポートの速度に基づいてポリシーマップを自動的に再設定します。 ただし、ポリシーが存在ない場合、ポリシー マネージャ（PM）は、ポート シェーパー API（アプリケーションプログラミングインターフェイス）を呼び出すことによってポートの速度を設定する必要があります。 システムは、AN によって基本となるポートの速度が変更された場合に、パーセンテージベースのポリシーを変更します。 ASR9000 シリーズルータ上のポリシーに自動ネゴシエーションされた速度を伝播すると、時間差が発生する場合があります。この期間中は、衛星デバイスでパケット ドロップが発生することが想定されます。

（注） 入力サービス ポリシーでのキューイングは、衛星インターフェイスではサポートされていません。

衛星システムの QoS の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide*』を参照してください。

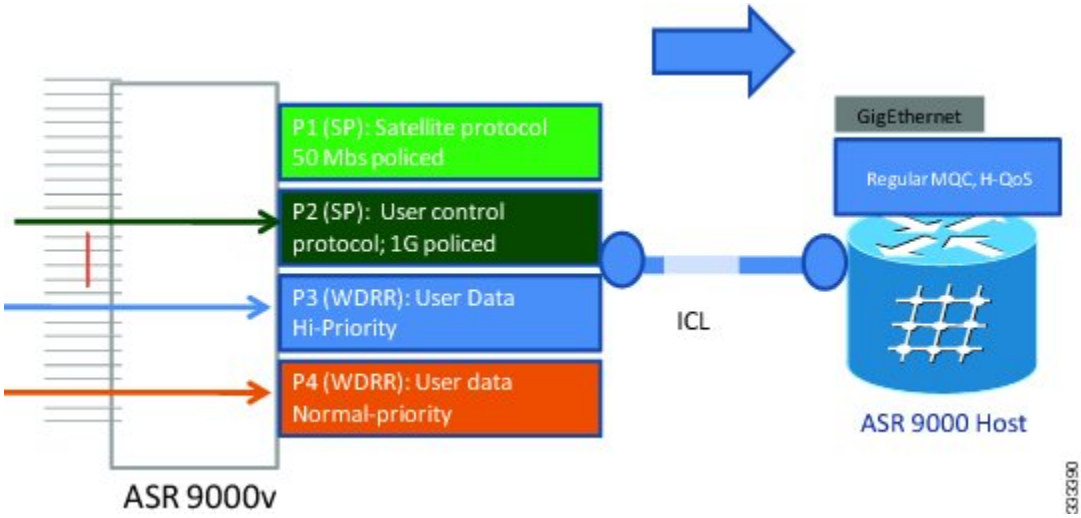
自動 QoS

衛星システムから Cisco IOS XR ASR9000 シリーズ ルータへのトラフィック、および ASR9000 シリーズ ルータから衛星システムへのトラフィックについて説明します。

衛星から ASR9000 シリーズ ルータ

- トラフィックは、信頼ポート モデルを使用して処理されます。
- パケットが制御パケット（LACP、STP、CDP、CFM、ARP、OSPF など）、高プライオリティのデータ（VLAN COS 5、6、7、IP prec 5、6、7）、または通常のプライオリティのデータであり、それに応じてキューイングされるかどうかは、自動パケット分類ルールによって決定されます。
- 衛星によって自動で優先順位付けされるプロトコル タイプ：すべての IEEE コントロール プロトコル（01 80 C2 xx xx xx）、LACP、802.3ah、CFM、STP、CDP、LLDP、ARP、OSPF、RIP、BGP、IGMP、RSVP、HSRP、VRRP p2 q。
- 衛星によって自動で優先順位付けされるユーザ データ パケット：VLAN CoS 5、6、7、IP precedence 5、6、7、MPLS EXP 5、6、7。

図 *8*：自動 *QoS*、衛星からホスト

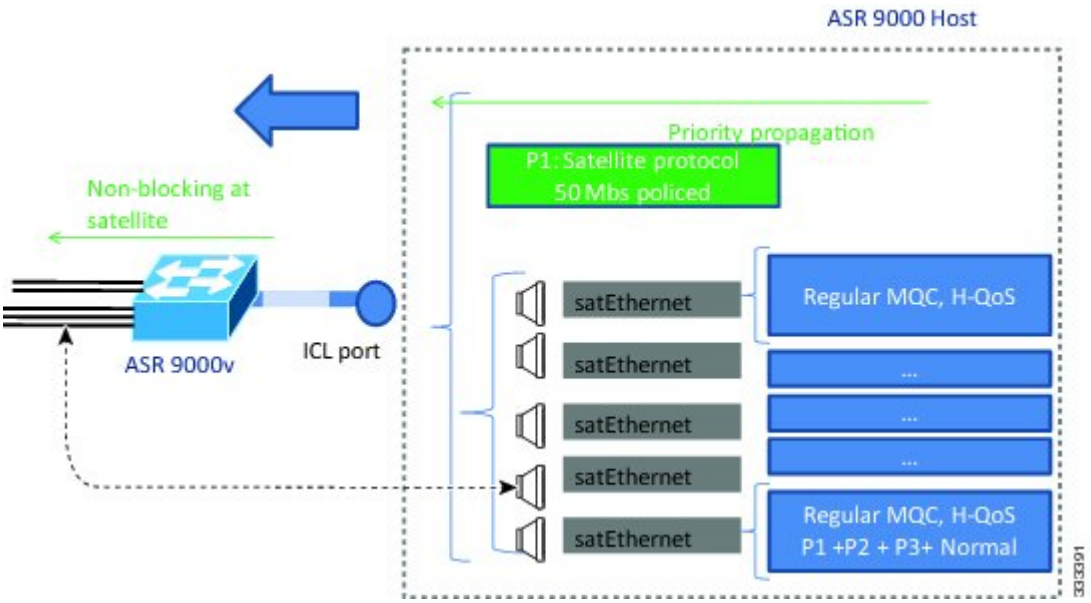


ASR9000 シリーズ ルータから衛星

- 衛星出力ポートに宛てられたトラフィックは、ダウンストリームのシェーピング アクセス ポートの速度を一致させるために ASR9K でシェーピングされます。
- トラフィックは、フル 3 レベル出力キューイング階層に基づいてストリーミングされます。

- リモートで管理されている各衛星アクセス GigE ポートは、アクセス回線速度を一致させるために自動シェーピングされます。

図 *9*：自動 *QoS*、ホストから衛星



PWHE 上の QoS

疑似配線ヘッド エンド（PWHE）上の QoS は、サービス プロバイダーのエッジ ルータの拡張 L3VPN サービスをイネーブルにします。

PWHE-QoS の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide*』を参照してください。

サポートされる機能

PWHE での QoS の機能：

- 入力 PWHE と出力 PWHE の両方のポリシー マップ。 ハードウェア制限内でのポリシング、マーキング、およびキューイングが入力と出力の両方でサポートされています。
- 通過トラフィック用のポートのポリシーは、PWHE インターフェイス用のポリシーと同時に適用できます。
- ポリシーは、すべての PWHE メンバでレプリケートされます。 これは、PWHE ポリシーマップで指定されたレートが、特定されたすべてのメンバの最低のレートに制限されることを意味します。 たとえば、PW-HE インターフェイスに 1G と 10G の両方で特定されたメンバが存在する場合、レートは 1G に制限されます。 10G メンバに 900 mbps のシェーパーがある場合、PWHE インターフェイス ポリシーのレートは、900 Mbps に制限されます。

- メンバ インターフェイスのポート シェーピング ポリシーは、そのポートを通過する PWHE トラフィックに影響を与えます。

制限事項

- PW-HE ポリシーの親レベルでのパーセンテージ ベースのシェーピングまたはポリシングはサポートされていません。
- QoS アカウンティングには、疑似配線ヘッダーが含まれません。

帯域幅の分配

異なる PW HE 仮想インターフェイスの QoS ポリシー、および物理インターフェイスの QoS ポリシーに対応するキューイング リソースは、すべてTM内の同一のポート下にあります。 スケジューリングの観点から、物理インターフェイス QoS ポリシーおよび PW HE インターフェイス QoS ポリシーで設定されたキューイング パラメータ（minimum bandwidth、maximum bandwidth/shape、weight/bandwidth remaining）は、互いに影響します。 物理インターフェイスの帯域幅は、すべての QoS ポリシーによって共有されます。

Bandwidth remaining コマンドを PW-HE ポリシーの親デフォルト クラスで使用して、さまざまな PW-HE インターフェイスと物理インターフェイス間の超過帯域幅の分配を制御できます。

QoS アカウンティング

- QoS 機能（ポリシング、シェーピング、統計情報など）を実行する際のパケット長は、カスタマー IP パケット、カスタマー L2 ヘッダー、および設定された追加オーバーヘッドに基づきます。
- QoS 統計情報には、カスタマー IP パケット、カスタマー L2 ヘッダー、および設定された追加オーバーヘッドが含まれます。
- 外部 MPLS ヘッダー（VC ラベル、トランスポート ラベルなど）および外部 L2 ヘッダー（基本となる物理インターフェイスのレイヤ 2 カプセル化）は、PW HE 仮想インターフェイスで QoS を実行する際のパケット長には含まれません。

マーキング サポート

PW ether：入力と出力

- カスタマー IP ヘッダー、qos-group、および discard-class のマーキングがサポートされます。
- インポーズされたすべての MPLS ラベルの EXP ビットのマーキングがサポートされます。
- インポーズされたラベルの EXP は、入力ポリシーにだけ設定できます。 ただし、出力 QoS ポリシーの処理後、より多くのラベルがカスタマー IP パケットにインポーズされるため、PW HE インターフェイスに付加された出力ポリシーでも設定できるように例外が適用されます。

- 転送 L2 ヘッダーの CoS ビットのマーキングはサポートされず、デフォルトの動作になります。
- 入力方向の無条件マーキングの場合は、DSCP/precedence、インポーズされたラベルの EXP、qos-group、および discard-class の各フィールドをマーキングできます。
- 出力方向の無条件マーキングの場合は、DSCP/precedence およびインポーズされたラベルの EXP の各フィールドをマーキングできます。
- 入力方向の条件付きポリサー マーキングの場合は、DSCP/precedence、インポーズされたラベルの EXP、qos-group、および discard-class の各フィールドのうち、最大で 2 つのフィールドをマーキングできます。
- 出力方向の条件付きポリサー マーキングの場合は、DSCP/precedence およびインポーズされたラベルの EXP の各フィールドをマーキングできます。

ポリシングおよびキューイングのサポート

通常の L3 インターフェイスでサポートされているすべてのポリシング機能は、PW-HE でもサポートされます。

キューイング

	入力および出力キュー	入力および出力ポリサー
ポリシー マップのない PW-HE インターフェイス	各 PW-HE メンバには、ポートごとにデフォルト キューがあります。 入力および出力の両方のトラフィックは、メンバ ポートのデフォルト キューを使用します。	N/A
ポリシー マップ付きの PW-HE インターフェイス	ポリシー マップの入力および出力キューは、各 PW-HE メンバで複製されます。	ポリシー マップの入力および出力ポリサーは、各 PW-HE メンバごとに複製されます。

（注） PW-HE メンバがバンドルの場合、ポリシー マップはバンドル メンバで複製されます。

統計

PW HE 仮想インターフェイス QoS ポリシーの show コマンドは、入力/出力の統計情報を次の条件で提供します。

- 特定されたメンバごと。
- 特定されたメンバがバンドルの場合、統計情報はバンドルごとに集約されます。
- pwhe インターフェイス全体で集約された統計情報。

ポリシーのインスタンス化

ここでは、PW-HE の QoS のさまざまなシナリオについて説明します。

- 任意のメンバ インターフェイスに適用されるポリシーがある場合は、非 PW-HE トラフィックだけがこれらのポリシーの対象になります。 これに対する例外は、設定されたポートシェーパーです。
- PW-HE ポリシーが PW-HE 仮想インターフェイスに追加されると、すべての PW-HE トラフィックがそのポリシーの対象になります。 ただし、メンバ インターフェイスの非 PW-HE トラフィックは、対応するメンバインターフェイスで設定されているポリシーの対象になります。
- PW-HE ポリシーは、2 レベル階層である必要があります。 仮想インターフェイスに適用される親ポリシーには、絶対レートに基づいて設定されたシェーピング/ポリシング付きの class-default が必要です。
- メンバ インターフェイスが異なるラインカードから割り当てられている場合、VC ラベル ベースのハッシュを使用して出力インターフェイス（PW-HE トラフィックにアクセスするコア）を判断する場合にだけ精度を保証できます。 VC ラベル ベースのハッシュは、PW-HE に対応するトラフィックを特定のメンバ インターフェイスに対して偏向します。 これにより、絶対値が設定される際に正確な QoS シェーピングを保証します。
- 複数の PW-HE インターフェイス（LC ごとに最大 1792）は、単一のメンバ インターフェイス（物理インターフェイスまたはバンドル インターフェイス）を共有できます。 それぞれの PW-HE インターフェイス QoS ポリシがメンバ インターフェイス上でインスタンス化されます。
- PW-HE メンバインターフェイスがバンドルの場合、PW-HE ポリシーは、各バンドル メンバでインスタンス化されます。

（注） PWHE インターフェイスが作成された場合で、PWHE QoS ポリシーが適用されない場合、PW-HE と非 PW-HE の両方のトラフィックがメンバ インターフェイスのデフォルト キューを介して渡されます。

QoS ポリシーのない PW-HE

次の 2 つのケースは、疑似配線ヘッドエンド インターフェイスのデフォルト動作を表します。

- PW-HE 入力からコア側出力（アクセスからコア）：カスタマー IP パケットからの DSCP/precedence 値は、コア側方向のすべてのインポーズされたラベル（VPN および転送）の EXP にコピーされます。

- PW-HE 出力（コアからアクセス）：カスタマー IP パケットからの DSCP/precedence 値は、アクセス側方向のすべてのインポーズされたラベル（VPN および転送）の EXP にコピーされます。

例：PW-HE

```
policy-map pw_child_in
 class voip
  priority level 1
  police rate 1 percent 1

class video
police rate percent 10

 priority level 2

class data
  police rate percent 70 peak-rate-percent
  100
  exceed-action transmit
  violate action drop
end-policy-map
!
policy-map pw_child_out
 class voip
 priority level 1
 police rate 1 mbps
 !
!
class data
 bandwidth remaining percent 70
 random-detect discard-class 3 40 ms 50 ms
!
class video
 priority level2
 police rate 10 mbps
!
1
class class-default
 random-detect discard-class 1 20 ms 30 ms
!
end policy-map

policy-map pw_child_out
 class voip
  priority level 1
  police rate 1 mbps
  !
 !
 class data
  bandwidth remaining percent 70
  random-detect discard-class 3 40 ms 50 ms
 !
 class video
  priority level 2
  police rate 10 mbps
  !
 !
 class class-default
  random-detect discard-class 1 20 ms 30 ms
 !
 end-policy-map
!
policy-map pw_parent_out
 class class-default
  service-policy pw_child_out
  shape average 100 mbps
 !
```

```
 end-policy-map
!

interface pw-ether 1
 service-policy input pw_parent_in
 service-policy output pw_parent_out
```

その他の PW-HE の関連情報については、『*Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide*』を参照してください。

In-Place ポリシーの変更

In-Place ポリシーの変更機能では、QoS ポリシーが 1 つ以上のインターフェイスに付加されている場合でも QoS ポリシーを変更できます。 1 つ以上のインターフェイスに付加されている QoS ポリシーを変更すると、その QoS ポリシーが付加されているすべてのインターフェイスで QoS ポリシーが自動的に変更されます。 変更されたポリシーは、新しいポリシーをインターフェイスにバインドするときと同じチェックを受けます。

ポリシー変更が成功した場合、変更されたポリシーは、ポリシーが付加されているすべてのインターフェイスに対して有効になります。 コンフィギュレーションセッションはポリシーの変更が完了するまでブロックされます。

ただし、ポリシーの変更がいずれかのインターフェイスで失敗した場合には、すべてのインターフェイスに対して変更前のポリシーが有効になるように、自動ロールバックが開始されます。 コンフィギュレーションセッションは、影響を受けるすべてのインターフェイスでロールバックが完了するまでブロックされます。

In-Place ポリシーの変更時に回復不可能なエラーが発生した場合は、ポリシーは対象のインターフェイスに対して矛盾した状態になります。 各場所における矛盾を表示するには、**show qos inconsistency** コマンドを使用してください。（このコマンドは、ASR 9000 イーサネット ラインカードでのみサポートされています）。コンフィギュレーションセッションは、変更されたポリシーが、ポリシーを使用するすべてのインターフェイスで有効になるまでブロックされます。 コンフィギュレーション セッションのブロックが解除されるまで、新たな設定を行うことはできません。

インターフェイスに付加されている QoS ポリシーを変更したとき、変更されたポリシーを使用するインターフェイスでは、短期間、有効なポリシーがない場合が生じる可能性があります。

（注） インターフェイスに付加されているポリシーの QoS 統計情報は、ポリシーを変更すると失われます（0 にリセット）。

In-Place ポリシーの変更を引き起こす可能性のある変更

QoS ポリシーの変更

- 帯域幅またはポリシングなどの新しいアクションの追加
- 新しいサービス ポリシーの追加（階層レベルを上げる）

- 既存のアクションの削除
- 既存のアクションの変更
- サービス ポリシーの削除（階層レベルを下げる）
- 新しいアクションを伴う新しいクラスの追加
- ポリシーへの複数のクラスの追加または削除
- 子ポリシーの変更

クラス マップの変更

- 新しい match 文の追加
- 既存の match 文の削除
- 照合タイプの変更（match-all から match-any、またはその逆）
- 既存の match 文の変更

クラス マップで使用するアクセス リストの変更

- 新しいアクセス コントロール エントリ（ACE）の追加
- ACE の削除
- ACE の修正

In-Place ポリシー変更に関する推奨事項

QoS ポリシーを変更している間の短期間、変更するポリシーを使用するインターフェイスでは、有効なポリシーがない状態が生じることがあります。 このため、同時に最小限のインターフェイスに影響する QoS ポリシーを変更します。 ポリシー マップの変更時に影響するインターフェイスの数を確認するには、**show policy-map targets** コマンドを使用します。

インターフェイス帯域幅の動的な変更

ここでは、インターフェイス帯域幅機能の動的な変更について説明します。

ポリシー状態

- 検証：この状態は、新しいインターフェイス帯域幅値について、設定されたQoSポリシーの非互換性を示します。 システムは、ベストエフォート方式でトラフィックを処理します。また、トラフィック ドロップが発生する場合があります。

モジュラ QoS のパケット分類の設定方法

ここでは、次のタスクの手順を示します。

トラフィック クラスの作成

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

概念の情報については、トラフィック クラスの要素を参照してください。

制約事項

この設定作業で指定するすべての **match** コマンドの使用は任意ですが、1 つのクラスに少なくとも 1 つの一致基準を設定する必要があります。

手順の概要

1. **configure**
2. **class-map** [type qos] [match-**any**] [**match**-all] *class-map-name*
3. **match access-group** [**ipv4** | **ipv6**] *access-group-name*
4. **match** [**not**] **cos** [*cos-value*] [*cos-value0 ... cos-value7*]
5. **match** [**not**] **cos inner** [*inner-cos-value*] [*inner-cos-value0...inner-cos-value7*]
6. **match destination-address mac** *destination-mac-address*
7. **match source-address mac** *source-mac-address*
8. **match** [**not**] **discard-class** *discard-class-value* [*discard-class-value1 ... discard-class-value6*]
9. **match** [**not**] **dscp** [**ipv4** | **ipv6**] *dscp-value* [*dscp-value ... dscp-value*]
10. **match** [**not**] **mpls experimental topmost** *exp-value* [*exp-value1 ... exp-value7*]
11. **match** [**not**] **precedence** [**ipv4** | **ipv6**] *precedence-value* [*precedence-value1 ... precedence-value6*]
12. **match** [**not**] **protocol** *protocol-value* [*protocol-value1 ... protocol-value7*]
13. **match** [**not**] **qos-group** [*qos-group-value1 ... qos-group-value8*]
14. **match vlan [inner]** *vlanid* [vlanid1 ... vlanid7]
15. 次のいずれかのコマンドを使用します。
    - **end**
    - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**class-map** [type qos] [match-**any**] [**match**-all] *class-map-name* 例： `RP/0/RSP0/CPU0:router(config)# class-map class201`	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。 • 名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。 • **match-any** を指定すると、トラフィック クラスで受信したトラフィックの場合、一致基準の 1 つに必ず一致し、そのトラフィック クラスの一部と分類されます。 これがデフォルトです。 **match-all** を指定した場合は、トラフィックがすべての一致基準を満たす必要があります。
ステップ 3	**match access-group** [**ipv4** | **ipv6**] *access-group-name* 例： `RP/0/RSP0/CPU0:router(config-cmap)# match access-group ipv4 map1`	（任意）指定したアクセス コントロール リスト（ACL）名に基づいて、クラス マップの一致基準を設定します。
ステップ 4	**match** [**not**] **cos** [*cos-value*] [*cos-value0 ... cos-value7*] 例： `RP/0/RSP0/CPU0:router(config-cmap)# match cos 5`	（任意）クラス マップにパケットに一致する *cos-value* を指定します。 • *cos-value* 引数は、0 ～ 7 の整数で指定します。
ステップ 5	**match** [**not**] **cos inner** [*inner-cos-value*] [*inner-cos-value0...inner-cos-value7*] 例： `RP/0/RSP0/CPU0:router match cos inner 7`	（任意）クラス マップにパケットに一致する *inner-cos-value* を指定します。 • inner-cos-value 引数は、0 ～ 7 の整数で指定します。
ステップ 6	**match destination-address mac** *destination-mac-address* 例： `RP/0/RSP0/CPU0:router(config-cmap)# match destination-address mac 00.00.00`	（任意）指定する宛先 MAC アドレスに基づくクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 7	**match source-address mac** *source-mac-address* 例： `RP/0/RSP0/CPU0:router(config-cmap)# match source-address mac 00.00.00`	（任意）指定する送信元 MAC アドレスに基づくクラス マップの一致基準を設定します。
ステップ 8	**match** [**not**] **discard-class** *discard-class-value* [*discard-class-value1 ... discard-class-value6*] 例： `RP/0/RSP0/CPU0:router(config-cmap)# match discard-class 5`	（任意）クラス マップにパケットに一致する *discard-class-value* を指定します。 • *discard-class-value* 引数は、0 ～ 7 の整数で指定します。 **match discard-class** コマンドは、出力ポリシーに対してのみサポートされています。
ステップ 9	**match** [**not**] **dscp** [**ipv4** | **ipv6**] *dscp-value* [*dscp-value ... dscp-value*] 例： `RP/0/RSP0/CPU0:router(config-cmap)# match dscp ipv4 15`	（任意）一致基準として特定の DSCP 値を指定します。 • 値の範囲は 0 ～ 63 です。 • 数値の代わりに、予約済みキーワードも指定できます。 • match 文ごとに最大 8 つの値または範囲を使用できます。
ステップ 10	**match** [**not**] **mpls experimental topmost** *exp-value* [*exp-value1 ... exp-value7*] 例： `RP/0/RSP0/CPU0:router(config-cmap)# match mpls experimental topmost 3`	（任意）クラスマップを設定し、最上位のマルチプロトコル ラベル スイッチング（MPLS）ラベルの 3 ビット experimental（EXP）フィールドが、EXP フィールド値に対して検査されるようにします。 値の範囲は 0 ～ 7 です。
ステップ 11	**match** [**not**] **precedence** [**ipv4** | **ipv6**] *precedence-value* [*precedence-value1 ... precedence-value6*] 例： `RP/0/RSP0/CPU0:router(config-cmap)# match precedence ipv4 5`	（任意）IP precedence 値を一致基準として確認します。 • 値の範囲は 0 ～ 7 です。 • 数値の代わりに、予約済みキーワードも指定できます。
ステップ 12	**match** [**not**] **protocol** *protocol-value* [*protocol-value1 ... protocol-value7*] 例： `RP/0/RSP0/CPU0:router(config-cmap)# match protocol igmp`	（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。

	コマンドまたはアクション	目的
ステップ 13	**match** [**not**] **qos-group** [*qos-group-value1 ... qos-group-value8*] 例： `RP/0/RSP0/CPU0:router(config-cmap)# match qos-group 1 2 3 4 5 6 7 8`	（任意）クラスマップにパケットに一致するサービス（QoS）グループ値を指定します。 • *qos-group-value* ID 引数の値は、0 ～ 63 の範囲の正確な値または値の範囲として指定します。 • 1 つの match 文に対して最大 8 つの値（スペースで区切る）を入力できます。 • **match qos-group** コマンドは、出力ポリシーに対してのみサポートされています。
ステップ 14	**match vlan [inner]** *vlanid* [vlanid1 ... vlanid7] 例： `RP/0/RSP0/CPU0:router(config-cmap)# match vlan vlanid vlanid1`	（任意）クラス マップにパケットに一致する VLAN ID または VLAN ID の範囲を指定します。 • *vlanid* は、1 ～ 4094 の範囲の正確な値または値の範囲として指定します。 • サポートされている VLAN の値または範囲の総数は 8 つです。

ステップ 15	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

	コマンドまたはアクション	目的

トラフィック ポリシーの作成

トラフィック ポリシーを作成するには、**policy-map** グローバル コンフィギュレーション コマンドを使用して、トラフィック ポリシーの名前を指定します。

トラフィック クラスは、**class** コマンドを使用したときにサービス ポリシーと関連付けられます。**class** コマンドは、ポリシー マップ コンフィギュレーション モードを開始した後に実行しなければなりません。 **class** コマンドを入力すると、ルータは自動的にポリシー 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。ここでトラフィック ポリシーの QoS ポリシーを定義します。

次のクラス アクションがサポートされています。

- bandwidth：クラスの帯域幅を設定します。 このガイドの Cisco ASR 9000 シリーズ ルータでのモジュラ QoS の輻輳管理の設定に関するモジュールを参照してください。
- police：トラフィックをポリシングします。 このガイドの Cisco ASR 9000 シリーズ ルータでのモジュラ QoS の輻輳管理の設定に関するモジュールを参照してください。
- priority：クラスにプライオリティを割り当てます。 このガイドの Cisco ASR 9000 シリーズ ルータでのモジュラ QoS の輻輳管理の設定に関するモジュールを参照してください。
- queue-limit：クラスにキュー制限（テール ドロップしきい値）を設定します。 このガイドの「Configuring Modular QoS Congestion Avoidance on Cisco ASR 9000 Series Routers」を参照してください。
- random-detect：ランダム早期検出をイネーブルにします。 このガイドの「Configuring Modular QoS Congestion Avoidance on Cisco ASR 9000 Series Routers」を参照してください。
- service-policy：子サービス ポリシーを設定します。
- set：このクラスのマーキングを設定します。 クラスベース無条件パケット マーキングの機能と利点を参照してください。
- shape：クラスのシェーピングを設定します。 このガイドの Cisco ASR 9000 シリーズ ルータでのモジュラ QoS の輻輳管理の設定に関するモジュールを参照してください。

一致基準として入力できるその他のコマンドについては、『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』を参照してください。

概念の情報については、トラフィック ポリシーの要素を参照してください。

手順の概要

1. **configure**
2. policy-map [type qos] policy-name
3. class **class-name**
4. **set precedence**
5. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	policy-map [type qos] policy-name 例： RP/0/RSP0/CPU0:router(config)# policy-map policy1	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	class **class-name** 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**set precedence** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# set precedence 3`	IP ヘッダーに優先順位を設定します。

ステップ 5	**end** または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-pmap-c)# end`
	または
	`RP/0/RSP0/CPU0:router(config-pmap-c)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。

	コマンドまたはアクション	目的
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、ルータは現在のコンフィギュレーションセッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

トラフィック ポリシーのインターフェイスへの適用

トラフィック クラスとトラフィック ポリシーの作成後、service-policyインターフェイス コンフィギュレーション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付加し、ポリシーを適用する方向を指定します（インターフェイスに着信するパケットまたはインターフェイスから送信されるパケット）。

ポリシー マップ クラス コンフィギュレーション モードで入力できるその他のコマンドについては、『Cisco ASR 9000 Series Aggregation Services RoutersModular Quality of Service Command Reference.』を参照してください。

前提条件

インターフェイスにトラフィック ポリシーを付加する前に、トラフィック クラスとトラフィック ポリシーを作成する必要があります。

制約事項

なし

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **service-policy** {**input** | **output**} *policy-map*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
5. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/9`	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、インターフェイスを設定します。
ステップ 3	**service-policy** {**input**	**output**} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシー マップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。

	コマンドまたはアクション	目的
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 設定変更を実行コンフィギュレーションファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。
ステップ 5	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0/RSP0/CPU0:router# show policy-map interface gigabitethernet 0/1/0/9`	（任意）指定されたインターフェイスのポリシーの統計情報を表示します。

複数のサブインターフェイスへの共有ポリシー インスタンスの付加

トラフィック クラスとトラフィック ポリシーの作成後、任意で **service-policy**（インターフェイス）コンフィギュレーションコマンドを使用して、共有ポリシーインスタンスを複数のサブインターフェイスに付加し、ポリシーを適用する方向を指定します（サブインターフェイスに着信するパケットまたはサブインターフェイスから送信されるパケット）。

（注） 共有ポリシーには、レイヤ 2 とレイヤ 3 のサブ インターフェイスの組み合わせを含めることができます。

ポリシー マップ クラス コンフィギュレーション モードで入力できるその他のコマンドについては、『Cisco ASR 9000 Series Aggregation Services Routers Modular Quality of Service Command Reference』を参照してください。

前提条件

共有ポリシーのインスタンスをサブインターフェイスに付加する前に、トラフィック クラスとトラフィック ポリシーを作成する必要があります。

制約事項

複数の物理インターフェイスにまたがる共有ポリシー インスタンスはサポートされていません。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **service-policy** {**input** | **output**} *policy-map* [shared-**policy-instance** instance-name]
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
5. **show policy-map shared-policy-instance** *instance-name* [**input** | **output**] **location** *rack/slot/module*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0.1`	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、サブインターフェイスを設定します。
ステップ 3	**service-policy** {**input** | **output**} *policy-map* [shared-**policy-instance** instance-name] 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1 shared-policy-instance Customer1`	サブインターフェイスのサービス ポリシーとして使用する入力サブインターフェイスまたは出力サブインターフェイスにポリシー マップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。

	コマンドまたはアクション	目的
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。
ステップ 5	**show policy-map shared-policy-instance** *instance-name* [**input** | **output**] **location** *rack/slot/module* 例： `RP/0/RSP0/CPU0:router# show policy-map shared-policy-instance Customer1 location 0/1/0/7.1`	（任意）指定した共有ポリシー インスタンスのサブインターフェイスに対するポリシーの統計情報を表示します。

バンドル インターフェイスまたは EFP バンドルへの共有ポリシー インスタンスの付加

トラフィック クラスとトラフィック ポリシーの作成後、任意で **service-policy**（**インターフェイス**）コンフィギュレーション コマンドを使用して、共有ポリシー インスタンスをバンドル インターフェイスやバンドル EFP に付加し、ポリシーを適用する方向を指定します（サブインターフェイスに着信するパケットまたはサブインターフェイスから送信されるパケット）。

ポリシー マップ クラス コンフィギュレーション モードで入力できるその他のコマンドについては、『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』を参照してください。

前提条件

共有ポリシー インスタンスをバンドル インターフェイスまたは EFP バンドルに付加する前に、トラフィック クラスとトラフィック ポリシーを作成する必要があります。

制約事項

複数の物理インターフェイスにまたがる共有ポリシー インスタンスはサポートされていません。

手順の概要

1. **configure**
2. **interface Bundle-Ether** *bundle-id*
3. **service-policy** {**input** | **output**} *policy-map* [shared-policy-instance instance-name]
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
5. **show policy-map shared-policy-instance** *instance-name* [**input** | **output**] **location** *location-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**interface Bundle-Ether** *bundle-id* 例： `RP/0/RP1/CPU0:router(config)# interface Bundle-Ether 100.1 l2transport`	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、バンドル インターフェイスを設定します。
ステップ 3	**service-policy** {**input** | **output**} *policy-map* [shared-policy-instance instance-name] 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1 shared-policy-instance Customer1`	サブインターフェイスのサービス ポリシーとして使用する入力または出力バンドル インターフェイスにポリシー マップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーションファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。

	コマンドまたはアクション	目的
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。
ステップ 5	**show policy-map shared-policy-instance** *instance-name* [**input** | **output**] **location** *location-id* 例： `RP/0/RSP0/CPU0:router# show policy-map shared-policy-instance Customer1 location 0/rsp0/cpu0`	（任意）指定した共有ポリシー インスタンスの場所でのポリシーの統計情報を表示します。

クラスベース無条件パケット マーキングの設定

この設定作業では、以下のクラスベースの無条件パケット マーキング機能をルータに設定する方法を説明します。

- IP precedence 値
- IP DSCP 値
- QoS グループ値（入力のみ）
- CoS 値（レイヤ 3 サブ インターフェイスの出力のみ）
- MPLS EXP 値
- 廃棄クラス

（注） MPLS タグ付きパケットに適用される IPv4 および IPv6 QoS アクションはサポートされていません。 設定は受け入れられますが、アクションは実行されません。

（注） クラスごとに **set** コマンドを 2 つだけ選択します。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **set precedence**
5. **set dscp**
6. **set qos-group** *qos-group-value*
7. **set cos** *cos-value*
8. **set cos** [inner] *cos-value*
9. **set mpls experimental** {**imposition** | **topmost**} *exp-value*
10. **set srp-priority** *priority-value*
11. **set discard-class** *discard-class-value*
12. **set atm-clp**
13. **exit**
14. **exit**
15. **interface** *type* interface-path-id
16. **service-policy** {**input** | **output**]} *policy-map*
17. 次のいずれかのコマンドを使用します。
    - **end**
    - **commit**
18. **show policy-map interface** *type interface-path-id* [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map policy1`	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。 • 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。

	コマンドまたはアクション	目的
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	ポリシー 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。 • ポリシーを作成または変更するクラスの名前を指定します。 クラスごとに 1 つの set コマンドを選択します
ステップ 4	**set precedence** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# set precedence 1`	IP ヘッダーに優先順位を設定します。 • **tunnel** キーワードは、外側 IP ヘッダーで IP precedence を設定します。 このオプションは、IPSec がインストールおよび設定されている Cisco XR 12000 シリーズ ルータだけで使用できます。
ステップ 5	**set dscp** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# set dscp 5`	ToS バイトに DSCP を設定することにより、パケットにマーキングします。 • **tunnel** キーワードは、外側 IP ヘッダーで IP DSCP を設定します。 このオプションは、IPSec がインストールおよび設定されている Cisco XR 12000 シリーズ ルータだけで使用できます。
ステップ 6	**set qos-group** *qos-group-value* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# set qos-group 31`	IPv4 パケットまたは MPLS パケットに QoS グループ ID を設定します。 **set qos-group** コマンドは入力ポリシーでのみサポートされています。
ステップ 7	**set cos** *cos-value* 例： `RP/0/RP0/CPU0:router(config-pmap-c)# set cos 7`	発信パケットの固有の IEEE 802.1Q レイヤ 2 CoS 値を設定します。 値は 0 ～ 7 です。 発信パケットのレイヤ 2 CoS 値を設定します。 • このコマンドは、スイッチに送信中のパケットにマーキングをする場合に、ルータで使用する必要があります。 スイッチは、CoS 値のマーキングを含む レイヤ 2 ヘッダー情報を利用できます。 • インターフェイスが受信するパケットは、CoS 値で設定できません。

	コマンドまたはアクション	目的
ステップ 8	**set cos** [inner] *cos-value* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# set cos 7`	発信パケットの固有の IEEE 802.1Q レイヤ 2 CoS 値を設定します。 値は 0 ～ 7 です。 発信パケットのレイヤ 2 CoS 値を設定します。 • このコマンドは、スイッチに送信中のパケットにマーキングをする場合に、ルータで使用する必要があります。 スイッチは、CoS 値のマーキングを含む レイヤ 2 ヘッダー情報を利用できます。 • レイヤ 2 インターフェイスでは、set cos コマンドは次のように処理されます。 メイン インターフェイスの入力または出力ポリシーでは拒否されます。 サブインターフェイスの入力ポリシーでは受け入れられますが、無視されます。 サブインターフェイスの出力ポリシーではサポートされています。 • レイヤ 3 インターフェイスでは、set cos コマンドは次のように処理されます。 メイン インターフェイスの入力ポリシーでは無視されます。 サブインターフェイスの入力ポリシーで拒否されます。 メイン インターフェイスとサブインターフェイスの出力ポリシーではサポートされています。
ステップ 9	**set mpls experimental** {**imposition** | **topmost**} *exp-value* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# set mpls experimental imposition 3`	MPLS パケットの最上位ラベルまたはインポジション ラベルの EXP 値を設定します。 • **imposition** は、入力ポリシーに付加されるサービス ポリシーに対してのみ使用できます。
ステップ 10	**set srp-priority** *priority-value* 例： `RP/0//CPU0:router(config-pmap-c)# set srp-priority 3`	発信パケットのスペース再利用プロトコル（SRP）のプライオリティ値を設定します。 • このコマンドは、インターフェイスの出力方向に対応付けられたサービス ポリシーでのみ使用できます。

	コマンドまたはアクション	目的
ステップ 11	**set discard-class** *discard-class-value* 例： `RP/0//CPU0:router(config-pmap-c)# set discard-class 3`	IP Version 4（IPv4）またはマルチプロトコル ラベル スイッチング（MPLS）パケットの廃棄クラスを設定します。 • このコマンドは、入力ポリシーに付加されるサービス ポリシーに対してのみ使用できます。
ステップ 12	**set atm-clp** 例： `RP/0/0/CPU0:router(config-pmap-c)# set atm-clp`	セル損失率優先度（CLP）ビットを設定します。
ステップ 13	**exit** 例： RP/0/RSP0/CPU0:router(config-pmap-c)# exit	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 14	**exit** 例： `RP/0/RSP0/CPU0:router(config-pmap)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 15	**interface** *type* interface-path-id 例： `RP/0/RSP0/CPU0:router(config)# interface pos 0/2/0/0`	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、インターフェイスを設定します。
ステップ 16	**service-policy** {**input** | **output**]} *policy-map* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy output policy1`	インターフェイスのサービス ポリシーとして使用する入力インターフェイスまたは出力インターフェイスにポリシーマップを付加します。 • この例では、トラフィック ポリシーでそのインターフェイスから送信されるすべてのトラフィックを評価します。
ステップ 17	次のいずれかのコマンドを使用します。 • **end** • **commit** 例： `RP/0/RSP0/CPU0:router(config-if)# end`	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:` ◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッ

	コマンドまたはアクション	目的
	または `RP/0/RSP0/CPU0:router(config-if)# commit`	ションが終了して、ルータが EXEC モードに戻ります。 ◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。
ステップ 18	**show policy-map interface** *type interface-path-id* [**input** | **output**] 例： `RP/0/RSP0/CPU0:router# show policy-map interface pos 0/2/0/0`	（任意）指定されたインターフェイス上のすべてのサービス ポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

ボーダー ゲートウェイ プロトコルを使用した QoS ポリシー伝搬の設定

ここでは、ボーダー ゲートウェイ プロトコル（BGP）コミュニティ リスト、BGP 自律システム パス、アクセス リスト、送信元プレフィックス アドレス、または宛先プレフィックス アドレスに基づいて、BGP を使用したポリシー伝搬をルータ上で設定する方法について説明します。

BGP を使用したポリシー伝搬の設定のタスク リスト

BGP を使用したポリシー伝搬では、BGP コミュニティ リスト、BGP 自律システム パス、アクセス リスト、送信元プレフィックスアドレス、および宛先プレフィックスアドレスに基づいて、IP precedence または QoS グループ ID（あるいはその両方）でパケットを分類できます。 パケットを分類しておくと、重み付けランダム早期検出（WRED）などの他の QoS 機能を使用して、ビジネス モデルに適合するようにポリシーを指定し、実行できます。

タスクの概要

BGP によるポリシー伝搬を設定するには、次の基本作業を実行します。

- BGP およびシスコ エクスプレス フォワーディング（CEF）を設定します。 BGP を設定するには、『*Cisco IOS XR Routing Configuration Guide*』を参照してください。 CEF を設定するには、『*Cisco IOS XR IP Address and Services Configuration Guide*』を参照してください。
- BGP コミュニティ リストまたはアクセス リストを設定します。
- ルート ポリシーを定義します。 BGP コミュニティ リスト、BGP 自律システム パス、アクセス リスト、送信元プレフィックス アドレス、または宛先プレフィックス アドレスに基づいて、IP precedence または QoS グループ ID を設定します。
- BGP にルート ポリシーを適用します。
- 目的のインターフェイス上で QPPB を設定します。
- 上記の分類（IP precedence または QoS グループ ID による分類）を使用するように QoS ポリシーを設定します。 専用アクセス レート（CAR）、WRED、およびテール ドロップを設定するには、「Configuring Modular QoS Congestion Avoidance on Cisco IOS XR Software」モジュールを参照してください。

ルート ポリシーの定義

この作業では、IP precedence または QoS グループ ID による BGP プレフィックスの分類に使用するルート ポリシーを定義します。

前提条件

ルート ポリシーで使用する BGP コミュニティ リストまたはアクセス リストを設定します。

制約事項

- 出力 QoS ポリシーを使用した IPv4 QPPB および IPv6 QPPB は、すべてのイーサネットおよび SIP-700 ラインカードでサポートされています。
- 入力 QoS ポリシーを使用した IPv4 QPPB は、最初の世代の ASR9000 イーサネット ラインカードでサポートされています。

手順の概要

1. **configure**
2. **route-policy** *name*
3. **set qos-group***qos-group-value*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**route-policy** *name* 例： `RP/0/RSP0/CPU0:router(config)# route-policy r1`	ルート ポリシー コンフィギュレーション モードに切り替え、設定するルート ポリシーの名前を指定します。
ステップ 3	**set qos-group***qos-group-value* 例： `RP/0/RSP0/CPU0:router(config-pmap-c) # set qos-group 30`	QoS グループ ID を設定します。 set qos-group コマンドは入力ポリシーでのみサポートされています。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

BGP に対するルート ポリシーの適用

この作業では、BGP にルート ポリシーを適用します。

前提条件

BGP および CEF を設定します。

手順の概要

1. **configure**
2. **router bgp***as-number*
3. **address-family***address-prefix*
4. **table-policy***policy-name*
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**router bgp***as-number* 例： `RP/0/RSP0/CPU0:router(config) # router bgp 120`	BGP 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	**address-family***address-prefix* 例： `RP/0/RSP0/CPU0:router(config-bgp) # address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始します。このモードでは、アドレス ファミリを設定できます。
ステップ 4	**table-policy***policy-name* 例： `RP/0/RSP0/CPU0:router(config-bgp-af) # table-policy qppb a1`	ルーティング ポリシーを適用します。
ステップ 5	次のいずれかのコマンドを使用します。	設定変更を保存します。

	コマンドまたはアクション	目的

	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーションファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

目的のインターフェイスでの QPPB の設定

この作業では、指定したインターフェイスにQPPBを適用します。ルートポリシーでのプレフィックスの一致に基づいて、トラフィックの分類が始まります。トラフィックの送信元または宛先の IP アドレスを使用して、ルート ポリシーを照合できます。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **ipv4 | ipv6 bgp policy propagation input** {**ip-precedence** | **qos-group**} {**destination** [*ip-precedence {destination | source}]* | **source** [*ip-precedence {destination | source}]* }
   RP/0/RSP0/CPU0:router(config)#ipv4 bgp policy propagation input qos-group destination

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)#interface POS 0/0/0/0`	インターフェイス コンフィギュレーション モードを開始して、1 つ以上のインターフェイスを VRF に関連付けます。
ステップ 3	**ipv4 | ipv6 bgp policy propagation input** {**ip-precedence** | **qos-group**} {**destination** [*ip-precedence {destination | source}]* | **source** [*ip-precedence {destination | source}]* } RP/0/RSP0/CPU0:router(config)#ipv4 bgp policy propagation input qos-group destination	いずれかのインターフェイスでQPPBをイネーブルにします。

QPPB の使用例

トラフィックが（単一の）ルータ port1 および port2 を介して Network1 から Network2 に移動する場合について考えます。 QPPB が port1 でイネーブルの場合

- 入力の QoS の場合：インターフェイス port1 の入力ポリシーに対応付けます。
- 出力の QoS の場合：インターフェイス port2 の出力ポリシーに対応付けます。

階層型入力ポリシングの設定

手順の概要

1.
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **service-policy** *policy-name*
5. **police rate percent** *percentage*
6. **conform-action** *action*
7. **exceed-action** *action*
8. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	例： `RP/0//CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0//CPU0:router(config)# policy-map parent`	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。 1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します
ステップ 3	**class** *class-name* 例： `RP/0//CPU0:router(config-pmap)# class class-default`	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。 ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**service-policy** *policy-name* 例： `RP/0//CPU0:router(config-pmap-c)# service-policy child`	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。
ステップ 5	**police rate percent** *percentage* 例： `RP/0//CPU0:router(config-pmap-c)# police rate percent 50`	トラフィック ポリシングを設定し、ポリシーマップ 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** *action* 例： `RP/0//CPU0:router(config-pmap-c-police)# conform-action transmit`	レート制限に適合したパケットに対して実行するアクションを設定します。 可能なアクションは次のとおりです。 **transmit**：パケットを送信します。
ステップ 7	**exceed-action** *action* 例： `RP/0//CPU0:router(config-pmap-c-police)# exceed-action drop`	レート制限を超過したパケットに対して実行するアクションを設定します。 可能なアクションは次のとおりです。 **drop**：パケットをドロップします。
ステップ 8	**end** または **commit** 例： `RP/0//CPU0:router(config-pmap-c-police)# end`	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。

	コマンドまたはアクション	目的
	または `RP/0//CPU0:router(config-pmap-c-police)# commit`	Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータがEXECモードに戻ります。 **no** と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、ルータは現在のコンフィギュレーションセッションで継続されます。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

モジュラ QoS パケット分類の設定例

ここでは、次の例を示します。

定義されたトラフィック クラス：例

次に、2 つのトラフィック クラスを作成し、その一致条件を定義する例を示します。 1 つ目のトラフィック クラス class1 では、ACL 101 を一致基準として使用します。 2 番めのトラフィック クラス class2 では、ACL 102 を一致条件として使用しています。 パケットはこれらの ACL の内容と照合され、そのクラスに属するかどうかが判断されます。

```
class-map class1
  match access-group ipv4 101
  exit
!
class-map class2
  match access-group ipv4 102
  exit
```

not キーワードを **match** コマンドに使用すると、指定していないフィールド値に基にして照合を行います。 次の例では、DSCP 値が 4、8、10 以外である qos_example クラスのすべてのパケットが含まれます。

```
class-map match-any qos_example
  match not dscp 4 8 10
```

```
!
end
```

トラフィック ポリシーの作成：例

次の例では、policy1 というトラフィック ポリシーを定義し、class1 と class2 という 2 つのクラスのポリシー設定を含めます。 これらのクラスの一致基準は、定義されたトラフィック クラス：例で作成されたトラフィック クラスで定義されています。

class1 では、帯域幅割り当て要求と、そのクラス用に予約されるキューの最大バイト数の制限がポリシーに含まれています。 class2 に対しては、帯域幅割り当て要求だけがポリシーで指定されています。

```
policy-map policy1
  class class1
    bandwidth 3000
    queue-limit bytes 1000000000
    exit
!
  class class2
    bandwidth 2000
    exit

policy-map policy1
  class class1
    bandwidth 3000 kbps
    queue-limit 1000 packets
!
  class class2
    bandwidth 2000 kbps
!
  class class-default
!
end-policy-map
!
end
```

インターフェイスへのトラフィック ポリシーの付加：例

次に、既存のトラフィック ポリシーをインターフェイスに付加する例を示します（定義されたトラフィック クラス：例を参照）。 policy-map コマンドを使用してトラフィック ポリシーを定義した後、インターフェイス コンフィギュレーション モードで service-policy コマンドを使用して、このポリシーを 1 つ以上のインターフェイスに付加し、これらのインターフェイスのトラフィック ポリシーを指定できます。 同じトラフィック ポリシーは複数のインターフェイスに付加することができますが、各インターフェイスには入力と出力に対してそれぞれトラフィック ポリシーを 1 つだけ付加することができます。

```
interface gigabitethernet 0/1/0/9
  service-policy output policy1
  exit
!
interface TenGigE 0/5/0/1
  service-policy output policy1
  exit
```

複数のサブインターフェイスへのトラフィック ポリシーの付加：例

次に、複数のサブ インターフェイスに既存のトラフィック ポリシーを付加する例を示します。**policy-map** コマンドを使用してトラフィック ポリシーを定義した後、サブインターフェイス コンフィギュレーション モードで service-policy コマンドを使用して、このポリシーを 1 つ以上のサブインターフェイスに付加できます。

```
interface gigabitethernet 0/1/0/0.1
  service-policy input policy1 shared-policy-instance ethernet101
  exit
!
interface gigabitethernet 0/1/0/0.2
  service-policy input policy1 shared-policy-instance ethernet101
  exit
```

バンドル インターフェイスへのトラフィック ポリシーの付加：例

次に、既存のトラフィック ポリシーをバンドル インターフェイスに付加する例を示します。**policy-map** コマンドを使用してトラフィック ポリシーを定義した後、サブインターフェイス コンフィギュレーション モードで service-policy コマンドを使用して、このポリシーを 1 つ以上のバンドル サブインターフェイスに付加できます。

```
interface Bundle-Ether 100.1
  service-policy tripleplaypolicy shared-policy-instance subscriber1
  exit
!
interface Bundle-Ether 100.2
  service-policy output tripleplaypolicy shared-policy instance subscriber1
  exit
```

共有ポリシー インスタンスによる EFP ロード バランシング：例

次に、SPI が実装されている場合に EFP に対してロード バランシングを設定する例を示します。リンク バンドルの EFP ロード バランシングの詳細については、『Cisco IOS XR Interface and Hardware Component Configuration Guide』を参照してください。

バンドル インターフェイスの設定：例

```
interface Bundle-Ether 50
interface gigabitethernet 0/1/0/5
  bundle id 50 mode active
interface gigabitethernet 0/1/0/8
  bundle id 50 mode active
```

ロード バランス オプションによる 2 つのバンドル EFP の設定：例

次の例では、同じ物理メンバ リンクを通過する 2 つのバンドル EFP 宛てのトラフィックを設定します。

```
interface Bundle-Ether 50.25 l2transport
  encapsulation dot1q 25
  bundle load-balance hash-select 2
!
interface Bundle-Ether 50.36 l2transport
  encapsulation dot1q 36
  bundle load-balance hash-select 2
```

デフォルト トラフィック クラスの設定例

次に、トラフィック ポリシー policy1 のデフォルト クラスに対してトラフィック ポリシーを設定する例を示します。 デフォルト クラスの名前は class-default で、他のすべてのトラフィックから構成され、インターフェイスの帯域幅の 60 パーセントでシェーピングされます。

```
policy-map policy1
  class class-default
    shape average percent 60
```

class-map match-any コマンドの設定: 例

次の例では、一致基準が複数ある場合に、パケットがどのように評価されるかについて説明します。 **class-map match-any** コマンド中のパケットがトラフィック クラスのメンバであると見なされるためには、一致基準が 1 つだけが満たされる必要があります（論理的な OR 演算子）。 この例では、プロトコル IP OR QoS グループ 4 OR アクセス グループ 101 が成功する一致基準になる必要があります。

```
class-map match-any class1
  match protocol ipv4
  match qos-group 4
  match access-group ipv4 101
```

トラフィック クラス class1 では、成功する一致条件が見つかるまで連続的に一致基準が評価されます。 各一致基準が評価され、パケットがその基準に一致するかどうかが判断されます。パケットが指定した条件のうち少なくとも 1 つに一致すると、パケットはトラフィック クラスのメンバとして分類されます。

（注） **match qos-group** コマンドは、出力ポリシーでのみサポートされています。

クラスベースの無条件パケット マーキングの例

次に、一般的なクラスベースの無条件パケット マーキングの例を示します。

IP precedence のマーキングの設定：例

次の例では、*policy1* というサービス ポリシーを作成します。 このサービス ポリシーは、**class** コマンドを使用して事前に定義したクラス マップ *class1* に関連付けられ、その後、出力 POS インターフェイス 0/1/0/0 に付加されます。 ToS バイトの IP precedence ビットを 1 に設定します。

```
policy-map policy1
  class class1
    set precedence 1
!
interface pos 0/1/0/0
  service-policy output policy1
```

IP DSCP マーキングの設定：例

次の例では、policy1 というサービス ポリシーを作成します。 このサービス ポリシーは、**class** コマンドを使用して事前に定義したクラス マップに関連付けられます。 この例では、class1 というクラス マップが事前に設定されていることを前提としています。

次の例では、ToS バイトの IP DSCP 値を 5 に設定します。

```
policy-map policy1
  class class1
    set dscp 5

  class class2
    set dscp ef
```

エッジで音声パケットに対して示される設定を行った後、すべての中間ルータは次のように音声パケットに低遅延処理を行うよう設定されます。

```
class-map voice
  match dscp ef
policy-map qos-policy
  class voice
    priority level 1
    police rate percent 10
```

QoS グループ マーキングの設定：例

次の例では、*policy1* というサービス ポリシーを作成します。 このサービス ポリシーは、**class** コマンドを使用してクラス マップ *class1* に関連付けられ、その後 GigabitEthernet インターフェイス 0/1/0/9 の入力方向に付加されます。 qos-group 値は 1 に設定されます。

```
class-map match-any class1
  match protocol ipv4
  match access-group ipv4 101

policy-map policy1
  class class1
    set qos-group 1
  !
interface gigabitethernet 0/1/0/9
  service-policy input policy1
```

（注） **set qos-group** コマンドは入力ポリシーでのみサポートされています。

CoS マーキングの設定：例

次の例では、*policy1* というサービス ポリシーを作成します。 このサービス ポリシーは、**class** コマンドを使用してクラス マップ *class1* に関連付けられ、その後 10-Gigabit Ethernet インターフェイス TenGigE0/1/0/0 の出力方向に付加されます。 レイヤ 2 ヘッダーの IEEE 802.1p（CoS）ビットは 1 に設定します。

```
class-map match-any class1
  match protocol ipv4
  match access-group ipv4 101

policy-map policy1
  class class1
    set cos 1
  !
interface TenGigE0/1/0/0
interface TenGigE0/1/0/0.100
  service-policy output policy1
```

MPLS EXP ビット インポジション マーキングの設定：例

次の例では、*policy1* というサービス ポリシーを作成します。 このサービス ポリシーは、**class** コマンドを使用してクラス マップ *class1* に関連付けられ、その後 10-Gigabit Ethernet インターフェイス TenGigE0/1/0/0 の入力方向に付加されます。 すべてのインポーズされたラベルの MPLS EXP ビットは 1 に設定します。

```
class-map match-any class1
  match protocol ipv4
  match access-group ipv4 101

policy-map policy1
  class class1
    set mpls exp imposition 1
 !
interface TenGigE0/1/0/0
  service-policy input policy1
```

（注） **set mpls exp imposition** コマンドは入力ポリシーでのみサポートされています。

MPLS EXP 最上位マーキングの設定：例

次の例では、*policy1* というサービス ポリシーを作成します。 このサービス ポリシーは、**class** コマンドを使用してクラス マップ *class1* に関連付けられ、その後 10-Gigabit Ethernet インターフェ

イス TenGigE0/1/0/0 の出力方向に付加されます。 最上位ラベルの MPLS EXP ビットは 1 に設定します。

```
class-map match-any class1
  match mpls exp topmost 2

policy-map policy1
  class class1
    set mpls exp topmost 1
  !
interface TenGigE0/1/0/0
  service-policy output policy1
```

In-Place ポリシーの変更：例

この例では、ポリシーを定義してインターフェイスに付加した後、precedence を 3 から 5 に変更します。

クラスを定義します。

```
class-map match-any class1
 match cos 7
 end-class-map
```

クラスを使用するポリシー マップを定義します。

```
policy-map policy1
 class class1
 set precedence 3
```

インターフェイスにポリシー マップを付加します。

```
interface gigabitethernet 0/6/0/1
 service-policy output policy1
 commit
```

ポリシー マップの precedence 値を変更します。

```
policy-map policy1
 class class1
 set precedence 5
 commit
```

（注） 変更されたポリシー *policy1* は、ポリシーが付加されるすべてのインターフェイスに反映されます。 また、ポリシーマップに使用するすべてのクラスマップを変更できます。クラスマップに対して行った変更は、ポリシーが付加されているすべてのインターフェイスに反映されます。

この **show policy-map targets** コマンドの出力は、ギガ ビット イーサネット インターフェイス 0/1/0/0に、メインポリシーとして付加されているポリシーマップがあることを示しています（階層型QoS設定の子ポリシーに付加されるのではなく）。 このインターフェイスの発信トラフィックは、ポリシーが変更された場合に影響を受けます。

```
show policy-map targets

Fri Jul 16 16:38:24.789 DST
1) Policymap: policy1    Type: qos
     Targets (applied as main policy):
```

```
  GigabitEthernet0/1/0/0 output
Total targets: 1

Targets (applied as child policy):
Total targets: 0
```

その他の関連資料

ここでは、パケット分類の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
初期システム起動と設定	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
マスター コマンド リファレンス	『*Cisco ASR 9000 Series Aggregation Services Router Master Command Listing*』
QoS コマンド	『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』
ユーザ グループとタスク ID	『Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide』の「Configuring AAA Services on Cisco ASR 9000 Series Router」モジュール

標準

標準	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
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

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
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

第 7 章

モジュラ QoS の導入シナリオ

このモジュールでは、L2VPN または MPLS などの他のテクノロジー ガイドに記載されている特定の QoS 機能または QoS 実装の導入シナリオの使用例について説明します。

ラインカード、SIP および SPA のサポート

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
802.1ad DEI	yes	no
フレーム リレー QoS	no	yes
IPHC QoS	no	2 ポート チャネライズド OC-12c/DS0 SPA のみ
L2VPN QoS	yes	yes
MLPPP/MLFR QoS	no	2 ポート チャネライズド OC-12c/DS0 SPA のみ
MPLS QoS	yes	yes
マルチキャスト VPN での QoS	yes	yes
NxDS0 インターフェイスでの QoS	no	2 ポート チャネライズド OC-12c/DS0 SPA のみ

Cisco ASR 9000 シリーズ ルータの QoS 導入シナリオの機能履歴

リリース	変更内容

リリース 3.7.2	L2VPN QoS 機能が、ASR 9000 イーサネット ラインカードに導入されました。 MPLS QoS 機能が、ASR 9000 イーサネット ラインカードに導入されました。
リリース 3.9.0	MLPPP QoS 機能が、ASR 9000 用 SIP 700 に導入されました。
リリース 3.9.1	マルチキャスト VPN での QoS 機能が、ASR 9000 イーサネット ラインカードに導入されました。
リリース 4.0.0	802.1ad DEI 機能が、ASR 9000 用 SIP 700 に導入されました。 フレーム リレー QoS 機能が、ASR 9000 用 SIP 700 に導入されました。 IP ヘッダー圧縮 QoS 機能が、ASR 9000 用 SIP 700 に導入されました。 L2VPN QoS 機能が、ASR 9000 用 SIP 700 でサポートされました。 MLFR QoS 機能が、ASR 9000 用 SIP 700 に導入されました。 一時停止/再開の方法が MLPPP および MLFR インターフェイスに追加されました。 MPLS QoS 機能が、ASR 9000 用 SIP 700 でサポートされました。 NxDS0 インターフェイスの QoS 機能が、ASR 9000 用 SIP 700 に導入されました。
リリース 4.1.0	VPLS と VPWS QoS 機能が導入されました。

- 802.1ad DEI, 175 ページ
- フレーム リレー QoS, 176 ページ
- IP ヘッダー圧縮の QoS, 179 ページ
- L2VPN QoS, 181 ページ
- MLPPP QoS/MLFR QoS, 183 ページ
- MPLS QoS, 186 ページ
- マルチキャスト VPN での QoS, 191 ページ
- NxDS0 インターフェイスでの QoS, 193 ページ
- VPLS と VPWS QoS, 194 ページ
- 関連情報, 197 ページ

802.1ad DEI

802.1ad フレームと 802.1ah フレームに含まれる Drop Eligible Indicator（DEI）ビットに基づいてトラフィックを分類できます。 DEI のサポートには次の機能が含まれます。

- 特定のレートにポリシングし、トラフィックが適合または超過しているかどうかに基づいて、DEI を 0 または 1 としてマークします。
- 入力に対して、ポリシングを行い、廃棄クラスを設定します（802.1ad カプセル化が設定されていないインターフェイスでも）。
- 出力に対して、廃棄クラス値に基づいて DEI をマーキングします（802.1ad インターフェイスのみ）。

802.1ad フレームと 802.1ah フレームに含まれる Drop Eligible Indicator（DEI）ビットに基づいて輻輳を管理できます。 DEI のサポートには次の機能が含まれます。

- DEI ビットの値に基づいて、重み付けランダム早期検出（WRED）を実行します。
- あるインターフェイスでの輻輳時にトラフィックに優先処理（他より大きなしきい値）を与えることによって、アクティブ キュー管理を行います。あるいは、DEI 値に基づいて不適合なトラフィックに他より小さなしきい値を設定します。

ポリシング アクションに基づく DEI のマーキング：例

この例では、ポリシング レートを 5 Mbps に設定しています。 適合するトラフィックは 0 の DEI 値でマーキングします。ポリシング レートを超過したトラフィックは 1 の DEI 値でマーキングします。

```
policy-map 1ad-mark-dei
class c1
police rate 5 mbps
      conform-action set dei 0
      exceed-action set dei 1
end-policy-map
```

着信フィールドに基づく DEI のマーキング：例

この例では、802.1ad CoS と DEI は、着信する 802.1q CoS から導かれます。 CoS 値が 0 のパケットは、DEI 値 1 でマーキングされます。

```
class-map match-any remark-cos
  match cos 0
end-class-map

policy-map p1
  class remark-cos
  set dei 1
end-policy-map

interface GigabitEthernet0/4/0/39.1 l2transport
```

```
 encapsulation dot1q 1
 rewrite ingress tag push dot1ad 5 symmetric
 service-policy input p1
!
```

DEI を使用する輻輳管理：例

この例では、DEI 値が 0 のパケットをドロップする前に、DEI 値が 1 のパケットをドロップすることで輻輳を管理します。

```
policy-map dei-sample
  class class-default
    random-detect dei 1 1000 6000
    random-detect dei 0 5000 10000
end-policy-map
```

フレーム リレー QoS

フレーム リレー QoS と他のインターフェイス タイプとの主な違いは、以下のことを実行できることです。

- フレーム リレー DLCI の分類
- フレーム リレー DE の分類
- フレーム リレー DE のマーキング

（注） QoS ポリシーは、フレーム リレー サブ インターフェイスの PVC に対してのみ適用できます。フレーム リレー サブ インターフェイスに直接適用することはできません。

フレーム リレー DLCI の分類

この設定では、フレーム リレーでカプセル化されたパケットのフレーム リレー DLCI 値に基づいて照合できます。 フレーム リレーでカプセル化されていないパケットはこの設定に対応しません。

```
class-map foo
            match frame-relay list of dlci-values
```

DLCI 値のリストには、次の例のように、範囲や個々の値を含めることができます。

```
class-map foo
            match frame-relay dlci 1-100 150 200-300
```

（注） DLCI のマッチングはメイン インターフェイスでのみサポートされています。

フレーム リレー DE の分類

この設定では、フレーム リレー ヘッダーに廃棄適性（DE）ビットが設定されているフレーム リレー パケットを照合できます。

```
class-map fr_class
  match fr-de 1
```

フレーム リレー DE ビット 0 を照合するには、次の設定を使用します。

```
class-map match-not-fr-de
 match not fr-de 1
```

（注） DE ビットの分類は、レイヤ 3 インターフェイスではサポートされていません。

フレーム リレー DE のマーキング

この例では、トラフィックがポリシング認定情報レートを超えたときに fr-de ビットを設定します。そのため、（輻輳が発生したとき）下位システムでは fr-de ビットが 1 に設定されたトラフィックを廃棄します。

```
policy-map fr_de_marking
 class class-default
  police rate percent 50
   conform-action transmit
   exceed-action set fr-de 1
  !
 !
 end-policy-map
```

（注） DE ビットのマーキングは、レイヤ 3 インターフェイスではサポートされていません。

フレームリレー QoS：例

この例では、parent_policy をマルチリンク フレーム リレーのメイン インターフェイスに適用します。 フレーム リレー DLCI で一致する parent_policy には 2 つのクラスがあります。 マルチリンク フレーム リレーのメイン インターフェイスには、2 つのフレーム リレー PVC が設定されています（DLCI 16、DLCI 17）。

```
show run int multi 0/2/1/0/1
Mon Aug  2 11:34:31.019 UTC
interface Multilink0/2/1/0/1
 service-policy output parent_policy
 encapsulation frame-relay
 frame-relay intf-type dce
!

show run policy-map parent_policy
```

```
Mon Aug  2 11:34:36.118 UTC
policy-map parent_policy
 class parentQ_1
  service-policy child_queuing_policy
  shape average 64 kbps
 !
 class parentQ_2
  service-policy child_queuing_policy
  shape average 1 mbps
 !
 class class-default
 !
 end-policy-map
!

show run class-map  parentQ_1 <----- class map parent class dlci=16
Mon Aug  2 11:34:43.363 UTC
class-map match-any parentQ_1
 match frame-relay dlci 16
 end-class-map
!

show run class-map  parentQ_2 <----- class map parent class dlci=17
Mon Aug  2 11:34:45.647 UTC
class-map match-any parentQ_2
 match frame-relay dlci 17
 end-class-map
!

show run int multi 0/2/1/0/1.16 <------ dlci 16 pvc config
Mon Aug  2 11:34:53.988 UTC
interface Multilink0/2/1/0/1.16 point-to-point
 ipv4 address 192.1.1.1 255.255.255.0
 pvc 16
  encap cisco
 !
!
show run int multi 0/2/1/0/1.17  <------ dlci 17 pvc config
Mon Aug  2 11:34:56.862 UTC
interface Multilink0/2/1/0/1.17 point-to-point
 ipv4 address 192.1.2.1 255.255.255.0
 pvc 17
  encap cisco
 !
!
show run policy-map child_queuing_policy <--------- child policy-map
Mon Aug  2 11:35:05.821 UTC
policy-map child_queuing_policy
 class voice-ip
  priority level 1
  police rate percent 20
  !
 !
 class video
  bandwidth percent 40
 !
 class premium
  service-policy gchild_policy
  bandwidth percent 10
  random-detect discard-class 2 10 ms 100 ms
  random-detect discard-class 3 20 ms 200 ms
  queue-limit 200 ms
 !
 class best-effort
  bandwidth percent 20
  queue-limit 200 ms
 !
 class class-default
 !
 end-policy-map
!

show run policy-map gchild_policy  <-------- grandchild policy map
```

```
Mon Aug  2 11:35:15.428 UTC
policy-map gchild_policy
 class premium_g1
  police rate percent 10
  !
  set discard-class 2
 !
 class premium_g2
  police rate percent 50
  !
  set discard-class 3
 !
 class class-default
 !
 end-policy-map
!

show run class-map  <----------- shows all class map configs
Mon Aug  2 11:35:19.479 UTC
class-map match-any video
 match precedence 1
 end-class-map
!
class-map match-any premium
 match precedence 2 3
 end-class-map
!
class-map match-any voice-ip
 match precedence 0
 end-class-map
!
class-map match-any parentQ_1
 match frame-relay dlci 16
 end-class-map
!
class-map match-any parentQ_2
 match frame-relay dlci 17
 end-class-map
!
class-map match-any premium_g1
 match precedence 2
 end-class-map
!
class-map match-any premium_g2
 match precedence 3
 end-class-map
!
class-map match-any best-effort
 match precedence 4
 end-class-map
!
```

IP ヘッダー圧縮の QoS

IP ヘッダー圧縮（IPHC）プロファイルはインターフェイス上でイネーブルにできるため、QoS サービス ポリシーと一致するパケットにのみ IPHC プロファイルが適用されます。 この場合、QoS サービス ポリシー クラス属性によって、圧縮するパケットが決定されます。 これにより、ユーザはより IPHC の精度を最適化できます。

ポリシー マップは、**service-policy** コマンドを使用してインターフェイスに割り当てます。 IPHC アクションは、出力サービス ポリシーにだけ適用されます。 IPHC は、入力サービス ポリシーではサポートされません。 （IPHC は入力方向でサポートされていますが、入力ポリシーで IPHC を設定する使用例はありません）。

次のように QoS を使用して IPHC を設定できます

- **compression header ip** アクションで QoS ポリシーを作成します。
- **ipv4 iphc profile** *profile_name* **mode service-policy** コマンドを使用して、IPHC プロファイルをインターフェイスに付加します。
- **service-policy output** コマンドを使用して **compression header ip** アクションが含まれる QoS ポリシーを付加します。

また、次の例に示すように、**show policy-map interface** コマンドを使用して、IPHC の統計情報を表示できます。

```
show policy-map interface Serial0/0/3/0/3:0 output

show policy-map int  Serial0/0/3/0/3:0  output
Mon May 18 22:06:14.698 UTC
Serial0/0/3/0/3:0 output: p1
Class class-default
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                 0/0                   0
    Transmitted         :                 0/0                   0
    Total Dropped       :                 0/0                   0
  Queueing statistics
    Queue ID                               : 0
    High watermark  (Unknown)              : 0
    Inst-queue-len  (packets)              : 0
    Avg-queue-len   (packets)              : 0
    Taildropped(packets/bytes)             : 0/0
  Compression Statistics
    Header ip rtp
    Sent Total       (packets)             : 880
    Sent Compressed  (packets)             : 877
    Sent full header (packets)             : 342
    Saved            (bytes)               : 31570
    Sent             (bytes)               : 24750
    Efficiency improvement factor          : 2.27
```

IP ヘッダー圧縮の QoS：例

この例では、**compress header ip** コマンドを使用し、クラス マップのアクションとしての QoS を通じて、IPHC を設定しています。

パケットはクラス マップの基準に基づいて分類されます。 ポリシー マップでは、クラスに適用する動作を指定します。 IPHC は、クラスに対する **compress header ip** アクションを使用してイネーブルにします。 QoS サービス ポリシーを持つ IPHC プロファイルを、シリアル インターフェイスに適用します。

```
class-map match-all voice1
  match precedence 2
class-map match-all voice2
  match access-group acl_iphc

access-list acl_iphc permit udp any range lower-bound src udp port 5000 upper-bound src udp
 port15000 any lower-bound udp dst port 5000 upper-bound dst udp port 15000

ipv4 access-list acl_iphc permit udp any range 5000 15000 any range 5000 15000

policy-map iphc_policy
 class iphc_class_1
  compress header ip
 class iphc_class_2
  compress header ip
```

```
interface serial 0/1/0/1:1
 ipv4 iphc profile Profile_3 mode service-policy
  service-policy output iphc_policy

interface Serial 0/2/0/0/1/1/1:1
  ipv4 address 10.0.0.1 255.255.255.252
  ipv4 iphc profile Profile_3 mode service-policy
  service-policy output iphc_policy
  encapsulation ppp
```

L2VPN QoS

ここでは、次のフレーム リレー L2VPN の導入シナリオについて説明します。

- フレーム リレー <-> 疑似配線上でのフレーム リレー
- フレーム リレー <-> 疑似配線上でのイーサネット

（注） これらのシナリオの疑似配線を経由しないローカル接続形態もあります。 ここでは、疑似配線シナリオに重点を置いて説明します。

フレーム リレー <-> 疑似配線上でのフレーム リレーの例

この例では、ルータ PE1 の入力フレーム リレー インターフェイスのフレーム リレー DLCI に基づいて照合を行い、fr-de 値を設定できることを示します。 この設定は、L2VPN 疑似配線に引き継がれます。 フレーム リレー パケットがフレーム リレー l2transport インターフェイスを経由してルータ PE2 から出るとき、fr-de 値はそのままです。

この設定を変更し、L2VPN を越えてフレーム リレー QoS 値に引き継ぐことができます。 図 2 に、ネットワーク トポロジを示します。

図 *10*：*MPLS* 上のフレーム リレー

CE1

```
interface pos0/2/0/0.26
 pvc 26
 ipv4 add 10.0.0.1 255.0.0.0
```

PE1

```
interface pos0/2/0/0.26 l2transport
 pvc 26
```

```
l2vpn
 xconnect group frfr
 p2p p1
interface pos0/2/0/0.26
 neighbor y.y.y.y pw-id 1001

!QoS Policy
class-map matchdlci
 match frame-relay dlci 26

policy-map setde1
 class matchdlci
  set fr-de 1

interface pos0/2/0/0
 service-policy input setde1
```

PE2

```
interface pos0/3/0/0.26 l2transport
 pvc 26

l2vpn
 xconnect group frfr
 p2p p1
interface pos0/3/0/0.26
 neighbor x.x.x.x pw-id 1001
```

CE2

```
interface pos0/3/0/0.26
 pvc 26
 ipv4 add 10.0.0.2 255.0.0.0
```

フレーム リレー <-> 疑似配線上でのイーサネット：例

この例では、ルータ PE1 の入力フレーム リレー l2transport インターフェイスの fr-de 値に基づいて照合を行い、特定の MPLS EXP 値を設定できることを示します。 MPLS パケットが PE1 コア インターフェイスを出るとき、この EXP 値が設定されます。 パケットがイーサネット l2transport インターフェイスを経由してルータ PE2 から出るとき、この値はイーサネット パケットの CoS フィールドの値の一部になります。

この設定により、QoS フィールドをフレーム リレー ネットワークからイーサネット ネットワークに引き継ぐ、またはマップできます。 図 3 に、ネットワーク トポロジを示します。

図 *11*：*MPLS* 上の *IP Interworking*

CE1

```
interface pos0/2/0/0.26
```

```
 pvc 26
 ipv4 add 10.0.0.1 255.0.0.0
```

PE1

```
interface pos0/2/0/0.26 l2transport
 pvc 26

l2vpn
 xconnect group freth
 p2p p1
interface pos0/2/0/0.26
 neighbor y.y.y.y pw-id 1001
 interworking ipv4

!QoS Policy
class-map matchfrde
 match fr-de 1

policy-map setexp
 class matchfrde
  set mpls exp imposition 5

interface pos0/2/0/0.26 l2transport
 pvc 26
 service-policy input setexp
```

PE2

```
interface gig0/4/0/0.26 l2transport
 encapsulation dot1q 100

l2vpn
 xconnect group freth
 p2p p1
interface gig0/4/0/0.26
 neighbor x.x.x.x pw-id 1001
 interworking ipv4
```

CE2

```
interface gig0/4/0/0.26
 encapsulation dot1q 100
 ipv4 add 10.0.0.2 255.0.0.0
```

MLPPP QoS/MLFR QoS

マルチリンクとは、複数のシリアル リンクを 1 つのバンドルに集約するメカニズムです。 バンドルにより、より高い帯域幅、リンク間のロードバランシングが可能になり、シングルポイント障害からの保護によりサービスアベイラビリティが向上します。 このサービスで、複数の低速リンクを集約して帯域幅を増やすことができます。1 本の高速リンクにアップグレードするよりも費用対効果に優れています。 これは T1 レートより大きく T3 レートより小さい帯域幅の専用回線サービスを必要とするユーザにとって、費用対効果の高いソリューションです。

マルチリンク インターフェイスは、PPP カプセル化（MLPPP）またはフレーム リレー カプセル化（MLFR）で設定できます。 マルチリンク インターフェイスがフレーム リレー カプセル化で設定されている場合、その下にサブインターフェイスを設定できます。

マルチリンクインターフェイスで使用可能な総帯域幅は、マルチリンクインターフェイスへのリンクの追加や、マルチリンク インターフェイスからのリンクの削除によって動的に変化します。メンバのリンクの状態が動作面でアップまたはダウンに変化した場合や、ポリシーの保留状態を変更することによって、使用可能な総帯域幅も変化します。 このようなインターフェイスに付加されている QoS ポリシーは、帯域幅の変更に基づいて更新する必要があります。 この場合、次のいずれかの操作を実行します。

- ポリシーを保留にする：付加されているポリシーの帯域幅要件が使用可能な帯域幅（メンバリンクが運用面でダウンすると小さくなります）を上回ったときには、ポリシーが保留状態になります。 ポリシーが保留状態になると、そのインターフェイスの着信パケットまたは発信パケットは QoS の影響を受けなくなります。

  次の状況では、入力に対してポリシーは保留状態になります。

  - 拡張階層型の入力ポリシングでは、子ポリシング レートの合計が親ポリシングの適合レートよりも大きい場合
  - ポリシング ピーク レートがポリシング適合レートを下回っている場合

  次の状況では、出力に対してポリシーは保留状態になります。

  - 最小帯域幅レートとプライオリティ クラスのポリシング レートの合計がインターフェイスのレートを上回っている場合
  - シェーピング レートが最小帯域幅レートを下回っている場合
  - プライオリティ クラスのポリシング適合レートがインターフェイスのレートを上回っている場合
  - プライオリティ クラスのポリシング ピーク レートが、インターフェイスのレートを上回っている場合
  - ポリシング ピーク レートがポリシング適合レートを下回っている場合

- ポリシーを再開する：付加されているポリシーの帯域幅要件が使用可能な帯域幅（メンバリンクが運用面でアップすると大きくなります）以下のときには、ポリシーが再開されます。保留中のポリシーは、メンバ リンクのステータスの変化がなくても、ポリシー マップの保留状態を変更することでも再開できます。
- ポリシーを更新する：新しい使用可能な帯域幅を反映するように、アクティブなポリシー レートを更新します。 使用可能な帯域幅は、増加または減少している場合がありますが、適用されているポリシーの帯域幅要件は引き続き満たされています。

QoS 統計情報は、アクティブ状態から保留状態に移行するポリシーについては保持されません。ポリシーを再度アクティブにすると、それまでに収集された統計情報はすべて失われ、再アクティブ化後にインターフェイスを通過したパケットだけがカウントされます。 保留中のポリシーを変更して帯域幅要件を減らし、再アクティブ化することができます。 保留中のポリシーは、インターフェイスに付加したまま変更できます。

QoS を使用するマルチクラス MLPPP

マルチクラスのマルチリンク ポイントツーポイント プロトコル（MLPPP）は、QoS と一緒に使用することができ、ポリシーマップのクラスでの**encap-sequence** コマンドを使用して設定できます。**encap-sequence** コマンドは、MQC 定義クラス内のパケットの MLPPP MCMP クラス ID を指定します。

encap-sequence ID 番号の有効値は、**none**、1、2、または 3 です。 **none** 値は、**priority level** が 1 のときだけ適用でき、MLPPP カプセル化がないことを示します。1、2、または 3 の値は、プライオリティ 1 もしくは 2 のクラスまたはキューイング アクションを含むその他のクラスで使用できます。 ゼロ（0）の **encap-sequence** ID 番号は、システムでのみ使用し、デフォルト クラス用に予約されているため、他のクラスでは使用できません。

（注） **encap-sequence** ID 番号は番号順に設定する必要があります。 たとえば、1 と 2 をすでに割り当てていない限り、ID 番号 3 は割り当てることができません。

encap-sequence ID 番号の数は、マルチリンク ヘッダーによってピア間でネゴシエーションされた MLPPP クラスの数よりも小さくする必要があります。 システムによってこれが確認されないため、ユーザは設定がこれに合っていることを確認する必要があります。

ppp multilink multiclass remote apply コマンドは、これを確認する方法を提供します。**encap-sequence** ID 番号（デフォルト値の 0 を含む）を使用するクラスの数が、**ppp multilink multiclass remote apply** コマンドの *min-number* 値よりも小さいことを確認します。 たとえば、min-number 値が 4 の場合は、encap-sequence ID 番号を持つクラスを 3 つまでしか使用できません。

QoS ポリシーは、次の条件を検証します。 これらの条件が満たされていない場合、ポリシーは拒否されます。

- **encap-sequence** ID 番号が 1～3 という許容値内である。
- **encap-sequence** がポリシー マップ内のいずれかのクラスに設定されている場合は、**priority level 1** を持つポリシー マップ内のすべてのクラスに **encap-sequence** ID 番号を含める必要があります。
- **encap-sequence** が **none** の設定は、**priority level** が 1 のクラスに限定されます。
- class-default には **encap-sequence** 設定は含まれていません。
- キューイング アクションを含むクラスだけが **encap-sequence** 設定を持ちます。

（注） 同じ **encap-sequence** ID 番号を共有するクラスは、プライオリティが同じである必要があります。

QoS ポリシー マップは、次のとおりに設定されます。

```
config
```

```
policy-map type qos policy-name class class-name action action action
. . .
```

次に、MLPPP のポリシー マップを設定する例を示します。

```
config
 policy-map foo
  class ip-prec-1
   encap-sequence none
   police rate percent 10
   priority level 1
 !
  class ip-prec-2
   encap-sequence 1
   shape average percent 80
 !
  class ip-prec-3
   encap-sequence 1
   bandwidth percent 10
 !
  class class-default
 !
 end-policy-map
 !
```

MLPPP QoS/MLFR QoS：例

メンバリンクがアップまたはダウンすると、バンドルインターフェイスの帯域幅は動的に変化するため、このようなインターフェイスに適用されている QoS ポリシーは帯域幅の変更に基づいて更新する必要があります。

MPLS QoS

（注） 導入テキストとトポロジ図は、『MPLS Fundamentals』（Luc De Ghein、Copyright 2007, Cisco Systems, Inc）から引用しました。

MPLS QoS には、均一モード、パイプ モード、およびショート パイプ モードという、トンネリング モデルに基づく 3 つの導入シナリオがあります。 表 2 に、トンネリング モデルの概要を示します。

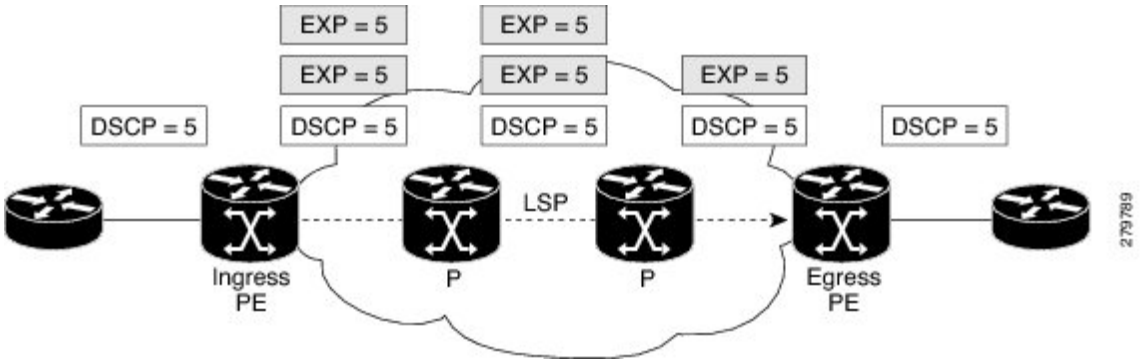
トンネリング モード	IP-to-Label	Label-to-Label	Label-to-IP
Uniform	IP precedence/DiffServ を MPLS EXP にコピー /DiffServ から MPLS EXP へ	コピーされた MPLS EXP	MPLS EXP を IP precedence/DiffServ にコピー
Pipe	サービス プロバイダーのポリシーに応じた MPLS EXP 設定	コピーされた MPLS EXP	IP precedence/DiffServ を保持 /DiffServ MPLS EXP に基づく転送処理

トンネリングモード	IP-to-Label	Label-to-Label	Label-to-IP
Short Pipe	サービスプロバイダーのポリシーに応じた MPLS EXP 設定	コピーされた MPLS EXP	IP precedence/DiffServ を保持 /DiffServ IP precedence/DiffServ に基づく転送処理

MPLS 均一モード

均一モードでは（図 4 に図示）、MPLS ネットワークを通過するときに、パケットに関連する DiffServ マーキングが 1 つだけ存在します。 パケットの DiffServ マーキングが MPLS ネットワーク内で変更された場合、更新情報は LSP の出口で意味のあるものになります。 MPLS ネットワーク内でのパケット マーキングに対するあらゆる変更は永続的であり、パケットが MPLS ネットワークを出るときに伝播されます。

図 *12*：均一モード



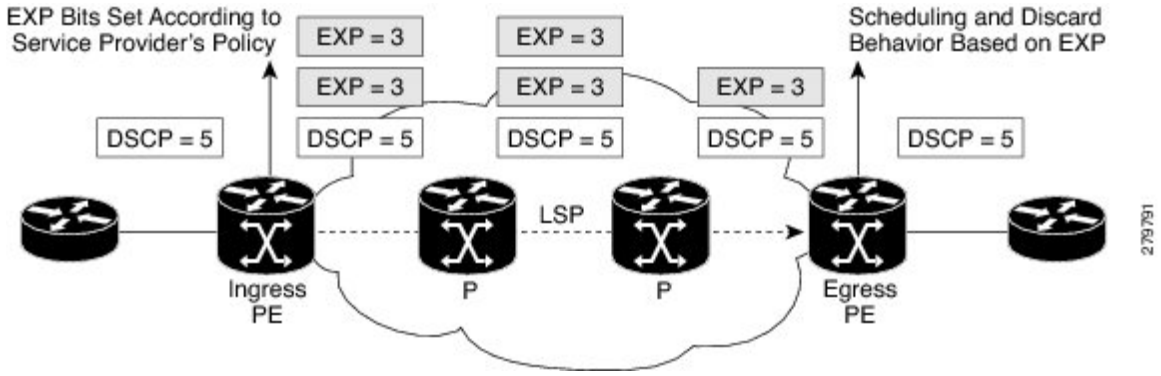
MPLS パイプ モード

パイプ モード（図 5 に図示）では、MPLS ネットワークを通過するときに、2 つのマーキングがパケットに関連します。 1 つめは、出力 LSR を含む LSP スパンに沿って中間ノードによって使用されるマーキングです。 2 つめは、元のマーキングであり、MPLS ネットワークに入る前にパケットによって伝送され、パケットを出た後も継続して使用されます。 MPLS ネットワーク内のパケット マーキングに対するあらゆる変更は、永続的なものではなく、パケットが MPLS ネットワークを出るときに伝播されません。

出力 LSR ではまだ中間 LSR で使用されたマーキングを引き続き使用することに注意してください。 ただし、出力 LSR は、元のパケットにインポーズされたすべてのラベルを削除する必要があります。 ラベルで伝送されるマーキングを維持するために、エッジ LSR は、マーキングの内部コピーを保管してから、ラベルを削除します。 この内部コピーは、ラベルが削除されたあとに、

（CE 方向の）アウトバウンド インターフェイスでパケットを分類するために使用されます。 これは通常、**set qos-group** コマンドと **match qos-group** コマンドを使用して行います。

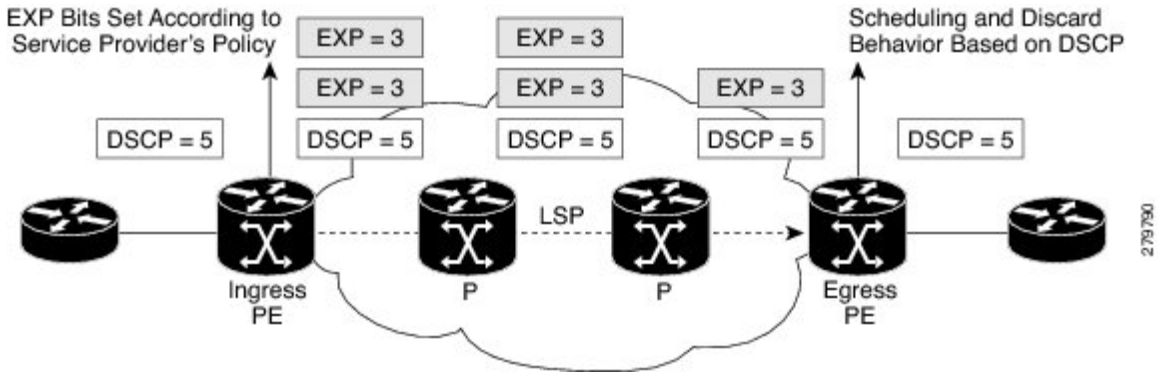
図 *13*：パイプ モード



MPLS ショート パイプ モード

ショートパイプモード（図6に図示）は、パイプモードとわずかに異なります。 唯一の違いは、出力 LSR が中間 LSR によって使用されるマーキングを使用する代わりに元のパケット マーキングを使用することです。

図 *14*：ショート パイプ モード



均一、パイプ、ショート パイプ モード：入力 PE の例

この例では、MPLS DiffServ を実装する方法と、入力 PE で必要な設定について説明します。 precedence 4 のみ一致します。 precedence 4 は、帯域幅が超過しない限り、ポリサーによって EXP ビット値 4 にマップされます。この場合、EXP ビットは値 2 にリカラーされます。 出力インターフェイスの設定は、MPLS DiffServ 均一モデルには不要ですが、EXP ビットに対する QoS の実行方法を示すために追加しています。

```
!Ingress interface:
```

```
class-map prec4
match precedence 4
!
policy-map set-MPLS-PHB
class prec4
police rate 8000 kbps
conform-action set mpls experimental imposition 4
exceed-action set mpls experimental imposition 2
!
interface GigabitEthernet0/0/0/1
service-policy input set-MPLS-PHB

!Egress interface:
class-map exp2and4
match mpls experimental topmost 2 4
!
policy-map output-qos
class exp2and4
bandwidth percent 40
random-detect default
!
interface GigabitEthernet0/0/0/2
service-policy output output-qos
```

均一モード：出力 PE の例

出力 PE では、EXP ビットは **set qos-group** コマンドと **match qos-group** コマンドを使用して precedence ビットにコピーします。

```
!Ingress interface:
class-map exp2
match mpls experimental topmost 2
!
class-map exp4
match mpls experimental topmost 4
!
policy-map policy2
class exp2
set qos-group 2
class exp4
set qos-group 4
!
interface GigabitEthernet0/0/0/2
service-policy input policy2

!Egress interface:
class-map qos2
match qos-group 2
class-map qos4
match qos-group 4
!
policy-map policy3
class qos2
set precedence 2
bandwidth percent 20
random-detect default
class qos4
set precedence 4
bandwidth percent 20
random-detect default
!
interface GigabitEthernet0/0/0/1
service-policy output policy3
```

パイプ モード：出力 PE の例

次に、MPLS DiffServ パイプ モードの出力 PE の設定例を示します。 出力 LSR では発信 IP パケットの precedence ビットに EXP ビットをコピーしません。 出力インターフェイスでのパケットのスケジューリングは、**set qos-group** コマンドと **match qos-group** コマンドを使用して EXP ビットに間接的に行います。

```
!Ingress interface:
class-map exp2
match mpls experimental topmost 2
!
class-map exp4
match mpls experimental topmost 4
!
policy-map policy2
class exp2
set qos-group 2
class exp4
set qos-group 4
!
interface GigabitEthernet0/0/0/2
service-policy input policy2

!Egress interface:
class-map qos2
match qos-group 2
class-map qos4
match qos-group 4
!
policy-map policy3
class qos2
bandwidth percent 20
random-detect default
class qos4
bandwidth percent 20
random-detect default
!
interface GigabitEthernet0/0/0/1
service-policy output policy3
```

ショート パイプ モード：出力 PE の例

次に、MPLS DiffServ ショート パイプ モードの出力 PE の設定例を示します。 出力 LSR では、ラベルを削除した後、IP パケットの precedence または DiffServ コード ポイント（DSCP）ビットに基づいてパケットを転送します。 出力 LSR では発信 IP パケットの precedence ビットに EXP ビットをコピーしません。

```
! Configuration is not needed for ingress interface

!Egress interface:
class-map prec4
match precedence 4
!
policy-map policy3
class prec4
bandwidth percent 40
random-detect precedence 4 100 ms 200 ms
!
interface GigabitEthernet0/0/0/1
service-policy output policy3
```

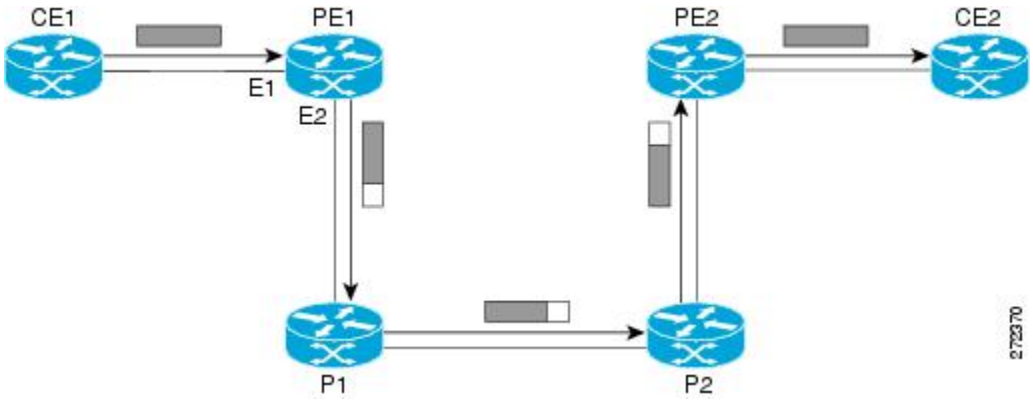
マルチキャスト VPN での QoS

ASR 9000 イーサネット ラインカード

マルチキャスト VPN（mVPN）対応ネットワークでの QoS サービスのサポートには、トンネル IP ヘッダーの DSCP または precedence ビットのマーキングが含まれます。 この機能により、mVPN サービスの QoS を行う MPLS キャリアがイネーブルになります。 mVPN ネットワークでは、プロバイダー エッジ（PE）デバイス間の総称ルーティング カプセル化（GRE）トンネルを使用します。 マルチキャスト パケットは、MPLS コア ネットワーク上で送信するために GRE トンネルに置かれます。

入力インターフェイスでは、入力インターフェイスに適用される入力ポリシー セット内で **set precedence tunnel** コマンドと **set dscp tunnel** コマンド（条件付きと無制限の両方）を使用します。 一般的な mVPN ネットワークを示します。 IP パケットが入力インターフェイス E1 の PE1 に着信すると、GRE トンネル内で IP パケットをカプセル化することによって、パケットがトンネル インターフェイス E2 からコア ネットワークに送信されます。

図 *15*：*mVPN* ネットワーク



set dscp tunnel コマンドまたは **set precedence tunnel** コマンドが入力インターフェイス E1 で設定されている場合、DSCP または precedence 値はインターフェイス E2 から送信されるカプセル化パケットの GRE トンネル ヘッダーに設定されます。 そのため、次の点に注意してください。

- **set dscp** コマンドまたは **set precedence** コマンド（条件付きまたは無条件）により、IP ヘッダー内の DSCP または precedence 値がマークされます。
- **set dscp tunnel** コマンドまたは **set precedence tunnel** コマンド（条件付きまたは無条件）により、GRE ヘッダー内の DSCP または precedence 値がマークされます。

マルチキャスト VPN での QoS：例

mVPN 対応ネットワークで QoS をサポートするには、トンネル ヘッダーに DSCP または precedence ビットの条件付きおよび無条件マーキングが必要です。 無条件マーキングでは、ポリシー アクションとして DSCP または precedence トンネルをマークします。 条件付きマーキングでは、ポリサーのアクションとしてトンネル ヘッダーに DSCP または precedence 値をマークします（適合、超過、または違反）。

無条件マーキング

```
class-map c1
  match vlan 1-10

policy-map p1
 class c1
  set precedence tunnel 3
```

条件付きマーキング

```
policy-map p2
 class c1

  police rate percent 50
  conform action set dscp tunnel af11
  exceed action set dscp tunnel af12
```

ASR 9000 用 SIP 700

set precendence tunnel コマンドおよび **set dscp tunnel** コマンドはサポートされませんが、次の例に示すように一般的なマルチキャスト VPN はサポートされます。

マルチキャスト VPN での QoS：例

この例では、ネットワーク全体で、モバイル、エンタープライズ、およびその他の 3 つのサービスが提供されています。 モバイル トラフィックは、ブロードバンド 2G モバイル トラフィックと 3G モバイル トラフィックとして分類されます。

制御トラフィックには最高のプライオリティが必要であり、プライオリティ レベル 1 を持ちます。 ブロードバンド 2G モバイル トラフィックは、プライオリティ レベル 2 を持ちます。 プライオリティ キューは、これらの各トラフィック クラスに関連付けられます。 これらのクラスのトラフィックは、100 パーセントのレートでポリシングされます。つまり、フル回線レート帯域幅がこれらのトラフィック クラス専用であることを意味します。

残存帯域幅は Mcast_BBTV_Traffic クラス、Enterprise_Traffic クラス、および Enterprise_Low_Traffic クラスに分配されます。

```
policy-map CompanyA-Profile
 class Control_Traffic
```

```
 priority level 1
 police rate percent 100
 !
!
class BB_2GMobile_Traffic
 priority level 2
 police rate percent 100
 !
!
class Mcast_BBTV_Traffic
 bandwidth remaining ratio 1000
!
class 3GMobile_Traffic
 bandwidth remaining ratio 100
!
class Enterprise_Traffic
 bandwidth remaining ratio 10
!
class Enterprise_Low_Traffic
 bandwidth remaining ratio 1
!
class class-default
!
end-policy-map
```

NxDS0 インターフェイスでの QoS

NxDS0 インターフェイスの QoS では、シェーピング、ポリシング、およびキューイングの最小レートは 8 kbps、粒度は 1 kbps です。 QoS が低速 NxDS0 リンクに適用されると、リアルタイム プライオリティ トラフィックに低遅延を行うために、フレーム リレー フラグメンテーション（frf12）設定を行うことを推奨します。 NxDS0 インターフェイスでの一般的な設定は次のとおりです。

- 1 レベルのポリシーが、フレーム リレーの設定のないメイン インターフェイスに適用される
- 2 レベルのポリシーが、フレーム リレーが設定されたサブインターフェイスに適用される

メイン インターフェイスに適用される 1 レベルのポリシー：例

```
show run int Serial0/2/1/0/1/1:0

Mon Aug  9 11:29:50.721 UTC
interface Serial0/2/1/0/1/1:0
 service-policy output fractional_T1_E1_policy fl--------policy applied to serial interface
 encapsulation frame-relay
!

RP/0/RSP1/CPU0:viking-1#show run policy-map
policy-map fractional_T1_E1_policy
 class Conversational
  priority level 1
  police rate 64 kbps
  !
 !
 class Streaming-Interactive
  bandwidth remaining percent 35
 !
 class Background
  bandwidth remaining percent 15
 !
 class TCP-traffic
```

```
 bandwidth remaining percent 10
!
class class-default
bandwidth remaining percent 40
!
end-policy-map
```

サブインターフェイスに適用される 2 レベルのポリシー：例

```
show run int Serial0/2/1/0/1/1:0

Mon Aug  9 11:29:50.721 UTC
interface Serial0/2/1/0/1/1:0
 encapsulation frame-relay
 frame-relay intf-type dce
!

Mon Aug  9 11:29:37.150 UTC
interface Serial0/2/1/0/1/1:0.16 point-to-point
 ipv4 address 192.1.1.1 255.255.255.0
 pvc 16
 service-policy output parent_policy fl--------policy applied to serial subinterface
  encap cisco
  fragment end-to-end 350  fl-------------------frf12 enabled
  !
 !
!

show run policy-map

policy-map parent_policy
 class class-default
  shape average rate 768 kbps

show run policy-map

policy-map fractional_T1_E1_policy
 class Conversational
  priority level 1
  police rate 64 kbps
  !
 !
 class Streaming-Interactive
  bandwidth remaining percent 35
 !
 class Background
  bandwidth remaining percent 15
 !
 class TCP-traffic
  bandwidth remaining percent 10
 !
 class class-default
 bandwidth remaining percent 40
 !
 end-policy-map
```

VPLS と VPWS QoS

1 つまたは複数の Virtual Private Wire Services（VPWS）対応ネットワーク上で、次の一致基準に基づいてパケットを分類できます。

- vpls ブロードキャストとの一致（VPLS に適用可能）

- vpls マルチキャストとの一致（VPLS に適用可能）
- vpls 制御との一致（VPLS に適用可能）
- arp ethertype との一致（VPLS と VPWS の両方に適用可能）

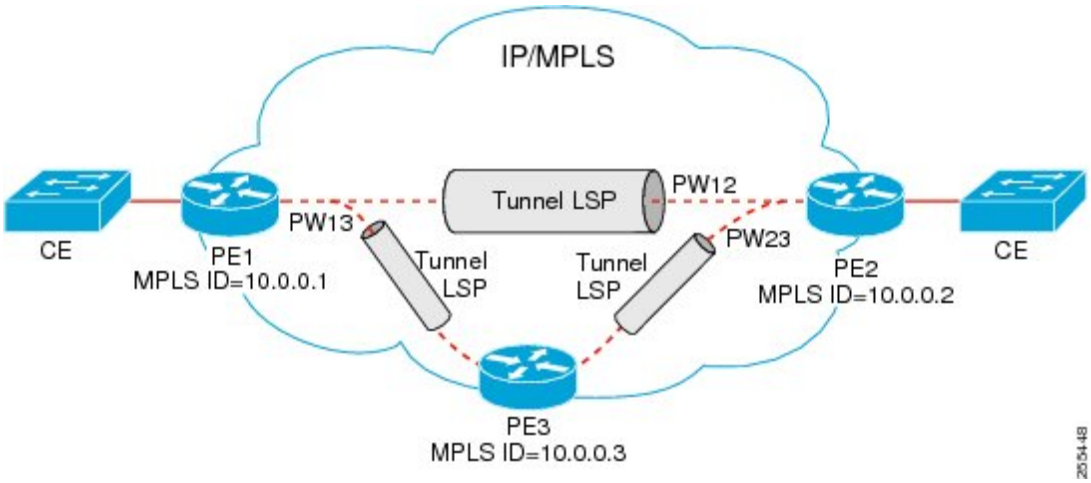
（注） VPLS 固有および VPWS 固有の分類は、入力方向に対してのみ実行されます。

次のガイドラインが、VPLS と VPWS の QoS 機能に適用されます。

- 入力レイヤ 2 バンドルおよび非バンドル サブインターフェイスでサポートされます。
- レイヤ 3 サブインターフェイスではサポートされませんが、ポート継承ポリシーを持つポートではサポートされます。システムは、ポートに対応付けられたレイヤ 3 サブインターフェイスの VPLS の分類を無視します。
- match vpls <control | multicast | broadcast> および match ethertype arp は、レイヤ 2 のサービス タイプに関係なくレイヤ 2 インターフェイスに適用されますが、vpls <control | multicast | broadcast> の分類は非 VPLS レイヤ 2 インターフェイス タイプでは無視されます。

図 9 は標準的な VPLS トポロジを示しています。VPLS ネットワークはルータのドメインをブリッジングするために相互接続された疑似配線（PW）のメッシュです。プロバイダー エッジ（PE）ルータのそれぞれがブリッジ ドメインを持ちます。各 PW は、ブリッジ ドメインに対するブリッジ ポートです。各 PE ルータに対するカスタマー エッジ（CE）接続は、同じブリッジ ドメインに対する接続回線（AC）ブリッジ ポートです。QoS のコンフィギュレーション コマンドは、一方の CE ルータに接続する AC と、他方の PE ルータのブリッジ ドメインに適用されます。

図 *16*：一般的な *VPLS* ネットワーク トポロジ



VPLS と VPWS の QoS：例

ここでは、図 9 に示す構成要素に基づいて設定例を説明し、さらに設定された値に基づいてネットワークでパケットを照合する方法について説明します。

PE1 ルータ上では、次のようにポリシーマップと PE-to-CE 接続が設定されています。

```
class c1
  match vpls multicast
!
class c2
  match vpls broadcast
!
class c3
  match vpls control
!
class c4
  match ethertype arp
!
policy-map p1
  class c1
   set qos-group 3
   set mpls experimental imposition 4
   shape average percent 40
!
  class c2
   bandwidth remaining percent 10
   set mpls experimental imposition 5
!
  class c3
   police rate percent 10
   set mpls experimental imposition 6
!
  class c4
   bandwidth remaining percent 10
   set mpls experimental imposition 7
!
class class-default
!
end policy-map

interface GigabitEthernet0/2/0/0 l2transport
  description PE to CE connection
  service-policy input p1
!

l2vpn
 bridge group examples
  bridge-domain vpls-bridge
   interface GigabitEthernet0/2/0/0
   !
   vfi pe12link
    neighbor 10.0.0.2 pw-id 12
    !
   !
   vfi pe13link
    neighbor 10.0.0.3 pw-id 13
    !
   !
  !
 !
!
```

この例に従い、VPLS と VPWS をイネーブルにして設計および実装されているネットワークでは、一致基準を満たすパケットは、ポリシーに定義されているポリシーアクションに従って QoS の処理を受けます。

- VPLS のマルチキャスト パケットが PE ルータの入力インターフェイスに着信すると、クラス c1 に一致します。
- VPLS のブロードキャスト パケットが PE ルータの入力インターフェイスに着信すると、クラス c2 に一致します。
- VPLS 制御パケットが、MAC アドレスの範囲が 01-80-C2-00-00-00 ～ 01-80-C2-00-00-3F の PE ルータの入力インターフェイスに着信すると、クラス c3 に一致します。
- ARP パケットが PE ルータの入力インターフェイスに着信すると、クラス c4 に一致します。

関連情報

このモジュールでは、他のテクノロジー ガイドに記載されている機能での QoS 実装について説明します。 次の表に、これらの機能の詳細を入手できるマニュアルを示します。

機能	ガイド
802.1ad DEI	このマニュアルの「モジュラ QoS パケット分類とマーキングの設定」および「モジュラ QoS の輻輳管理の設定」
フレーム リレー	『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*』 『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Command Reference*』
IP ヘッダー圧縮	『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*』 『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Command Reference*』
L2VPN	『*Cisco ASR 9000 Series Aggregation Services Router L2VPN*』および『*Ethernet Services Configuration Guide*』 『*Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Command Reference*』
MLPPP/MLFR	『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*』 『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Command Reference*』

機能	ガイド
MPLS	『*Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide*』 『*Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference*』
マルチキャスト VPN での QoS	『*Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide*』 『*Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference*』
NxDS0 インターフェイスでの QoS	『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*』 『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Command Reference*』

第 8 章

階層型モジュラ QoS の設定

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

ラインカード、SIP および SPA のサポート

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
拡張階層型の入力ポリシング	no	yes
階層型ポリシング	yes	yes
階層型 QoS	yes	yes
3 つのパラメータによるスケジューラ	yes	yes

Cisco ASR 9000 シリーズ ルータの階層型 QoS の機能履歴

リリース	変更内容
リリース 3.7.1	階層型ポリシング機能が、ASR 9000 イーサネット ラインカードの Cisco ASR 9000 シリーズ ルータで導入されました。 階層型 QoS 機能が、ASR 9000 イーサネット ラインカードの Cisco ASR 9000 シリーズ ルータで導入されました。 3 パラメータ スケジューラ機能が、ASR 9000 イーサネット ラインカードの Cisco ASR 9000 シリーズ ルータで導入されました。
リリース 3.9.0	階層型 QoS 機能は、ASR 9000 用 SIP 700 でサポートされるようになりました。 （2 レベルのポリシーのみ）

リリース 4.0.0	拡張階層型入力ポリシング機能が、ASR 9000 に対する SIP 700 の Cisco ASR 9000 シリーズ ルータで導入されました。 階層型ポリシング機能が、ASR 9000 に対する SIP 700 の Cisco ASR 9000 シリーズ ルータでサポートされました。 階層型 QoS 機能については、ASR 9000 用 SIP 700 で 3 レベル ポリシーのサポートが追加されました。 3 つのパラメータによるスケジューラ機能が、ASR 9000 用 SIP 700 でサポートされるようになりました。

- 階層型 QoS の設定方法，200 ページ
- 階層型ポリシー設定の確認，217 ページ
- その他の関連資料，218 ページ

階層型 QoS の設定方法

階層型 QoS を設定する場合は、次の注意事項に従ってください。

- ポリシーを定義する場合は、階層の最下位から開始します。 たとえば、2 レベルの階層型ポリシーには、最下位ポリシーの後で最上位ポリシーを定義します。 3 レベルの階層型ポリシーでは、最下位ポリシー、中位ポリシー、最上位ポリシーの順に定義します。
- 最上位ポリシー内に最下位ポリシーを設定する際、service-policy コマンドで input または output キーワードを指定しないでください。
- 中位および最上位ポリシーだけに最下位ポリシーを設定します。

3 つのパラメータによるスケジューラの設定

3 つのパラメータによるスケジューラを設定する場合は、次の注意事項に従ってください。

- 3 つのパラメータによるスケジューラを使用するには、キューイング クラスをイネーブルにする必要があります。 キューイング クラスをイネーブルにするには、3 つのパラメータのうち少なくとも 1 つを設定する必要があります。 少なくとも 1 つのパラメータを設定すると、キューがクラスに割り当てられます。
- 1 つのパラメータだけを設定すると、スケジューラは他の 2 つのパラメータにデフォルト値を使用します。
- 3 つのパラメータすべてを同じクラスに設定できます。
- 最小帯域幅は、最大帯域幅未満でなければなりません。

ASR 9000 イーサネット ラインカード

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **shape average** {**percent** *percentage* | *rate* [*units*]}
5. **exit**
6. **policy-map** *policy-name*
7. **class class-default**
8. **bandwidth** {*rate* [*units*] | **percent** *percentage-value*} **or bandwidth remaining** [**percent** *percentage-value* | **ratio** *ratio-value*] **or shape average** {**percent** *percentage* | *rate* [*units*]}
9. **service-policy** *policy-map-name*
10. end
11. または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map bottom-child`	最下位ポリシーを作成または変更します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class Bronze`	指定するトラフィック クラスをポリシーマップに割り当てます。 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 4	**shape average** {**percent** *percentage*	*rate* [*units*]} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# shape average 1 mbps`	表示されたビット レートにトラフィックをシェーピングします。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `RP/0/RSP0/CPU0:router(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 6	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# policy-map Top-Parent`	最上位ポリシーを作成または変更します。
ステップ 7	**class class-default** 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class-default`	親 class-default クラスを設定または変更します。 （注） • 親ポリシーの class-default クラスは 1 つだけ設定できます。 他のトラフィック クラスは設定しないでください。

ステップ 8	**bandwidth** {*rate* [*units*] | **percent** *percentage-value*} **or bandwidth remaining** [**percent** *percentage-value* | **ratio** *ratio-value*] **or shape average** {**percent** *percentage* | *rate* [*units*]}
	例：
	`RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth percent 30`
	`or`
	`RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 80`
	`or`
	`RP/0/RSP0/CPU0:router(config-pmap-c)# shape average percent 50`
		クラスに割り当てられた最小帯域幅をリンク帯域幅の割合で指定します。
		クラスに超過帯域幅を割り当てる方法を指定します。
		（他のクラスがすべての帯域幅共有を使用していない場合）最大帯域幅をリンク帯域幅の割合で指定します。
		（注） • 3 つのパラメータの少なくとも 1 つを設定する必要があります。

ステップ 9	**service-policy** *policy-map-name* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# service-policy Bottom-Child`	最上位 class-default クラスに最下位ポリシーを適用します。
ステップ 10	end	
ステップ 11	または **commit** 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# end`	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:

	コマンドまたはアクション	目的
	または `RP/0/RSP0/CPU0:router(config-pmap-c)# commit`	**yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ASR 9000 用 SIP 700

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **bandwidth** {*rate* [*units*] | **percent** *percentage-value*} **or bandwidth remaining** [**percent** *percentage-value* | **ratio** *ratio-value*] **or shape average** {**percent** *percentage* | *rate* [*units*]}
5. **exit**
6. **policy-map** *policy-name*
7. **class class-default**
8. **shape average** {**percent** *percentage* | *rate* [*units*]}
9. **service-policy** *policy-map-name*
10. end
11. または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map bottom-child`	最下位ポリシーを作成または変更します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class Bronze`	指定するトラフィック クラスをポリシーマップに割り当てます。 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 4	**bandwidth** {*rate* [*units*] | **percent** *percentage-value*} **or bandwidth remaining** [**percent** *percentage-value* | **ratio** *ratio-value*] **or shape average** {**percent** *percentage* | *rate* [*units*]}
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth percent 30`
	`or`
	`RP/0/RSP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 80`
	`or`
	`RP/0/RSP0/CPU0:router(config-pmap-c)# shape average percent 50`
		クラスに割り当てられた最小帯域幅をリンク帯域幅の割合で指定します。
		クラスに超過帯域幅を割り当てる方法を指定します。
		（他のクラスがすべての帯域幅共有を使用していない場合）最大帯域幅をリンク帯域幅の割合で指定します。
		（注） • 3 つのパラメータの少なくとも 1 つを設定する必要があります。

ステップ 5	**exit** 例： `RP/0/RSP0/CPU0:router(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 6	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# policy-map Top-Parent`	最上位ポリシーを作成または変更します。

	コマンドまたはアクション	目的
ステップ 7	**class class-default** 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class-default`	親 class-default クラスを設定または変更します。 （注） • 親ポリシーの class-default クラスは 1 つだけ設定できます。他のトラフィック クラスは設定しないでください。
ステップ 8	**shape average** {**percent** *percentage* | *rate* [*units*]} 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# shape average 1 mbps`	（任意）指定ビット レートにトラフィックをシェーピングします。
ステップ 9	**service-policy** *policy-map-name* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# service-policy Bottom-Child`	最上位 class-default クラスに最下位ポリシーを適用します。
ステップ 10	end	

ステップ 11	または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-pmap-c)# **end**`
	または
	`RP/0/RSP0/CPU0:router(config-pmap-c)# **commit**`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーションセッションで継続されます。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

物理および仮想リンクへの階層型ポリシーの付加

階層型ポリシーをインターフェイス、サブインターフェイス、仮想回線、および仮想LANに付加するには、**service-policy** {**input** | **output**} *policy-map-name* コマンドを使用します。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **service-policy {input | output}** *policy-map-name*
4. end
5. または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config)# interface pos 0/2/0/0`	階層型ポリシーを付加するインターフェイスを指定します。
ステップ 3	**service-policy {input | output}** *policy-map-name* 例： `RP/0/RSP0/CPU0:router(config-if)# service-policy input All_Traffic`	指定したポリシー マップを付加します。 • **input**：着信パケットに QoS ポリシーを適用します。 • **output**：送信パケットに QoS ポリシーを適用します。 • *policy-map-name*：設定済み最上位ポリシー マップの名前。
ステップ 4	end	

ステップ 5	または **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-pmap-c)# end`
	または
	`RP/0/RSP0/CPU0:router(config-pmap-c)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。

	コマンドまたはアクション	目的
		no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、ルータは現在のコンフィギュレーションセッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

拡張階層型入力ポリシングの設定

拡張階層型入力ポリシングの設定と階層型入力ポリシングの設定の違いは、child-conform-aware コマンドが追加されていることです。

親ポリサーで使用すると、child-conform-aware コマンドは親ポリサーが子ポリサーで指定される最大レートに適合する入力トラフィックをドロップしないようにします。

制約事項

拡張階層型入力ポリシングには次の制限があります。

- 入力方向のみ。
- すべての子ポリサー レートの合計は親ポリサー レートを超えることはできません。
- シングル レート、2 カラー ポリサー（カラー ブラインド）のみ。
- **police rate** コマンドでバースト サイズを指定する設定がサポートされています。ピーク バーストを指定する設定はシングル レート 3 カラー ポリサーになり、拒否されます。
- **child-conform-aware** コマンドは親ポリサーだけで設定します。

手順の概要

1. **configure**
2. **policy-map** *policy-name*
3. **class** *class-name*
4. **service-policy** *policy-map-name*
5. **police rate** {*value* [*units*] | **percent** *percentage*} [**burst** *burst-size* [*burst-units*]] [**peak-rate** *value* [*units*]] [**peak-burst** *peak-burst* [*burst-units*]]
6. **child-conform-aware**
7. **conform-action** [**drop** | **set** *options* | **transmit]**
8. **exceed-action** [**drop** | **set** *options* | **transmit**]
9. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 2	**policy-map** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# policy-map parent`	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。 1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
ステップ 3	**class** *class-name* 例： `RP/0/RSP0/CPU0:router(config-pmap)# class class-default`	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。 ポリシーを作成または変更するクラスの名前を指定します。
ステップ 4	**service-policy** *policy-map-name* 例： `RP/0/RSP0/CPU0:router(config-pmap-c)# service-policy child`	親 class-default クラスに最下位ポリシー マップを適用します。 （注） • input または output キーワードを指定しないでください。
ステップ 5	**police rate** {*value* [*units*]	**percent** *percentage*} [**burst** *burst-size* [*burst-units*]] [**peak-rate** *value* [*units*]] [**peak-burst** *peak-burst* [*burst-units*]]	トラフィック ポリシングを設定し、ポリシー マップ 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。

	コマンドまたはアクション	目的
	例： `RP/0/RSP0/CPU0:router(config-pmap-c)# police rate percent 50`	
ステップ 6	**child-conform-aware** 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# child-conform-aware`	親ポリサーが子ポリサーで指定される最大レートに適合する入力トラフィックをドロップしないようにします。
ステップ 7	**conform-action** [**drop** | **set** *options* | **transmit**] 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# conform-action transmit`	レート制限に適合したパケットに対して実行するアクションを設定します。 可能なアクションは次のとおりです。 **transmit**：パケットを送信します。
ステップ 8	**exceed-action** [**drop** | **set** *options* | **transmit**] 例： `RP/0/RSP0/CPU0:router(config-pmap-c-police)# exceed-action drop`	レート制限を超過したパケットに対して実行するアクションを設定します。 可能なアクションは次のとおりです。 **drop**：パケットをドロップします。

ステップ 9	**end** または **commit**
	例：
	`RP/0/RSP0/CPU0:router(config-pmap-c-police)# end`
	または
	`RP/0/RSP0/CPU0:router(config-pmap-c-police)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
		yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		no と入力すると、コンフィギュレーションセッションが終了して、ルータがEXECモードに戻ります。変更はコミットされません。
		cancel と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

	コマンドまたはアクション	目的

2 レベルの階層型キューイング ポリシー：例

次に、マルチリンク フレーム リレー メイン インターフェイスに適用される 2 レベルのポリシーの例を示します。同じポリシーは、マルチリンク PPP メイン インターフェイスに適用できます。

```
class-map match-any video
 match precedence 1
 end-class-map
!
class-map match-any premium
 match precedence 2 3
 end-class-map
!
class-map match-any voice-ip
 match precedence 0
 end-class-map
!
class-map match-any best-effort
 match precedence 4
 end-class-map

policy-map parent_shape
 class class-default
  service-policy child_policy
  shape average percent 90
 !
 end-policy-map
!

policy-map child_policy
 class voice-ip
  priority level 1
  police rate percent 20
  !
 !
 class video
  bandwidth percent 40
 !
 class premium
  bandwidth percent 10
  random-detect precedence 2 10 ms 100 ms
  random-detect precedence 3 20 ms 200 ms
  queue-limit 200 ms
 !
 class best-effort
  bandwidth percent 20
  queue-limit 200 ms
 !
 class class-default
 !
 end-policy-map
!

interface Multilink0/2/1/0/1
 service-policy output parent_shape
 encapsulation frame-relay
 frame-relay intf-type dce
```

3 レベル階層型キューイング ポリシー：例

3 レベル階層型キューイング ポリシー：例

この例では、ポリシー grand-parent はメイン イーサネット インターフェイスに適用されます。 親の親ポリシーは、500 Mbps までのインターフェイスのすべての発信トラフィックを制限します。 親ポリシーにクラス vlan1 および vlan2 があり、vlan1 または vlan2 のトラフィックは 500 Mbps の 40 % に制限されます。 ポリシー child_policy はさまざまなサービスに基づいてトラフィックを分類し、それに応じて各クラスの帯域幅を割り当てます。

```
class-map match-any video
 match precedence 1
 end-class-map
!
class-map match-any premium
 match precedence 2 3
 end-class-map
!
class-map match-any voice-ip
 match precedence 0
 end-class-map
!
class-map match-any best-effort
 match precedence 4
 end-class-map

class-map match-any vlan1
 match vlan 1
 end-class-map

class-map match-any vlan2
 match vlan 2
 end-class-map

policy-map grand-parent
class class-default
 shape average 500 Mbps
 service-policy parent
 !
 end-policy-map

policy-map parent
 class vlan1
  service-policy child_policy
  shape average percent 40
 !
 class vlan2
  service-policy child_policy
  shape average percent 40
 !
 end-policy-map
!

policy-map child_policy
 class voice-ip
  priority level 1
  police rate percent 20
  !
 !
 class video
  bandwidth percent 40
 !
 class premium
  bandwidth percent 10
```

```
  random-detect precedence 2 10 ms 100 ms
  random-detect precedence 3 20 ms 200 ms
  queue-limit 200 ms
 !
 class best-effort
  bandwidth percent 20
  queue-limit 200 ms
 !
 class class-default
 !
 end-policy-map

 interface GigabitEthernet0/0/0/9
 service-policy output grand-parent
```

ASR 9000 用 SIP 700

この例では、parent_policy ポリシーは、マルチリンク フレーム リレー メイン インターフェイスに適用されます。 ポリシー parent_policy にはフレーム リレー DLCI で一致する 2 つのクラスがあります。 マルチリンク フレーム リレーのメイン インターフェイスには、2 つのフレーム リレー PVC が設定されています（DLCI 16、DLCI 17）。

```
interface Multilink0/2/1/0/1
 mtu 1504
 service-policy output parent_policy
 encapsulation frame-relay
 frame-relay intf-type dce
!

policy-map parent_policy
 class parentQ_1
  service-policy child_queuing_policy
  shape average 64 kbps
 !
 class parentQ_2
  service-policy child_queuing_policy
  shape average 1 mbps
 !
 class class-default
 !
 end-policy-map
!

class-map match-any parentQ_1 <----- class map parent class dlci=16
 match frame-relay dlci 16
 end-class-map
!

class-map match-any parentQ_2 <----- class map parent class dlci=17
 match frame-relay dlci 17
 end-class-map
!

interface Multilink0/2/1/0/1.16 point-to-point <------ dlci 16 pvc config
 ipv4 address 192.1.1.1 255.255.255.0
 pvc 16
  encap cisco
 !
!
interface Multilink0/2/1/0/1.17 point-to-point <------ dlci 17 pvc config
 ipv4 address 192.1.2.1 255.255.255.0
 pvc 17
  encap cisco
 !
!
policy-map child_queuing_policy <--------- child policy map
 class voice-ip
```

```
  priority level 1
  police rate percent 20
  !
 !
 class video
  bandwidth percent 40
 !
 class premium
  service-policy gchild_policy
  bandwidth percent 10
  random-detect discard-class 2 10 ms 100 ms
  random-detect discard-class 3 20 ms 200 ms
  queue-limit 200 ms
 !
 class best-effort
  bandwidth percent 20
  queue-limit 200 ms
 !
 class class-default
 !
 end-policy-map
!

policy-map gchild_policy <-------- grandchild policy map
 class premium_g1
  police rate percent 10
  !
  set discard-class 2
 !
 class premium_g2
  police rate percent 50
  !
  set discard-class 3
 !
 class class-default
 !
 end-policy-map
!

show run class-map  <----------- shows all class-map configs
Mon Aug  2 11:35:19.479 UTC
class-map match-any video
 match precedence 1
 end-class-map
!
class-map match-any premium
 match precedence 2 3
 end-class-map
!
class-map match-any voice-ip
 match precedence 0
 end-class-map
!
class-map match-any parentQ_1
 match frame-relay dlci 16
 end-class-map
!
class-map match-any parentQ_2
 match frame-relay dlci 17
 end-class-map
!
class-map match-any premium_g1
 match precedence 2
 end-class-map
!
class-map match-any premium_g2
 match precedence 3
 end-class-map
!
class-map match-any best-effort
 match precedence 4
 end-class-map
```

3 つのパラメータによるスケジューラ：例

3 つのパラメータによるスケジューラ：例

次に、2 レベルの階層型ポリシーに 3 つのパラメータによるスケジューラを設定する例を示します。

```
policy-map Bottom-ChildA
class A1
      shape average 400 kbps
class A2
     shape average 400 kbps

policy-map Bottom-ChildB
class B1
      shape average 250 kbps
class B2
     shape average 450 kbps

policy-map Top-Parent
 class parentA
  shape average 500 kbps
  bandwidth percent 30
  bandwidth remaining percent 80
 service-policy Bottom-ChildA
class parentB
  shape average 500 kbps
  bandwidth percent 60
  bandwidth remaining percent 10
 service-policy Bottom-ChildB
```

ASR 9000 用 SIP 700

次に、2 レベルの階層型ポリシーに 3 つのパラメータによるスケジューラを設定する例を示します。

```
policy-map Bottom-Child
 class A
   bandwidth percent 30
   bandwidth remaining percent 80
   shape average percent 50
 class B
   bandwidth percent 60
   bandwidth remaining percent 10
class class-default
exit

policy-map Top-Parent
 class-default
   shape average 1 mbps
 service-policy Bottom-Child
```

階層型ポリシング：例

階層型ポリシング：例

次に、各レベルでポリシング アクションを持つ 2 レベルのポリシーの例を示します。 最上位に 2 つのクラスがあり、顧客ごとに 1 つです。 各顧客からの集約されたトラフィックは、最上位の **police rate** コマンドで指定されたレート制限が適用されます。 最下位の各クラスのトラフィックは、追加の一連のポリシング アクションによって、顧客ごとに異なるタイプのトラフィックを制御するように制限されています。

```
class-map match-any customera
 match vlan 10-14
class-map match-any customerb
 match vlan 15-19
class-map match-any prec1
 match precedence 1
class-map match-any prec3
 match precedence 3

policy-map parent
 class customera
  service-policy childa
  bandwidth remaining ratio 10
  police rate percent 50
    conform-action transmit
    exceed-action drop
 class customerb
  service-policy childb
  bandwidth remaining ratio 100
  police rate percent 70
    conform-action transmit
    exceed-action drop

policy-map childa
 class prec1
  police rate percent 25
  conform-action transmit
  exceed-action drop
 class prec3
  police rate percent 25
   conform-action transmit
   exceed-action drop

policy-map childb
 class prec1
  police rate percent 30
  conform-action transmit
  exceed-action drop
 class prec3
  police rate percent 30
   conform-action transmit
   exceed-action drop
```

ASR 9000 用 SIP 700

この例では、ポリサーは Prec1 および Prec3 クラスのポリシー child で、およびポリシー parent の class-default で指定されます。 子ポリシーのポリサーは、クラス Prec1 のトラフィックを（50 % のうち）30 % でポリシングし、クラス Prec3 のトラフィックを（50 % のうち）60 % でポリシングし、その他のトラフィックを（50 % のうち）10 % でポリシングします。 累積方式で、インター

フェイスのすべてのトラフィックは親ポリシーのポリサーによってインターフェイス レートの50 % でポリシングされます。

```
class-map match-any prec1
    match precedence 1

class-map match-any prec3
    match precedence 3

policy-map parent
    class class-default
       service-policy child
           police rate percent 50
        conform-action transmit
        exceed-action drop
policy-map child
    class prec1
       police rate percent 30
           conform-action transmit
           exceed-action drop
    class prec3
       police rate percent 60
           conform-action transmit
           exceed-action drop
    class class-default
       police rate percent 10
           conform-action transmit
           exceed-action drop
```

物理および仮想リンクへのサービス ポリシーの付加：例

物理リンク：例

この例では、ポリシー p1 はギガビット イーサネット インターフェイスに適用されます。

```
interface gigabitethernet 0/2/0/0
service-policy input p1
```

仮想リンク：例

この例では、p2 ポリシーは、マルチリンク フレーム リレー サブインターフェイス下のプライベート仮想回線（PVC）に適用されます。 QoS ポリシーは、フレーム リレー サブ インターフェイスの PVC に対してのみ適用できます。フレーム リレー サブ インターフェイスに直接適用することはできません。

```
interface Multilink0/2/1/0/1.16 point-to-point
 encapsulation frame-relay
 ipv4 address 192.1.1.1 255.255.255.0
 pvc 16
  service-policy output p2
  encap cisco
```

拡張階層型の入力ポリシング：例

次に、2 つのクラスが子ポリシーに定義された親と子ポリシーの例を示します。 クラス AF1 では、exceed アクションがトラフィックをドロップする以外のアクションに設定されます。

child-conform-aware コマンドが親ポリシーで設定されていない場合、親ポリサーは子ポリサーの適合レートと一致し、親ポリサーの適合レートを超過するトラフィックをドロップします。

親ポリサーで使用すると、child-conform-aware コマンドは親ポリサーが子ポリサーで指定した認定レートに適合する入力トラフィックをドロップしないようにします。

この例では、子ポリシーのクラス EF が 1 Mbps の認定レート、conform アクション、exceed アクションで設定されます。 1 Mbps 未満のトラフィックは MPLS EXP ビットが 4 に設定された親ポリサーが適用され、1 Mbps を超えるトラフィックはドロップされます。

子ポリシーのクラス AF1 は 1 Mbps の認定レート、conform アクション、exceed アクションで設定されます。 1 Mbps 未満のトラフィックは MPLS EXP ビットが 3 に設定された親ポリサーが適用され、1 Mbps を超えるトラフィックは MPLS EXP ビットが 2 に設定された親ポリシーが適用されます。

この子ポリシーを設定すると、親ポリサーは子クラスのトラフィックが 2 Mbps の認定レートを超えていると見なします。 親ポリサーの **child-conform-aware** コマンドがない場合、親は 2 Mbps にポリシングします。これにより、子ポリシーのクラス EF から一部の適合トラフィックがドロップされることがあります。 **child-conform-aware** コマンドが親ポリサーに設定されている場合、親ポリサーは、子ポリシーで適合するトラフィックをドロップしません。

```
policy-map parent
  class class-default
    service-policy child
    police rate 2 mbps
      child-conform-aware
      conform-action transmit
      exceed-action drop

policy-map child
  class EF
    police rate 1 mbps
      conform-action set mpls experimental imposition 4
      exceed-action drop
  class AF1
    police rate 1 mbps
      conform-action set mpls experimental imposition 3
      exceed-action set mpls experimental imposition 2
```

階層型ポリシー設定の確認

階層型ポリシーを確認するには、特権 EXEC モードで次のいずれかのコマンドを入力します。

show policy-map interface	指定されたインターフェイス上のすべてのサービスポリシーに対して設定されている全クラスのポリシー設定情報を表示します。

show qos interface	指定したインターフェイスに適用されているサービス ポリシーの全クラスの QoS 情報を表示します。
show running-config class-map	ルータに設定されているすべてのクラスマップ設定を表示します。
show running-config policy-map	ルータに設定されているすべてのポリシーマップ設定を表示します。
show running-config policy-map policy-map-name	指定するポリシーマップに含まれるすべてのクラスの設定を表示します。

その他の関連資料

ここでは、階層型 QoS の実装に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
初期システム起動と設定	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
マスター コマンド リファレンス	『*Cisco ASR 9000 Series Aggregation Services Router Master Command Listing*』
QoS コマンド	『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』
ユーザ グループとタスク ID	『Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide』の「Configuring AAA Services on Cisco ASR 9000 Series Router」モジュール

標準

標準	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
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

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
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

第 9 章

リンク バンドルのモジュラ QoS の設定

リンク バンドルは、1 つ以上のポートを集約したグループで、1 つのリンクとして扱われます。このモジュールでは、リンク バンドルの QoS について説明します。

ラインカード、SIP および SPA のサポート

機能	ASR 9000 イーサネット ラインカード	ASR 9000 用 SIP 700
リンク バンドルの QoS	yes	yes

Cisco ASR 9000 シリーズ ルータのリンク バンドルでの QoS 設定の機能履歴

リリース	変更内容
リリース 3.9.0	リンク バンドルの QoS 機能が、ASR 9000 イーサネット ラインカードに導入されました。

リンク バンドルの概要

リンク バンドル機能を使用すると、複数のポイントツーポイント リンクを 1 つの論理リンクにグループ化して、2 台のルータ間により高い双方向帯域幅、冗長性とロード バランシングを提供で

きます。 仮想インターフェイスは、バンドル リンクに割り当てられます。 コンポーネント リンクは仮想インターフェイスに動的に追加および削除できます。

仮想インターフェイスは、IP アドレスやリンク バンドルで使用されるその他のソフトウェア機能を設定できる、単一のインターフェイスとして扱われます。 リンク バンドルに送信されたパケットは、バンドル内のリンクの 1 つに転送されます。

リンク バンドルは、1 つに束ねられたポートのグループであり、1 つのリンクとして振る舞います。 リンク バンドルには次のような利点があります。

- 複数のリンクが複数のラインカードにまたがり、1 つのインターフェイスを形成します。 そのため、単一のリンクで障害が発生しても接続性は失われません。
- バンドルされたインターフェイスでは、バンドルの使用可能なすべてのメンバにわたってトラフィックが転送されるため、帯域幅の可用性が向上します。 したがって、バンドル内のリンクの 1 つで障害が発生した場合、トラフィックは使用可能なリンクを通過できます。 パケット フローを中断することなく、帯域幅を追加できます

1 つのバンドル内の個別リンクは、すべて同じタイプと同じ速度でなければなりません。

Cisco IOS XR ソフトウェアは、次のイーサネット インターフェイスのバンドルを形成する方法をサポートしています。

- IEEE 802.3ad：バンドル内のすべてのメンバー リンクの互換性を確保するため、Link Aggregation Control Protocol（LACP）を採用した標準テクノロジー。 互換性がないリンクや障害になったリンクは、バンドルから自動的に削除されます。
- EtherChannel：ユーザがリンクを設定してバンドルに参加させることができるシスコの専用テクノロジー。バンドル内のリンクに互換性があるかどうかを確認するための仕組みはありません

ロード バランシング

ロード バランシングは、バンドル内のすべてのリンクでサポートされています。 ロード バランシング機能は、ルータのレイヤ 3 ルーティング情報に基づいて、複数のリンクにトラフィックを分散する転送メカニズムです。 次の 2 種類のロード バランシング方式があります。

- 宛先別ロード バランシング
- パケット単位のロード バランシング

トラフィック ストリームがルータに着信すると、パケット単位のロードバランシングによって、トラフィックが均等に複数の等コスト リンク間に分散されます。パケット単位の方式では、個々の送信元/宛先ホストに関係なく、ラウンド ロビン技法に基づいてルーティングの決定を行います。

宛先別ロード バランシングだけがサポートされています。

宛先別ロード バランシングでは、ルータがバンドル リンクの 1 つにパケットを分散して、ロード シェアリングを行います。 この方法では、送信元/宛先アドレスとユーザ セッションに基づくハッシュ計算を利用します。

宛先別ロード バランシングがイネーブルの場合、使用可能なリンクが複数ある場合でも、特定の送信元/宛先のペア間のすべてのパケットが同じリンクを通過します。 つまり、宛先別ロード バランシングでは特定の送信元/宛先のペアに対するパケットが順々に着信するようになります。

リンク バンドルのレイヤ 3 ロード バランシング

デフォルトで、レイヤ 2 リンク バンドルのロード バランシングは、パケット ヘッダーの MAC SA/DA フィールドに基づいて行われます。 リンク バンドルのレイヤ 3 ロード バランシングは、イーサネット フロー ポイント（EFP）に基づいて実行され、パケットの IPv4 送信元アドレスおよび宛先アドレスに基づきます。レイヤ 3 サービス固有のロード バランシングが設定されている場合、すべての出力バンドルは IPv4 送信元アドレスおよび宛先アドレスに基づいてロード バランシングされます。 パケットに IPv4 アドレスがない場合、デフォルトのロード バランシングが使用されます。

リンク バンドルのレイヤ 3 ロード バランシングは、次のコマンドを使用して、グローバルにイネーブルになります。

hw-module load-balance bundle l2-service l3-params

QoS およびリンク バンドル

物理インターフェイスおよびサブインターフェイスで現在サポートされているすべての Quality of Service（QoS）機能は、すべてのリンク バンドル インターフェイスおよびサブインターフェイスでサポートされています。 QoS は、個々のインターフェイスに設定する方法と同じ方法でリンク バンドルに設定します。 ただし、次の点に注意してください。

- QoS ポリシーがバンドルに適用される場合（入力または出力方向）、ポリシーはそれぞれのメンバ インターフェイスに適用されます。 ポリシー マップ内のキューおよびポリサー（入力または出力方向）は、各バンドル メンバに複製されます。
- QoS ポリシーがバンドル インターフェイスまたはバンドル VLAN に適用されない場合、入力および出力トラフィックはどちらもリンク メンバごとのポートのデフォルト キューを使用します。
- リンク バンドル メンバは、複数のネットワーク処理装置やラインカードで表すことができます。 バンドル ポリシーマップで指定されたシェーピング レートは、すべてのバンドル メンバを集約したものではありません。 バンドルに適用されたシェーピング レートは、リンクのロード バランシングによって異なります。 たとえば 10 Mbps のシェーピング レートのポリシー マップが 2 つのメンバ リンクを持つバンドルに適用され、トラフィックが常に同じメンバ リンクにロード バランシングされると、全体で 10 Mbps のレートがバンドルに適用されます。 ただし、トラフィックが 2 つのリンクの間で均等にロード バランシングされている場合、バンドルの全体的なシェーピング レートは 20 Mbps になります。

例 1 では、トラフィック ポリシーが入力方向においてどのようにイーサネット リンク バンドルに適用されるかを示します。 ポリシーは、イーサネット リンク バンドルのメンバであるすべてのインターフェイスに適用されます。

例 1 イーサネット リンク バンドルへのトラフィック ポリシーの適用

```
interface Bundle-Ether bundle-id
 service-policy input policy-1
end
```

POS リンク バンドリングの QoS

POS リンク バンドルでは、ポリサーと出力キューに対してパーセンテージ ベースの帯域幅がサポートされています。 出力キューに対しては、時間指定のキュー制限がサポートされています。

入力 QoS ポリシーの設定

入力 QoS ではキューイングがサポートされていないので、帯域幅はポリサーでのみ使用されます。 入力 QoS を設定したバンドルでメンバ リンクの追加や削除があると、その影響を受けたラインカードの集約バンドルの帯域幅が変化します。 1 つの入力 QoS ポリシー インスタンスが、POS リンク バンドルの一部である各 SIP 700 ラインカードに割り当てられます。

出力 QoS ポリシーの設定

出力QoSを設定したバンドルにメンバリンクを追加すると、そのバンドルのポリシーマップが、追加したメンバ リンクに適用されます。

例 2 は、POS リンク バンドルでサポートされている出力 QoS ポリシーを示しています。

例 2 POS リンク バンドルでサポートされている出力 QoS ポリシー

```
policy-map out-sample
  class voice
    priority level 1
    police rate percent 10
  class premium
    bandwidth percent 30
    queue-limit 100 ms
  class class-default
    queue-limit 100 ms
```

その他の関連資料

ここでは、リンク バンドルの QoS の設定に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
初期システム起動と設定	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』

関連項目	マニュアル タイトル
リンク バンドル	『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*』の「Configuring Link Bundling on the Cisco ASR 9000 Series Router」モジュール
マスター コマンド リファレンス	『*Cisco ASR 9000 Series Aggregation Services Router Master Command Listing*』
QoS コマンド	『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』
ユーザ グループとタスク ID	『Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide』の「Configuring AAA Services on Cisco ASR 9000 Series Router」モジュール

標準

標準	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
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

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
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

索 引

数字

A

B

C

D

E

I

L

M

N

P

Q

R

S

V

い

か

き

く

け

こ

さ

し

ち

て

と

に

ね

は

ひ

ふ

ほ

ま

も

り