



A から C

- [access-list rate-limit](#) (3 ページ)
- [account](#) (6 ページ)
- [admit cac local](#) (8 ページ)
- [atm-address \(qos\)](#) (9 ページ)
- [attribute](#) (11 ページ)
- [auto discovery qos](#) (12 ページ)
- [auto qos](#) (14 ページ)
- [auto qos voip](#) (16 ページ)
- [auto qos voip \(6500\)](#) (19 ページ)
- [bandwidth \(policy-map クラス\)](#) (23 ページ)
- [bandwidth qos-reference](#) (35 ページ)
- [bandwidth remaining ratio](#) (39 ページ)
- [bump](#) (45 ページ)
- [bundle](#) (49 ページ)
- [bundle svc](#) (51 ページ)
- [class \(EtherSwitch\)](#) (53 ページ)
- [class \(ポリシー マップ\)](#) (56 ページ)
- [class-map arp-peruser](#) (64 ページ)
- [class-bundle](#) (65 ページ)
- [class-map](#) (68 ページ)
- [class-map arp-peruser](#) (75 ページ)
- [class type tag](#) (76 ページ)
- [clear control-plane](#) (78 ページ)
- [clear ip nbar](#) (80 ページ)
- [clear ip nbar classification auto-learn top-hosts](#) (82 ページ)
- [clear ip nbar protocol-discovery](#) (83 ページ)
- [clear ip rsvp authentication](#) (84 ページ)
- [clear ip rsvp counters](#) (86 ページ)
- [clear ip rsvp hello instance counters](#) (87 ページ)

- [clear ip rsvp hello instance statistics](#) (89 ページ)
- [clear ip rsvp hello statistics](#) (91 ページ)
- [clear ip rsvp high-availability counters](#) (93 ページ)
- [clear ip rsvp msg-pacing](#) (94 ページ)
- [clear ip rsvp reservation](#) (96 ページ)
- [clear ip rsvp sender](#) (98 ページ)
- [clear ip rsvp signalling fast-local-repair statistics](#) (100 ページ)
- [clear ip rsvp signalling rate-limit](#) (101 ページ)
- [clear ip rsvp signalling refresh reduction](#) (102 ページ)
- [clear mls qos](#) (103 ページ)
- [clear service-group traffic-stats](#) (106 ページ)
- [compression header ip](#) (107 ページ)
- [control-plane](#) (109 ページ)
- [copy interface](#) (114 ページ)
- [custom-queue-list](#) (116 ページ)

access-list rate-limit

専用アクセス レート (CAR) ポリシーで使用するアクセス リストを設定するには、グローバルコンフィギュレーションモードで **access-list rate-limit** コマンドを使用します。このコンフィギュレーションからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list rate-limit *acl-index* {*precedence**mac-address**exp*}**mask** *mask*}

no access-list rate-limit *acl-index* {*precedence**mac-address**exp*}**mask** *mask*}

構文の説明

<i>acl-index</i>	アクセス リスト番号。次のものでパケットを分類します <ul style="list-style-type: none"> • IP プレシデンス。1 ~ 99 の任意の数値を使用 • MAC アドレス。100 ~ 199 の任意の数値を使用 • マルチプロトコルラベルスイッチング (MPLS) 実験フィールド。200 ~ 299 の任意の数値を使用
<i>precedence</i>	IP プレシデンス。有効値の範囲は 0 ~ 7 です。
<i>mac-address</i>	MAC アドレス。
<i>exp</i>	MPLS 実験フィールド。有効値の範囲は 0 ~ 7 です。
mask <i>mask</i>	マスク。同じレート制限アクセス リストに複数の IP プレシデンスまたは MPLS 実験フィールドの値を割り当てる場合は、このオプションを使用します。

コマンドデフォルト

CAR アクセス リストは設定されていません。

コマンドモード

グローバル設定

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.1(5)T	このコマンドに MPLS 実験フィールドに基づくアクセス リストが含まれました。
12.2(2)T	このコマンドが Cisco IOS Release 12.2(2)T に統合されました。
12.2(4)T	このコマンドが Cisco MGX RPM-PR カードを持つ Cisco MGX 8850 スイッチおよび MGX 8950 スイッチに実装されました。
12.2(4)T2	このコマンドは、Cisco 7500 シリーズに実装されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更箇所
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

このコマンドを使用して、特定の CAR アクセスリストに対して指定した IP プレシデンス、MACアドレス、またはMPLS実験フィールド値によってパケットを分類します。次に、**rate-limit** コマンドを使用して、個々のレート制限アクセスリストに CAR ポリシーを適用できます。この方法によってアクセスリスト内のパケットが分類される場合は、異なる IP プレシデンス、MACアドレス、またはMPLS実験フィールド値を持つパケットに、CARプロセスで異なる処理が行われます。

レート制限アクセスリストごとに、1つだけのコマンドを指定できます。同じアクセスリスト番号を使用してこのコマンドを複数回入力すると、新しいコマンドが前のコマンドを上書きします。

複数の IP プレシデンスまたは MPLS 実験フィールドの値を同一のレート制限リストに割り当てるには、**mask** キーワードを使用します。**mask** 値を確認するには、次の手順を実行します。

1. このレート制限アクセスリストに割り当てるプレシデンスを決定します。
2. 各ビットを1つの値に対応させて、8ビットの数値をプレシデンスまたはMPLS実験フィールド値に変換します。たとえば、MPLS 実験フィールド値 0 は 00000001 に対応し、1 は 00000010 に対応し、6 は 01000000 に対応し、7 は 10000000 に対応します。
3. 選択した MPLS 実験フィールド値の 8 ビットの数値を加えます。たとえば、MPLS 実験フィールドの値 1 と 6 のマスクは、01000010 です。
4. **access-list rate-limit** コマンドは、16 進形式を予期します。バイナリマスクを、対応する 16 進数に変換します。たとえば、01000010 は 42 としてコマンドで使用します。1 または 6 の MPLS 実験フィールド値を持つすべてのパケットは、このアクセスリストに一致します。

マスク FF は、すべてのプレシデンスに一致します。また、00 はどのプレシデンスにも一致しません。

例

次の例では、値が 7 の MPLS 実験フィールドがレート制限アクセスリスト 200 に割り当てられます。

```
Router(config)# access-list rate-limit 200 7
```

次に、レート制限がレート制限アクセスリストに一致するパケットのみに適用されるように、そのレート制限アクセスリストを、**rate-limit** コマンドで使用できます。

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# rate-limit input access-group rate-limit 200 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
```

関連コマンド

コマンド	説明
rate-limit	CAR および DCAR ポリシーを設定します。
showaccess-listsrate-limit	レート制限アクセスリストに関する情報を表示します。

account

このコマンドを設定したトラフィッククラスに対して一致するパケットの統計収集を有効にするには、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、**account** コマンドを使用します。統計収集を無効にするには、このコマンドの **no** 形式を使用します。

account [drop]
no account

構文の説明

drop	(オプション) コマンドを設定するトラフィッククラスに対して破棄されるパケットの統計収集を有効にします。これはデフォルトの動作です。
-------------	--

コマンド デフォルト

account コマンドを設定すると、デフォルトの動作では、破棄される統計を収集します。**account** コマンドが設定されていない場合、統計は収集されません。

コマンド モード

ポリシーマップクラス (config-pmap-c)

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが導入されました。

使用上のガイドライン

account コマンド QoS の一部 (Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでサブスクリバごとの統計の収集をサポートする Cisco IOS XE リリース 2.6 のポリシー集約の拡張機能) として実装されました。

設定時のデフォルトでは、このコマンドは、設定したクラスのトラフィックに対して破棄される統計の収集を有効にします。したがって、オプションの **drop** キーワードは、破棄される統計の収集を有効にするために必須ではありません。

showpolicy-mapinterface コマンドを使用すると、特定のトラフィッククラスに対して収集されたサブスクリバの統計を表示できます。

例

サブスクリバのポリシーマップの EF トラフィック クラスに対して、破棄される統計収集 (デフォルト) を有効にする例を次に示します。

```
Router(config)# policy-map subscriber
Router(config-pmap)# class EF
Router(config-pmap-c)# account
```

関連コマンド

コマンド	説明
class(policy-map)	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルトクラス（一般に class-default クラスといいます）を指定します。
policy-map	ポリシーマップ コンフィギュレーションモードを開始し、サービスポリシーを指定するため1つ以上のインターフェイスに適用できるポリシー マップを作成または修正します。
showpolicy-mapinterface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

admit cac local

クラスに対する Per-Flow Admission ポリシーを有効にするには、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 **admitcac local** コマンドを使用します。クラスに対する Per-Flow Admission ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

admit cac local
no admit cac local

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Per-Flow Admission は、クラスに対して有効になっていません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード (**config-pmap-c**)

コマンド履歴

リリース	変更箇所
15.4(2)T	このコマンドが導入されました。

使用上のガイドライン

クラスで Per-Flow Admission を有効にしてフローを検出するには、このコマンドを使用します。Per-Flow Admission ポリシーは、フローを制限し、すでに流入したフローを保護します。

例

```
Device(config-pmap-c)# admit cac local
```

関連コマンド

コマンド	説明
rate	帯域幅プールのサイズを kbps 単位で設定するか、出力クラスの帯域幅のパーセンテージとして設定します。
flow rate fixed	各フローに割り当てる帯域幅の量を指定します。
flow idle-timeout	フローのタイムアウト期間を指定します。

atm-address (qos)

特定の ATM アドレスに関連付けられる QoS パラメータを指定するには、LANE QoS データベース設定モードで **atm-address** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

atm-address *atm-address* [**ubr+** **pcr** *value* **mcr** *value*]
no atm-address *atm-address* [**ubr+** **pcr** *value* **mcr** *value*]

構文の説明

<i>atm-address</i>	ATM アドレスを制御します。
ubr+	(オプション) 未指定ビットレートプラス (UBR+) 仮想チャネル接続 (VCC)。
pcr	(オプション) ピークセルレート (PCR)。
<i>value</i>	(オプション) UBR+ の PCR 値 (kbps)。
mcr value	(オプション) 最小セルレート (MCR) 値 (kbps)

コマンドデフォルト

デフォルトの ATM アドレスはありません。

コマンドモード

LANE QoS データベース設定

コマンド履歴

リリース	変更箇所
12.1(2)E	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

例

特定の ATM アドレスに関する PCR および MCR の値を使用し、必要な QoS パラメータを入力する方法を、次の例に示します。このコマンドは、LANE QoS データベース設定モードから入力します。

```
Router(lane-qos)# atm-address 47.0091810000000061705B0C01.00E0B0951A40.0A ubr+ pcr 500000
mcr 100000
```

関連コマンド

コマンド	説明
laneclientqos	QoS over LANE データベースをインターフェイスに適用します。
laneqosdatabase	QoS over LANE データベースを構築する処理を開始します。
showlaneqosdatabase	特定の QoS over LANE データベースの内容を表示します。
ubr+cos	CoS 値を UBR+ VCC にマップします。

attribute

属性プロファイルに属性を追加するには、属性マップコンフィギュレーションモードで **attribute** コマンドを使用します。

attribute *attribute-name* *attribute-value*

構文の説明

<i>attribute-name</i>	プロファイルに設定する属性の名前。
<i>attribute-value</i>	属性値。

コマンドモード

属性マップ コンフィギュレーション (config-attribute-map)

コマンド履歴

リリース	変更箇所
15.2(4)M2	このコマンドが導入されました。
Cisco IOS XE Release 3.8S	このコマンドが、Cisco IOS XE リリース 3.8S に統合されました。

使用上のガイドライン

このコマンドには **no** 形式はありません。

例

次の例は、**application-group** 属性をプロファイルに追加する方法を示しています。

```
Device# configure terminal
Device(config)# ip nbar attribute-map nntp-attrib
Device(config-attribute-map)# attribute application-group aol-group
Device(config-attribute-map)# end
```

関連コマンド

コマンド	説明
ip nbar attribute-map	プロトコルの属性を設定します。
ipnbarattribute-set	プロトコルに新しい属性プロファイルをアタッチします。

auto discovery qos

エンタープライズ機能の AutoQoS を設定するためにデータの検出および収集を開始するには、インターフェイス コンフィギュレーション モードで **autodiscoveryqos** コマンドを使用します。データの検出および収集を停止するには、このコマンドの **no** 形式を使用します。

auto discovery qos [trust]
no auto discovery qos

構文の説明

trust	(オプション) パケットの Differentiated Services Code Point (DSCP; DiffServ コードポイント) のマーキングが音声、ビデオ、およびデータ トラフィックの分類に対する trust (つまり、信頼されていること) を示します。 オプションの trust キーワードが指定されない場合、音声、ビデオ、およびデータ トラフィックは、Network-Based Application Recognition (NBAR) を使用して分類されます。また、パケットは適切な DSCP 値でマークされます。
--------------	---

コマンド デフォルト

データ収集は実行されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.3(7)T	このコマンドが導入されました。
12.3(11)T	信頼モードが、プロトコルタイプではなく DSCP 値でパケットが分類されるように変更されました。

使用上のガイドライン

autodiscoveryqos コマンドは、エンタープライズ機能の AutoQoS の自動検出 (データ収集) フェーズを開始します。このコマンドは、NBAR Protocol Discovery を呼び出してデータを収集し、インターフェイスの出力方向のトラフィックを分析します。

noautodiscoveryqos コマンドは、自動検出フェーズを終了し、生成されたすべてのデータ収集レポートを削除します。

指定された DSCP マーキングに基づいて、信頼されたモデルに **trust** キーワードを使用します。詳細については、Cisco IOS リリース 12.3(7)T の *AutoQoS for the Enterprise* 機能モジュールの「Trusted Boundary」セクションを参照してください。

例

serial2/1/1 サブインターフェイスでエンタープライズ機能の AutoQoS の自動検出 (データ収集) フェーズを有効にした設定例を、次に示します。

```
Router> enable
Router# configure terminal
```

```
Router(config)# interface serial2/1.1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto discovery qos
Router(config-if)# end
```

関連コマンド

コマンド	説明
autoqos	エンタープライズ機能の AutoQoS によって作成された QoS クラス マップおよびポリシー マップをインストールします。
servicepolicy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showautoqos	特定のインターフェイスまたはすべてのインターフェイスで AutoQoS によって作成されたインターフェイス コンフィギュレーション、ポリシー マップ、およびクラス マップを表示します。

auto qos

エンタープライズ機能の AutoQoS によって作成された Quality of Service (QoS) クラス マップ およびポリシー マップをインストールするには、インターフェイス コンフィギュレーション モードで **autoqos** コマンドを使用します。QoS ポリシーを削除するには、このコマンドの **no** 形式を使用します。

auto qos
no auto qos

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

QoS ポリシーはインストールされません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更箇所
12.3(7)T	このコマンドが導入されました。

使用上のガイドライン

エンタープライズ機能の AutoQoS によって自動的に生成されたテンプレートから、クラスマップ およびポリシーマップが作成されます。これらのテンプレート（および結果として作成されるクラスマップとポリシーマップ）は、エンタープライズ機能の AutoQoS の自動検出フェーズで収集したデータに基づいて生成されます。自動検出フェーズの詳細については、Cisco IOS リリース 12.3(7)T の *AutoQoS for the Enterprise* 機能モジュールの「Configuration Phases」セクションを参照してください。

noautoqos コマンドは、インターフェイスにインストールされている、AutoQoS によって生成されたすべてのクラスマップおよびポリシーマップを削除します。

autoqos コマンドは、ギガビット インターフェイスでサポートされていません。

例

serial2/1/1 サブインターフェイスでエンタープライズ機能の AutoQoS を有効にした設定例を、次に示します。この設定では、AutoQoS のクラスマップおよびポリシーマップは、serial2/1 インターフェイスにインストールされます。

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto qos
Router(config-if)# end
```

関連コマンド

コマンド	説明
servicepolicy	入力インターフェイスまたはVC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたはVCのサービス ポリシーとして使用するポリシー マップを対応付けます。
showautoqos	特定のインターフェイスまたはすべてのインターフェイスで AutoQoS によって作成されたインターフェイス コンフィギュレーション、ポリシー マップ、およびクラス マップを表示します。

auto qos voip

インターフェイスで AutoQoS--VoIP 機能を設定するには、インターフェイス コンフィギュレーションモードまたは フレームリレー DLCI コンフィギュレーションモードで **autoqosvoip** コマンドを使用します。インターフェイスから AutoQoS--VoIP 機能を削除するには、このコマンドの **no** 形式を使用します。

auto qos voip [trust] [fr-atm]
no auto qos voip [trust] [fr-atm]

構文の説明

trust	(オプション) パケットの Differentiated Services Code Point (DSCP; DiffServ コードポイント) のマーキングが音声トラフィックの分類に対する trust (つまり、信頼されていること) を示します。オプションの trust キーワードが指定されない場合、音声トラフィックは、Network-Based Application Recognition (NBAR) を使用して分類されます。また、パケットは適切な DSCP 値でマークされます。
fr-atm	(オプション) フレームリレー/ATM 間リンクに対して AutoQoS--VoIP 機能を有効にします。このオプションは、フレームリレー/ATM 間インターワーキングのみに対するフレームリレー データリンク接続識別子 (DLCI) で使用可能です。

コマンド デフォルト

デフォルト モードでは無効です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)
 フレームリレー DLCI コンフィギュレーション (フレームリレー DLCI で使用) (config-fr-dlci)

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが導入されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

使用上のガイドライン

AutoQoS--VoIP 機能を、フレームリレー/ATM 間インターワーキングに対して有効にするには、**fr-atm** キーワードを明示的に設定する必要があります。ただし、**fr-atm** キーワードは、低速 DLCI のみに影響します。高速 DLCI には影響しません。



(注) 768 kbps 以下のリンク速度の DLCI は低速 DLCI と見なされ、768 kbps を超えるリンク速度の DLCI は高速 DLCI と見なされます。

このコマンドに **trust** キーワードが設定されているかどうかに応じて、AutoQoS--VoIP 機能は自動的に次の 2 つのポリシー マップの 1 つを作成します。

- 「AutoQoS-Policy-Trust」 (**trust** キーワードが設定されている場合に作成される)
- 「AutoQoS-Policy-UnTrust」 (**trust** キーワードが設定されていない場合に作成される)

これらポリシー マップの両方は、インターフェイスまたは相手先固定接続 (PVC) 上の Voice over IP (VoIP) トラフィックを処理するように設計されています。また、ネットワークの Quality of Service (QoS) の要件に合わせて変更できます。これらのポリシー マップを変更するには、適切な Cisco IOS コマンドを使用します。

これらのポリシー マップは、**service-policy** コマンドを使用してインターフェイスまたは PVC にアタッチしないでください。この方法でポリシー マップをアタッチすると、AutoQoS--VoIP 機能 (つまり、ポリシーマップ、クラスマップ、およびアクセスコントロールリスト [ACL]) は、**noautoqosvoip** コマンドの設定時に適切に削除されません。

同一のネットワーク内で ATM PVC と相互接続されている低速フレーム リレー DLCI の場合は、**autoqosvoip** コマンドで **fr-atm** キーワードを明示的に設定し、AutoQoS--VoIP 機能を適切に設定する必要があります。つまり、コマンドを **autoqosvoipfr-atm** として設定する必要があります。

フレーム リレー/ATM 間によって設定される低速フレーム リレー DLCI では、マルチリンク PPP (MLP) over Frame Relay (MLPoFR) が自動的に設定されます。サブインターフェイスには IP アドレスが必要です。MLPoFR の設定時、この IP アドレスは削除され、MLP バンドルに置かれます。**autoqosvoip** コマンドを使用し、ATM 側で AutoQoS--VoIP 機能を設定する必要があります。

autoqosvoip コマンドは、サブインターフェイスまたはギガビット インターフェイスでサポートされていません。

autoqosvoip コマンドは、フレーム リレー DLCI に対して使用可能です。

AutoQoS--VoIP の無効化

noautoqosvoip コマンドは、AutoQoS--VoIP 機能を無効にし、この機能に関連付けられた設定を削除します。

noautoqosvoip コマンドを使用すると、AutoQoS--VoIP 機能によって最初に生成された個々のコマンドの **no** 形式が設定されます。個々のコマンドの **no** 形式を使用すると、システムのデフォルトが復元されます。コマンドの **no** 形式は、ユーザがコマンドを個別に入力するのと同様に適用されます。デフォルト設定を復元する設定が適用されるにしたがって、コマンドの処理によって生じるメッセージが表示されます。



(注) **noautoqosvoip** コマンドを設定することなくサブインターフェイスまたは PVC を削除した場合 (ATM の場合もフレーム リレー PVC の場合も)、AutoQoS--VoIP 機能は適切に削除されません。

例

シリアルのポイントツーポイントサブインターフェイス 4/1.2 で AutoQoS--VoIP 機能を設定した例を、次に示します。この例では、**trust** と **fr-atm** の両方のキーワードが設定されています。

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/1.2 point-to-point
Router(config-if)# bandwidth 100
Router(config-if)# ip address 192.168.0.0 255.255.255.0
Router(config-if)# frame-relay interface-dlci 102
Router(config-fr-dlci)# auto qos voip trust fr-atm
Router(config-fr-dlci)# end
Router(config-if)#
```

```
exit
```

関連コマンド

コマンド	説明
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showautoqos	特定のインターフェイスまたはすべてのインターフェイスで、AutoQoS--VoIP 機能によって作成された設定を表示します。

auto qos voip (6500)

Voice over IP (VoIP) ポートインターフェイスで AutoQoS を設定するには、インターフェイス コンフィギュレーション モードで **autoqosvoip** コマンドを使用します。このコンフィギュレーションから AutoQoS を削除するには、このコマンドの **no** 形式を使用します。

```
auto qos voip {cisco-phone|cisco-softphone|trust}
no auto qos voip {cisco-phone|cisco-softphone|trust}
```

構文の説明	パラメータ	説明
	cisco-phone	Cisco IP Phone に対して Quality of Service (QoS) 入力マクロを有効にします。
	cisco-softphone	Cisco IP SoftPhone に対して QoS 入力マクロを有効にします。
	trust	Differentiated Services Code Point (DSCP; DiffServ コードポイント) およびサービスクラス (CoS) トラフィック マーキングを信頼しているポートに対して AutoQoS を指定します。

コマンド デフォルト AutoQoS は、DSCP および CoS トラフィック マーキングを信頼します。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンド履歴	リリース	変更箇所
	12.2(33)SXH	このコマンドが導入されました。

使用上のガイドライン **autoqosvoip** コマンドは、ギガビット インターフェイスでサポートされていません。

QoS (AutoQoS) の自動化を使用すると、特定のポートに必要な QoS パラメータのタイプを指定できます。たとえば、**autoqosvoipcisco-softphone** コマンドを入力すると、Cisco IP SoftPhone に対して QoS 入力マクロを有効にすることができます。

Smartports 機能は、特定のアプリケーションに関連するすべてのスイッチ設定を、単一のコマンドで設定するためのツールセットを提供します。たとえば、**autoqosvoipcisco-phone** コマンドを入力すると、IP フォンをスイッチに接続するために必要なすべての設定が構成されます。

showautoqos コマンドを入力すると、設定済みの AutoQoS マクロを表示できます。

AutoQoS と Smartports は、次のモジュールでサポートされています。

- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6148-GE_TX
- WS-X6548-GE-TX-CR
- WS-X6148-RJ45V

- WS-X6148-RJ21V
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6248-TEL



(注) **noautoqosvoip** インターフェイス コンフィギュレーション コマンドは、QoS をグローバルに無効にすることはできません。また、AutoQoS によって作成された受信済みの CoS/内部 DSCP マップを削除することはありません。

autoqosvoipcisco-phone および **autoqosvoipcisco-softphone** コマンドを使用すると、インターフェイスの AutoQoS に対して、受信 QoS 設定マクロを有効にすることができます。場合によっては、インターフェイスに固有の **autoqosvoip** コマンドを使用して、グローバルに適用される設定コマンドを生成することもできます。

autoqosvoipcisco-phone コマンドを入力した場合は、**switchport** コマンドを使用してインターフェイスを設定する必要があります。**autoqosvoipcisco-softphone** コマンドを入力した場合、**switchport** コマンドを入力してインターフェイスを設定することはできません。

switchport コマンドを使用してインターフェイスを設定する場合は、AutoQoS によってインターフェイスが CoS を信頼するように設定されます。**switchport** コマンドを使用してインターフェイスを設定しない場合は、AutoQoS によってインターフェイスが DSCP を信頼するように設定されます。

AutoQoS は、デフォルト以外の CoS/DSCP マップを使用します。このため、ポート ASIC ベースでポートの信頼を設定する必要があります。

autoqosvoipcisco-phone コマンドを入力すると、次の動作が発生します。

- QoS が無効になっている場合は、有効になります。
- ポートは、ポートベースの QoS に変更されます。
- 適切な CoS マップが設定されます。
- (該当する場合) すべてのポートは、ポートベースのモードに変更されます。
- trust-CoS QoS ポリシーが作成され、trust-CoS QoS ポリシーが必要なポート (COIL2 と COIL1) に適用されます。
- ポート上で信頼境界を有効にします。
- 信頼境界の CoS 値が 0 に設定されます。
- ポートの信頼は、trust-cos に設定されます。
- 10/100 ポートと 10/100/1000 ポートのみがサポートされています。
- CDP バージョンがバージョン 2 でない場合、警告メッセージが表示されます。

autoqosvoipcisco-softphone コマンドを入力すると、次の動作が発生します。

- **cisco-softphone** マクロは、**cisco-phone** マクロのスーパーセットであり、Cisco IP Phone が Catalyst 6500 シリーズ スイッチで適切に動作するために必要なすべての機能を設定します。
- VoIP パケットを分類し、プライオリティキューまたは別の低遅延キューに登録するため、AutoQoS ポリシー マップ、クラス マップ、およびアクセス リストのグローバル設定が作成されます。インターフェイスの設定は、インターフェイスのタイプとリンク速度に応じて作成されます。
- **cisco-softphone** ポートベースの AutoQoS マクロが実行されるインターフェイスには、2つのレートリミッタが関連付けられています。2つのレートリミッタによって、**cisco-softphone** ポートのすべての着信トラフィックに次の特性が確保されます。
 - DSCP 46 のレートは、予期されたソフトフォン レート以下。
 - DSCP 26 のレートは、予期されたシグナリング レート以下。
 - その他すべてのトラフィックは DSCP 0 (デフォルト トラフィック) に再マークされる。
- DSCP-46 は、バーストが 2 KB の 320 Kbps のレートでポリシングされます。DSCP 26 は、バーストが 8 KB の 32 Kbps でポリシングされます。
- ポートは、すべてのポートタイプに対して信頼できないものとして設定されます。ポリシング済み DSCP マップでは、DSCP 46 が DSCP 0 にマークダウンされ、DSCP 26 が DSCP 0 にマークダウンされるように設定されます。デフォルトの QoS IP ACL は、他のすべてのトラフィックを DSCP 0 に再マークします。

autoqosvoipsoft-phone コマンドを入力すると、次の動作が発生します。

- QoS が無効な場合、QoS を有効にします。
- ポートベースの QoS にポートを変更します。
- 適切なポリシング済み DSCP マップを設定します。
- 適切な CoS/DSCP マップを設定します。
- (該当する場合) すべてのポートをポートベースのモードに変更します。
- 必要なポートに、**trust-dscp** QoS ポリシーを作成します (COIL2 と COIL1)。
- **trust-dscp** QoS ポリシーをポート (COIL2 と COIL1) に適用します。
- ポート上で信頼境界を無効にします。
- 信頼を **untrusted** に変更します。
- 10/100 ポートと 10/100/1000 ポートのみを許可します。
- 2つのレートリミッタを適用します。1つは DSCP 46、もう1つは DSCP 26 着信トラフィック用です。着信の DSCP 46 および DSCP 26 トラフィックに限り信頼します。

- トラフィックのレート制限結果のいずれかの違反を DSCP 0 にマークダウンします。
- その他すべて (DSCP 26 および 46 以外) の着信トラフィックを DSCP 0 に再マークします。

autoqosvoiptrust コマンドを入力すると、次のようになります。

- DSCP および CoS マーキングは、音声トラフィックの分類に対して信頼されます。
- QoS が無効な場合、QoS を有効にします。
- ポートベースの QoS にポートを変更します。
- (該当する場合) すべてのポートをポートベースのモードに変更します。
- 必要なポートに、**trust-dscp** および **trust-cos** QoS ポリシーを作成します (COIL2 と COIL1)。
- **trust-dscp** および **trust-cos** QoS ポリシーをポート (COIL2 と COIL1) に適用します。
- ポート上で信頼境界を無効にします。
- ポートの信頼を **trust-cos** に設定します。
- すべてのポートがサポートされます。
- **dscp-to-q** マッピングを許可するすべてのポートに対して、キューイングを DSCP に基づいて実行します。許可されていない場合は、キューイングを CoS に基づいて実行します。

例

Cisco IP Phone に対して QoS 入力マクロを有効にする方法を、次の例に示します。

```
Router(config-if)# auto qos voip cisco-phone
```

関連コマンド

コマンド	説明
showautoqos	AutoQoS 情報を表示します。
showrunning-configinterface	インターフェイスのステータスと設定を表示します。
switchport	LAN インターフェイスをレイヤ 2 スイッチドインターフェイスとして設定します。

bandwidth (policy-map クラス)

ポリシーマップに属するクラスに割り当てられる帯域幅を指定または変更するには、あるいは ATM オーバーヘッド アカウンティングを有効にするには、QoS 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 **bandwidth** コマンドを使用します。クラスに指定されている帯域幅を削除するか、または ATM オーバーヘッド アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
bandwidth {kbps|[remaining] percent percentage} [account {qinq|dot1q} aal5
subscriber-encapsulation]
no bandwidth
```

Cisco 10000 シリーズ ルータ (PRE3)

```
bandwidth {kbps|[remaining] percent percentage} account {qinq|dot1q} {aal5|aal3}
subscriber-encapsulationuser-defined offset [atm]
no bandwidth
```

構文の説明

<i>kbps</i>	クラスに割り当てる帯域幅の量 (kbps)。帯域幅の量は、使用中のインターフェイスとプラットフォームに応じて変わります。値は 1 ~ 2,000,000 kbps である必要があります。
remaining	(オプション) 保証帯域幅の割合は、使用可能な帯域幅の相対パーセントに基づくように指定します。
percent <i>percentage</i>	プライオリティ クラスのために確保される利用可能な帯域幅の絶対パーセントまたは使用可能な帯域幅の相対パーセントに基づいて、保証帯域幅のパーセンテージを指定します。有効な指定範囲は 1 ~ 100 です。
account	(任意) ATM オーバーヘッド アカウンティングをイネーブルにします。
qinq	(任意) ATM オーバーヘッド アカウンティングのデジタル加入者線アクセス マルチプレクサ (DSLAM) のカプセル化タイプに対して、キューインキューのカプセル化をブロードバンドアグリゲーションシステム (BRAS) として指定します。
dot1q	(任意) ATM オーバーヘッド アカウンティングの BRAS-DSLAM カプセル化タイプとして IEEE 802.1Q VLAN カプセル化を指定します。
aal5	(オプション) ATM オーバーヘッド アカウンティングの加入者線で ATM アダプテーション層とカプセル化タイプを指定します。AAL5 は、コネクション型の可変ビットレート (VBR) サービスをサポートします。有効なカプセル化タイプについては、「使用上のガイドライン」を参照してください。

<i>subscriber-encapsulation</i>	加入者線のカプセル化のタイプ。有効なカプセル化タイプについては、「使用上のガイドライン」を参照してください。
aal3	コネクションレス型リンクとコネクション型リンクの両方をサポートする ATM アダプテーション層 5 を指定します。 aal3 または aal5 のいずれかを指定する必要があります。
user-defined offset	ルータでの ATM オーバーヘッド計算に使用するオフセット サイズを指定します。 有効な値は、-127 ~ 127 バイトです。0 は有効な値ではありません。 (注) user-defined offset オプションを指定していない場合、ルータはオフセット サイズを設定します。
atm	ATM オーバーヘッドの計算に ATM セル タックスを適用します。 (注) <i>offset</i> オプションと atm オプションの両方を設定すると、オフセット サイズに合わせてパケット サイズが調整されてから、ATM セル タックスが追加されます。

コマンド デフォルト

帯域幅は指定されていません。

ATM オーバーヘッド アカウンティングはディセーブルです。

コマンド モード

QoS ポリシーマップ クラス コンフィギュレーション (config-pmap-c)

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合され、Versatile Interface Processor (VIP) 対応型 Cisco 7500 シリーズ ルータに実装されました。
12.0(7)T	このコマンドが変更されました。 percent キーワードが追加されました。
12.0(17)SL	このコマンドは、Cisco IOS Release 12.0(17)SL に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.0(22)S	このコマンドが変更されました。 percent キーワードのサポートが Cisco 10000 シリーズ ルータに追加されました。
12.0(23)SX	このコマンドが変更されました。 remaining percent キーワードのサポートが Cisco 10000 シリーズ ルータに追加されました。
12.1(5)T	このコマンドが Cisco IOS Release 12.1(5)T に統合され、VIP 対応型 Cisco 7500 シリーズ ルータに実装されました。

リリース	変更箇所
12.2(2)T	このコマンドが変更されました。 remaining percent キーワードが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(31)SB	このコマンドは、Cisco IOS Release 12.2(31)SB に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.2(31)SB2	このコマンドが、Cisco IOS Release 12.0(17)SL に統合され、Cisco 10000 シリーズ ルータの PRE3 に実装され、PRE3 向け Cisco 10000 シリーズ ルータでの ATM オーバーヘッド アカウンティング用に機能拡張されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.2(31)SB6	このコマンドが ATM オーバーヘッドを計算する際のオフセット サイズを指定するように変更され、PRE3 向け Cisco 10000 シリーズ ルータに実装されました。
12.2(33)SRC	このコマンドは、Cisco IOS Release 12.2(33)SRC に統合され、Cisco 7600 シリーズ ルータに実装されました。
12.2(33)SB	このコマンドは、Cisco IOS Release 12.2(33)SB に統合され、Cisco 7300 シリーズ ルータに実装されました。
12.4(20)T	このコマンドが変更されました。モジュラ Quality of Service (QoS) CLI (MQC) を使用する階層型キューイングフレームワーク (HQF) に対するサポートが追加されました。
15.1(1)T	このコマンドが変更されました。 <i>kbps</i> 引数の許容値が変更されました。8 ~ 2000000 の範囲で値を入力する必要があります。
15.2(1)T	このコマンドが変更されました。 <i>offset</i> 引数と <i>kbps</i> 引数の許容値が変更されました。

ポリシー マップ コンフィギュレーション

class-map コマンドで定義されたクラスのポリシー マップを設定する場合は、**bandwidth** コマンドを使用します。**bandwidth** コマンドは、そのクラス内のトラフィックの帯域幅を指定します。クラス ベース均等化キューイング (CBWFQ) は、クラスに属するパケットのウェイトを、クラスに割り当てられた帯域幅から導出します。次に、CBWFQはこのウェイトを使用し、このクラスのキューを適正に処理します。

帯域幅を持つ完全プライオリティの設定

完全プライオリティで設定できるクラスは1つだけです。その他のクラスは、プライオリティの設定も帯域幅の設定も持ってません。他のクラスに最小帯域幅を設定するには、**bandwidthremainingpercent** コマンドを使用します。

Cisco 10000 シリーズ ルータ以外のサポートされるすべてのプラットフォームに対するパーセンテージとしての帯域幅の指定

kbps 単位で帯域幅の量を指定する以外に、使用可能な帯域幅または総帯域幅に対するパーセント比率で帯域幅を指定することもできます。輻輳の発生中には、そのクラスは、設定されている帯域幅比率に比例した帯域幅で処理されます。帯域幅のパーセンテージは、インターフェイスの帯域幅に基づきます。使用可能な帯域幅とは、インターフェイスの帯域幅からリソース予約プロトコル (RSVP) 機能、IP RTP プライオリティ機能、低遅延キューイング (LLQ) 機能に予約されているすべての帯域幅の合計を差し引いた帯域幅です。



- (注) **bandwidthremainingpercent** コマンドが設定されていると、確実な保証帯域幅が提供されない場合があります。相対的な帯域幅しか確保されないことを念頭に置いておいてください。つまり、クラスの帯域幅は、常にインターフェイスの帯域幅に対する指定されたパーセント比率に比例します。リンク帯域幅が固定されている場合、クラス帯域幅の保証は、設定されているパーセンテージに比例します。リンク帯域幅がわからないか変動する場合、ルータは、kbps でのクラス保証帯域幅を計算することができません。

Cisco 10000 シリーズ ルータに対するパーセンテージとしての帯域幅の指定

kbps 単位で帯域幅の量を指定する以外に、使用可能な帯域幅または総帯域幅に対するパーセント比率で帯域幅を指定することもできます。輻輳の発生中には、そのクラスは、設定されている帯域幅比率に比例した帯域幅で処理されます。最小帯域幅のパーセンテージは、至近の親シェーピング レートに基づきます。



- (注) **bandwidthremainingpercent** コマンドが設定されていると、確実な保証帯域幅が提供されない場合があります。相対的な帯域幅しか確保されないことを念頭に置いておいてください。つまり、クラスの帯域幅は、常にインターフェイスの帯域幅に対する指定されたパーセント比率に比例します。リンク帯域幅が固定されている場合、クラス帯域幅の保証は、設定されているパーセンテージに比例します。リンク帯域幅がわからないか変動する場合、ルータは、kbps でのクラス保証帯域幅を計算することができません。

ルータは、指定された帯域幅をインターフェイス速度の 1/255 (ESR-PRE1) または 1/65535 (ESR-PRE2) の至近の倍数に変換します。実際の帯域幅を表示するには、**showpolicy-mapinterface** コマンドを使用します。

サポートされているすべてのプラットフォームの制限

bandwidth コマンドには、次の制限事項があります。

- 設定する帯域幅の量は、レイヤ2オーバーヘッドも十分処理できる量にする必要があります。
- ポリシー マップには、同一クラス内で **kbps** または割合のいずれか（両方ではない）で指定されたすべてのクラスの帯域幅が含まれる場合があります。ただし、プライオリティクラス内での **priority** コマンドの単位は、非プライオリティクラスの帯域幅単位と異なってもかまいません。
- **bandwidthpercent** コマンドが設定され、クラスポリシー設定が含まれているポリシーマップがインターフェイスに付加されて、そのインターフェイスのサービスポリシーが決定される場合、使用可能な帯域幅が評価されます。インターフェイスの帯域幅が不十分なことが原因で、特定のインターフェイスにポリシーマップがアタッチできない場合、そのポリシーは、正常にアタッチされていたすべてのインターフェイスから削除されます。この制限事項は、**bandwidthremainingpercent** には適用されません。



- (注) CSCsy73939 で **bandwidthpercent** コマンドから有効な範囲よりも低い帯域幅値が得られた場合、この値を指定するポリシーマップをインターフェイスに付加することはできません。ルータから「サービス ポリシー出力の親として設定されているパーセンテージは、範囲外の kbps です。許可された範囲は min-value-max-value で、現在の CIR 値は n です。（service-policy output parent Configured Percent results in out of range kbps. Allowed range is min-value-max-value. The present CIR value is n.）」というエラー メッセージが表示されます。

帯域割り当ての詳細については、『Cisco IOS Quality of Service Solutions Configuration Guide』の「Congestion Management Overview」モジュールを参照してください。

クラス ポリシー設定が含まれているポリシー マップがインターフェイスにアタッチされて、そのインターフェイスのサービスポリシーが決定される場合、使用可能な帯域幅が評価されることに注意してください。インターフェイスの帯域幅が不十分なことが原因で、特定のインターフェイスにポリシーマップがアタッチできない場合、そのポリシーは、正常にアタッチされていたすべてのインターフェイスから削除されます。

モジュラ QoS CLI キューの制限

bandwidth コマンドを MQC で使用すると、特定のクラスの帯域幅を指定できます。MQC で使用される場合、**bandwidth** コマンドには、クラスにデフォルトのキュー制限があります。このキュー制限は、**queue-limit** コマンドを使用して変更でき、**bandwidth** コマンドによって設定されたデフォルトが上書きされます。



- (注) インターフェイスに必要な最低帯域保証を満たすには、**queue-limit** コマンドを使用して高速インターフェイスのデフォルトのキュー制限を変更します。

Cisco 10000 シリーズ ルータ

Cisco 10000 シリーズ ルータでは、発信インターフェイスのみで **bandwidth** コマンドがサポートされます。着信インターフェイスでは、このコマンドはサポートされません。

PRE2 で、帯域幅値と帯域幅値の単位を指定します。帯域幅の有効な値は 1 ~ 2488320000 です。単位は bps、kbps、mbps、および gbps です。デフォルトの単位は kbps です。たとえば、次のコマンドは 10000 bps と 10000 kbps の帯域幅を PRE2 に設定します。

```
bandwidth 10000 bps
bandwidth 10000
```

PRE3 で指定するのは、帯域幅値のみです。単位は常に kbps であるため、PRE3 は unit 引数をサポートしません。有効な値は 1 ~ 2000000 です。たとえば、次のコマンドは、PRE3 に 128,000 kbps の帯域幅を設定します。

```
bandwidth 128000
```

PRE3 は、PRE2 **bandwidth** コマンドが unit 引数なしで使用される場合に限り、このコマンドを受け入れます。PRE3 は、PRE3 の有効な帯域幅値の範囲外の帯域幅が指定された場合 (1 ~ 2000000)、PRE2 **bandwidth** コマンドを拒否します。

kbps 単位で帯域幅の量を指定する以外に、使用可能な帯域幅または総帯域幅に対するパーセンテージで帯域幅を指定することもできます。輻輳の発生中には、そのクラスは、設定されている帯域幅比率に比例した帯域幅で処理されます。帯域幅のパーセンテージは、インターフェイスの帯域幅に基づきます。ただし、階層型ポリシーでは、最小帯域幅のパーセンテージは至近の親シェーピング レートに基づきます。



(注) **bandwidthremainingpercent** コマンドが設定されていると、確実な保証帯域幅が提供されない場合があります。相対的な帯域幅しか確保されない可能性があります。クラスの帯域幅は、常にインターフェイスの帯域幅に対する指定されたパーセンテージに比例します。リンク帯域幅が固定されている場合、クラス帯域幅の保証は、設定されているパーセンテージに比例します。リンク帯域幅がわからないか変動する場合、ルータは、kbps でのクラス保証帯域幅を計算することができません。

ルータは、指定された帯域幅をインターフェイス速度の 1/255 (PRE1) または 1/65535 (PRE2、PRE3) の至近の倍数に変換します。実際の帯域幅を表示するには、**showpolicy-mapinterface** コマンドを使用します。

ATM のオーバーヘッド アカウンティング (Cisco 10000 シリーズ ルータ)

ATM オーバーヘッド アカウンティングを設定する場合は、BRAS-DSLAM、DSLAM-CPE、および加入者線カプセル化タイプを指定する必要があります。ルータは、次の加入者線カプセル化タイプをサポートします。

- mux-1483routed
- mux-dot1q-rbe

- snap-pppoa
- mux-rbe
- snap-1483routed
- snap-dot1q-rbe
- mux-pppoa
- snap-rbe

user-defined offset オプションを指定していない場合、ルータはオフセット サイズを計算しません。

階層型ポリシーでは、次の方法で ATM オーバーヘッド アカウンティングを設定します。

- 親で有効：親ポリシー上の ATM オーバーヘッド アカウンティングを有効にした場合は、子ポリシー上のアカウンティングを有効にする必要はありません。
- 子および親で有効：子ポリシー上の ATM オーバーヘッド アカウンティングを有効にした場合は、親ポリシー上の ATM オーバーヘッド アカウンティングも有効にする必要があります。

カプセル化タイプは、子および親ポリシーと一致する必要があります。

ユーザ定義のオフセット値は、子および親ポリシーと一致する必要があります。

例

Cisco 10000 シリーズ ルータ：例

次の例では、ポリシー マップ VLAN がクラス Customer1 に帯域幅の 30 % を、クラス Customer2 に帯域幅の 60 % を保証します。VLAN ポリシー マップを 1-Mbps リンクに適用すると、クラス Customer1 に 300 kbps (1 Mbps の 30 %) が保証され、クラス Customer2 に 600 kbps (1 Mbps の 60 %) が保証されて、class-default クラス用に 100 kbps が残ります。class-default クラスが追加の帯域幅を必要としない場合、未使用の 100 kbps はクラス Customer1 とクラス Customer2 が使用できます。両方のクラスが帯域幅を必要としている場合、設定レートに比例して共有します。次の例では、共有比率は 30:60 または 1:2 です。

```
router(config)# policy-map VLAN
router(config-pmap)# class Customer1
router(config-pmap-c)# bandwidth percent 30
router(config-pmap-c)# exit
router(config-pmap)# class Customer2
router(config-pmap-c)# bandwidth percent 60
```

CBWFQ 帯域幅の保証 : 例

2つのクラスを持つポリシー マップを作成する方法、CBWFQ のみが設定されている場合に帯域幅を保証する方法、およびポリシーをシリアル インターフェイス 3/2/1 にアタッチする方法を、次の例で示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth percent 25
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/2/1
Router(config-if)# service output policy1
Router(config-if)# end
```

show policy-map コマンドからの次の出力は、ポリシー マップ policy1 の設定を示します。

```
Router# show policy-map policy1

Policy Map policy1
Class class1
  Weighted Fair Queuing
    Bandwidth 50 (%) Max Threshold 64 (packets)
Class class2
  Weighted Fair Queuing
    Bandwidth 25 (%) Max Threshold 64 (packets)
```

show policy-map interface コマンドからの出力は、インターフェイス帯域幅の 50% がクラス class1 に対して保証され、25% がクラス class2 に対して保証されることを示しています。この出力には、帯域幅の量がパーセンテージと kbps の両方で示されています。

```
Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:policy1
Class-map:class1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
    Output Queue:Conversation 265
    Bandwidth 50 (%)
    Bandwidth 772 (kbps) Max Threshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0
Class-map:class2 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
    Output Queue:Conversation 266
    Bandwidth 25 (%)
```

```

Bandwidth 386 (kbps) Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0
Class-map:class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match:any

```

この例では、シリアル インターフェイス 3/2 に合計 1544 kbps の帯域幅があります。輻輳時には、帯域幅の 50% (772 kbps) がクラス class1 に保証され、リンク帯域幅の 25% (386 kbps) がクラス class2 に保証されます。

CBWFQ と LLQ の帯域幅割り当て : 例

次の例では、インターフェイスには合計で 1544 kbps の帯域幅があります。輻輳時には、帯域幅の 50% (772 kbps) がクラス class1 に保証され、リンク帯域幅の 25% (386 kbps) がクラス class2 に保証されます。

show policy-map コマンドからの次の出力例は、ポリシー マップ p1 の設定を示します。

```

Router# show policy-map p1
Policy Map p1
Class voice
  Weighted Fair Queuing
  Strict Priority
  Bandwidth 500 (kbps) Burst 12500 (Bytes)
Class class1
  Weighted Fair Queuing
  Bandwidth remaining 50 (%) Max Threshold 64 (packets)
Class class2
  Weighted Fair Queuing
  Bandwidth remaining 25 (%) Max Threshold 64 (packets)

```

シリアル インターフェイス 3/2 での **show policy-map interface** コマンドからの次の出力は、500 kbps の帯域幅がクラス voice1 に対して保証されることを示します。クラス class1 とクラス class2 はそれぞれ、残りの帯域幅の 50% と 25% を得ることができます。未割り当ての帯域幅は、class1、class2、およびベストエフォートトラフィッククラス間に比例して分配されます。



(注) 次の出力例では（この項で前出の多くの出力例とは異なり）、class1 と class2 に対する帯域幅の表示はパーセンテージのみです。kbps の数で表現される帯域幅は、**percent** キーワードが **bandwidth remaining** コマンドで使用されたため、表示されていません。**bandwidth remaining percent** コマンドでは、インターフェイスで使用可能な全帯域幅の相対パーセンテージとして帯域幅を割り当てることができます。

```

Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:p1
Class-map:voice (match-all)

```

```

0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match:ip precedence 5
Weighted Fair Queuing
  Strict Priority
  Output Queue:Conversation 264
  Bandwidth 500 (kbps) Burst 12500 (Bytes)
  (pkts matched/bytes matched) 0/0
  (total drops/bytes drops) 0/0
Class-map:class1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match:none
Weighted Fair Queuing
  Output Queue:Conversation 265
  Bandwidth remaining 50 (%) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class2 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match:none
Weighted Fair Queuing
  Output Queue:Conversation 266
  Bandwidth remaining 25 (%) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match:any

```

ATM のトラフィック シェーピング オーバーヘッド アカウンティング : 例

親ポリシーで ATM オーバーヘッド アカウンティングが有効になっている場合は、**bandwidth** コマンドまたは **shape** コマンドを含まない子トラフィック クラス上で ATM オーバーヘッド アカウンティングを有効にする必要はありません。次に、**subscriber_classes** という名前の子ポリシー マップの **gaming** クラスと **class-default** クラス、および、**subscriber_line** という名前の親ポリシー マップの **class-default** クラスで ATM オーバーヘッド アカウンティングが帯域幅に対してイネーブルである設定例を示します。voip クラスおよび video クラスでは、ATM オーバーヘッド アカウンティングが明示的に有効になっていません。これらのプライオリティキューは、親ポリシーで ATM オーバーヘッド アカウンティングが有効になっているため、オーバーヘッド アカウンティングは暗黙的に有効になります。親ポリシーと子ポリシーの機能で同じカプセル化タイプが使用されていることに注意してください。

```

Router(config)# policy-map subscriber_classes
Router(config-pmap)# class voip
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
Router(config-pmap)# class video
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# police 20
Router(config-pmap-c)# exit
Router(config-pmap)# class gaming
Router(config-pmap-c)# bandwidth remaining percent 80 account aal5 snap-rbe-dot1q

```



```

Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# policy-map subscriber_line
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining ratio 10 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# shape average 512 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# service policy subscriber_classes

```

次の例では、ルータは ATM オーバーヘッドの計算に 20 のオーバーヘッドバイトと ATM セル タックスを使用します。子ポリシーと親ポリシーには必須の一致オフセット値が含まれています。親ポリシーが virtual template 1 に適用されます。

```

Router(config)# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 500 account user-defined 20 atm
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# shape average 30000 account user-defined 20 atm
Router(config-pmap)# exit
Router(config)# exit
Router(config)#

```

関連コマンド

コマンド	説明
class(policy-map)	クラスのポリシーを設定する前に、ポリシーを作成または変更するクラスの名前、およびデフォルトクラス（一般に class-default クラスとして知られるクラス）を指定します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
max-reserved-bandwidth	CBWFQ、LLQ、および IP RTP プライオリティに割り当てるインターフェイス帯域幅のパーセント比率を変更します。
policy-map	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。
priority	ポリシーマップに属するトラフィックのクラスのプライオリティを指定します。
queue-limit	キューが保持できる、ポリシーマップ内に設定されるクラスポリシーのパケットの最大数を指定または変更します。
random-detect(interface)	WRED または DWRED をイネーブルにします。

コマンド	説明
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectprecedence	特定の IP precedence に対する WRED パラメータと DWRED パラメータを設定します。
showpolicy-map	指定されたサービスポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、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 packets 統計情報を表示します。

bandwidth qos-reference

物理インターフェイスまたは論理インターフェイスに関する Quality of Service (QoS) のパーセント設定の割合を計算するための参照として使用される帯域幅を設定するには、インターフェイス コンフィギュレーションまたは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 **bandwidthqos-reference** コマンドを使用します。この明示的に指定された参照帯域幅を削除するには、このコマンドの **no** 形式を使用します。

bandwidth qos-reference *bandwidth-amount*

no bandwidth qos-reference *bandwidth-amount*

構文の説明

<i>bandwidth-amount</i>	キロビット/秒 (kb/秒) の帯域幅の量。有効な値は 1 ~ 10000000 です。
-------------------------	--

コマンド デフォルト

このコマンドはディセーブルです。論理インターフェイスの参照帯域幅は、メインインターフェイスまたはメインインターフェイスの QoS ポリシーから取得されます。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

サブインターフェイス コンフィギュレーション (config-subif)

コマンド履歴

リリース	変更箇所
12.2(33)XNE	このコマンドが導入されました。
15.1(3)T	論理インターフェイスのサポートが、メインインターフェイス、サブインターフェイス、フレームリレーを含むように拡張されます。
Cisco IOS XE リリース 3.17S	このコマンドが変更されました。論理インターフェイスのサポートが、メインインターフェイスと、サブインターフェイスに拡張されました。このコマンドが、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに実装されました。

使用上のガイドライン

bandwidthqos-reference コマンドは、論理インターフェイスの QoS パーセント設定の割合を計算するための参照としてのみ使用されます。このコマンドは、論理インターフェイスに対して指定した量の帯域幅を実際に割り当てるわけではありません。



(注) Cisco IOS Release 12.2(33)XNE では、**bandwidthqos-reference** コマンドは、トンネル論理インターフェイスでのみサポートされます。Cisco IOS Release 15.1(3)T では、メインインターフェイス、サブインターフェイス、フレームリレー、およびトンネル論理インターフェイスを含むようにサポートが拡張されています。

shape (パーセント) コマンドと **police** (パーセント) コマンドの互換性

bandwidthqos-reference コマンドは、**shape** (パーセント) コマンドおよび **police** (パーセント) コマンドとの互換性があり、これらのコマンドに関連します。**shape** (パーセント) コマンドを使用すると、インターフェイスで利用可能な帯域幅のパーセンテージに基づいて、平均レートまたはピーク レートのトラフィック シェーピングを設定できます。**police** (パーセント) コマンドを使用すると、インターフェイスで利用可能な帯域幅の割合に基づいて、トラフィック ポリシングを設定できます。

bandwidthqos-reference コマンドは、**shape** (パーセント) コマンドおよび **police** (パーセント) コマンドと、次のようにやりとりします。

- **bandwidthqos-reference** コマンドを使用して帯域幅が指定された場合、**shape** (パーセント) コマンドおよび **police** (パーセント) コマンドは、この指定された量を使用して、それぞれの帯域幅比率を計算します。
- 帯域幅の指定に **bandwidthqos-reference** コマンドが使用されない場合、**shape** (パーセント) コマンドと **police** (パーセント) コマンドは、インターフェイスで利用可能な帯域幅の量を使用して、それぞれの帯域幅比率を計算します。

bandwidth (インターフェイス) コマンドとの互換性

bandwidth (インターフェイス) コマンドを使用すると、インターフェイスに対して継承され、受け取った帯域幅値を設定できます。

bandwidth (インターフェイス) コマンドと **bandwidthqos-reference** コマンドの両方が任意のインターフェイスで有効になっている場合、**bandwidthqos-reference** コマンドによって指定された値は、その特定の物理インターフェイスまたは論理インターフェイスの QoS パーセント設定の割合を計算するための参照として使用されます。**bandwidth** (インターフェイス) コマンドによって指定された値は、無視されます。

以下のサンプル設定で、**bandwidthqos-reference** コマンドの値は 8000 kb/秒、**bandwidth** (インターフェイス) コマンドの値は 900 kb/秒として入力されています。**shapeaveragepercent** コマンドの値は、50 に設定されています。4000000 ビット/秒 (8000 kb/秒の 50 パーセント) に設定されている **targetshaperate** コマンドの出力で、その効果は次のように確認できます。

```
Router(config)# interface e0/1
Router(config-if)# bandwidth qos-reference 8000
Router(config-if)# bandwidth 900

Router(config)# interface e0/1
Router(config-if)# bandwidth 900
Router(config-if)# end
Router# show running-config interface e0/1
interface Ethernet0/1
  bandwidth 900
  bandwidth qos-reference 8000
  no ip address
  load-interval 30
end
Router(config-if)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# interface e0/1
Router(config-if)# service-policy out test
Router# show policy-map interface
```

```

Ethernet0/1
Service-policy output: test
Class-map: class-default (match-any)
  79 packets, 7837 bytes
  30 second offered rate 0 bps, drop rate 0 bps
Match: any
Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 79/7837
  shape (average) cir 4000000, bc 40000, be 40000
  target shape rate 4000000

```

例

bandwidthqos-reference コマンドを設定し、トンネル インターフェイス 1 に対して参照の割合として 2000 kb/秒の帯域幅を割り当てる方法を、次の例に示します。

```

Router> enable
Router# configure terminal
Router(config)# interface tunnell
Router#(config-if)# bandwidth qos-reference 2000

```

bandwidthqos-reference コマンドを設定し、メイン インターフェイス e0/1 に対して参照の割合として 700 kb/秒の帯域幅を使用する方法を、次の例に示します。

```

Router(config)# interface e0/1
Router(config-if)# bandwidth qos-ref 700
Router(config-if)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# interface e0/1
Router(config-if)# service-policy out test

```

bandwidthqos-reference コマンドを設定し、サブインターフェイス e0/1.1 に対して参照の割合として 500 kb/秒の帯域幅を使用する方法を、次の例に示します。

```

Router(config-subif)# interface e0/1
Router(config-if)# no service-policy out test
Router(config-if)# interface e0/1.1
Router(config-subif)# bandwidth qos-ref 500
Router(config-subif)# service-policy ou test

```

bandwidthqos-reference コマンドを設定し、フレーム リレー インターフェイス s6/0.1 に対して参照の割合として 400 kb/秒の帯域幅を使用する方法を、次の例に示します。

```

Router(config)# no policy-map test
Router(config)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# map-class frame-relay fr1
Router(config-map-class)# service-policy out test
Router(config-map-class)# end
Router# configure terminal
Router(config)# interface s6/0.1
Router(config-subif)# bandwidth qos-ref 400
Router(config-subif)# end

```

関連コマンド	コマンド	説明
	bandwidth (インターフェイス)	インターフェイスに対して継承され、受け取った帯域幅の値を設定します。
	police (パーセント)	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
	shape (パーセント)	インターフェイスで使用可能な帯域幅の割合 (%) に基づいて、平均レート トラフィック シェーピングとピーク レート トラフィック シェーピングを指定します。

bandwidth remaining ratio

超過帯域幅（優先トラフィックによって使用されていない帯域幅）の量を判断し、非プライオリティキューに割り当てるために、輻輳時に使用するクラスレベルまたはサブインターフェイスレベルのキューの帯域幅残量割合を指定するには、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、**bandwidthremainingratio** コマンドを使用します。帯域幅残量割合を削除するには、このコマンドの **no** 形式を使用します。

bandwidth remaining ratio *ratio*

no bandwidth remaining ratio *ratio*

bandwidth remaining ratio *ratio* [**account** {**qinq|dot1q**} [**aal5**]
{*subscriber-encapsulation|user-defined* *offset*}]

no bandwidth remaining ratio *ratio* [**account** {**qinq|dot1q**} [**aal5**]
{*subscriber-encapsulation|user-defined* *offset*}]

bandwidth remaining ratio *ratio*

no bandwidth remaining ratio *ratio*

構文の説明

<i>ratio</i>	その他のサブインターフェイスまたはクラス キューに関する、このサブインターフェイスまたはクラス キューの相対的ウェイト。有効な値は1～1000です。サブインターフェイス レベルでは、デフォルト値はプラットフォームに依存します。クラス キュー レベルでは、デフォルト値は1です。
Cisco 7300 シリーズ ルータ、Cisco 7600 シリーズルータ、および Cisco 10000 シリーズ ルータ	
<i>ratio</i>	その他のサブインターフェイスまたはクラス キューに関する、このサブインターフェイスまたはクラス キューの相対的ウェイト。 (注) Cisco 7300 シリーズ ルータおよび7600 シリーズルータの有効値は1から10000です。また、デフォルト値は1です。 (注) Cisco 10000 シリーズ ルータの有効値は1～1000です。また、デフォルト値は1です。
account	(オプション) ATM オーバーヘッド アカウンティングを有効にします。
qinq	(オプション) キューインキューのカプセル化をブロードバンドリモート アクセス サーバ-デジタル加入者線アクセス マルチプレクサ (BRAS-DSLAM) カプセル化タイプとして指定します。

dot1q	(オプション) IEEE 802.1Q VLAN カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。
aal5	(オプション) コネクション型可変ビット レート (VBR) サービスをサポートする ATM アダプテーション層 5 を指定します。
<i>subscriber-encapsulation</i>	(オプション) 加入者線でのカプセル化タイプを指定します。カプセル化タイプは、加入者線によって異なります。
user-defined offset	(オプション) ルータでの ATM オーバーヘッド計算に使用するオフセット サイズ (バイト単位) を指定します。 (注) Cisco 7300 シリーズルータおよび 7600 シリーズルータの場合、有効値は -48 ~ +48 です。 (注) Cisco 10000 シリーズルータの有効値は -63 ~ +63 です。
Cisco ASR 1000 シリーズルータ	
<i>ratio</i>	その他のサブインターフェイスまたはクラス キューに関する、このサブインターフェイスまたはクラス キューの相対的ウェイト。有効な値は 1 ~ 1000 です。サブインターフェイス レベルおよびクラス キュー レベルでは、デフォルトは 1 です。

コマンド デフォルト

ほとんどのプラットフォームでは、デフォルトの帯域幅比率は 1 です。

サブインターフェイス レベルでデフォルトの帯域幅残量割合を使用すると、Cisco 10000 シリーズルータは インターフェイス タイプを識別します。サブインターフェイス レベルでは、デフォルトの帯域幅残量割合は、VLAN サブインターフェイスとフレーム リレー データ リンク 接続識別子 (DLCI) で 1 です。ATM サブインターフェイスの場合、ルータはサブインターフェイス速度に基づいてデフォルトの帯域幅残量割合を計算します。

クラス レベルでデフォルトの帯域幅残量割合を使用すると、Cisco 10000 シリーズルータは インターフェイス タイプを識別しません。クラス レベルでは、デフォルトの帯域幅残量割合は 1 です。

コマンド モード

ポリシーマップ クラス (config-pmap-c)

コマンド履歴

リリース	変更箇所
12.2(31)SB2	このコマンドが導入されました。このコマンドが、PRE3 用の Cisco 10000 シリーズルータに実装されました。

リリース	変更箇所
12.2(33)SRC	このコマンドが変更されました。コマンドは、Cisco 7600 シリーズルータに実装されました。Cisco 7600 シリーズルータおよびPRE3用のCisco 10000 シリーズルータで ATM オーバーヘッド アカウンティング (オプション) をサポートするため、さらにキーワードおよび引数が追加されました。
12.2(33)SB	このコマンドが変更されました。Cisco 7300 シリーズルータのサポートが追加されました。ATM オーバーヘッドアカウンティングに関連付けられた追加のキーワードと引数もサポートされるようになりました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン Cisco 10000 シリーズルータ

スケジューラは、**bandwidthremainingratio** コマンドで指定された比率を使用して、超過帯域幅 (優先トラフィックによって使用されていない帯域幅) の量を判断し、輻輳時にクラスレベルキューまたはサブインターフェイスレベルキューの帯域幅残量割合に割り当てます。他のキューまたはサブインターフェイスに対して未使用になっている帯域幅がスケジューラにより割り当てられます。

bandwidthremainingratio コマンドは、同一のポリシーマップの異なるトラフィッククラス内で、別の **bandwidth** コマンドと共存できません。たとえば、次の設定は無効であるため、エラーメッセージが表示されます。

```
policy-map Precl
  class precedence_0
    bandwidth remaining ratio 10
  class precedence_2
    bandwidth 1000
```

PRE2 の場合、**bandwidthremainingratio** コマンドは、ポリシーマップの同一クラス内で別の **bandwidth** コマンドと共存できます。PRE3 では、**bandwidthremainingratio** コマンドは、同一クラスの別の **bandwidth** コマンドと共存できます。たとえば、PRE3 では、次の設定は無効であるため、エラーメッセージが表示されます。

```
policy-map Precl
  class precedence_0
    bandwidth 1000
    bandwidth remaining ratio 10
```

階層型ポリシーマップで、適用済みの子キューイングポリシーで定義された class-default クラスのみしか親ポリシーが持っていない場合、ルータは class-default クラスで **bandwidth** コマンドの **bandwidthremainingratio** 形式のみを受け入れます。

bandwidthremainingratio コマンドは、同一クラスの **priority** コマンドと共存できません。たとえば、次の設定は無効であるため、エラーメッセージが表示されます。

```
policy-map Precl
```

```
class precedence_1
  priority
  police percent 30
  bandwidth remaining ratio 10
```

bandwidthremainingratio コマンドが指定されていないすべてのキューは、プラットフォームが指定された最小帯域幅残量割合を取得します。ルータは、設定に基づいて最小の設定情報レート (CIR) を決定します。

ATM オーバーヘッド アカウンティング (オプション)

bandwidthremainingratio コマンドを使用して、ATM オーバーヘッドアカウンティングを有効にすることもできます。ATM オーバーヘッドアカウンティングを有効にするには、「構文の説明」の表で説明されているように **account** キーワードおよび後続のキーワードと引数を使用します。

Cisco 7200 シリーズ ルータ

Cisco 7200 シリーズ ルータでは、**bandwidthremainingratio** コマンドはサポートされていません。Cisco IOS Release 12.2(33)SRD から Cisco IOS Release 12.2(33)SRE にアップグレードした場合は、このコマンドの実行時にパーサー エラーが表示される場合があります。Cisco 7200 シリーズルータでは、**bandwidthremainingratio** コマンドの代わりに **bandwidthremainingpercent** コマンドを使用して同じ機能を得ることができます。

例

Cisco 7300 シリーズ ルータ、Cisco 7600 シリーズ ルータ、および Cisco 10000 シリーズ ルータ

ATM サブインターフェイスで帯域幅残量割合を設定する方法を、次の例に示します。この例では、ルータは、可変ビットレートの非リアルタイム (VBR-nrt) PVC 0/200 に対して 50 Mbps のピークセルレートを保証します。輻輳の期間中、サブインターフェイスは、物理インターフェイスで設定されたその他のサブインターフェイスに対し、帯域幅残量割合 10 をベースとして、超過帯域幅 (優先トラフィックによって使用されていない帯域幅) の共有を取得します。

```
policy-map Child
  class precedence_0
    bandwidth 10000
  class precedence_1
    shape average 100000
    bandwidth 100
  !
policy-map Parent
  class class-default
    bandwidth remaining ratio 10
    shape average 20000000
    service-policy Child
  !
interface ATM2/0/3.200 point-to-point
  ip address 10.20.1.1 255.255.255.0
  pvc 0/200
  protocol ip 10.20.1.2
  vbr-nrt 50000
  encapsulation aal5snap
  service-policy output Parent
```

個々のクラスキューに対して帯域幅残量割合を設定する方法を、次の例に示します。設定済みクラスの一部には、明示的に指定された帯域幅保証と帯域幅残量割合があります。サブインターフェイスレベルで輻輳が発生した場合、クラスキューは、クラスレベルの帯域幅残量割合に基づいて超過帯域幅（優先トラフィックによって使用されていない帯域幅）を取得します。この割合は、precedence_0、precedence_1、precedence_2、およびprecedence_5クラスでそれぞれ、20、30、120、および100です。通常、precedence_3クラス（定義済み割合なし）は、子ポリシーに定義されたclass-defaultクラスの帯域幅残量割合に基づいて帯域幅を取得します。しかし、この例では、子ポリシーはclass-default帯域幅残量割合を定義していません。したがって、ルータは、precedence_3トラフィックに対して比率1の超過帯域幅を割り当てます。

```
policy-map Child
  class precedence_0
    shape average 100000
    bandwidth remaining ratio 20
  class precedence_1
    shape 10000
    bandwidth remaining ratio 30
  class precedence_2
    shape average 200000
    bandwidth remaining ratio 120
  class precedence_3
    set ip precedence 3
  class precedence_5
    set ip precedence 5
    bandwidth remaining ratio 100
policy-map Parent
  class class-default
    bandwidth remaining ratio 10
    service-policy Child
!
interface GigabitEthernet 2/0/1.10
  encapsulation dot1q 10
  service-policy output Parent
```

オーバーヘッドアカウンティング：例

オプションの **account** キーワードおよび関連付けられたキーワードや引数を使用してオーバーヘッドアカウンティングを設定する方法を、次の例に示します。

```
policy-map subscriber_line
  class class-default
    bandwidth remaining ratio 10 account dot1q aal5 snap-rbe-dot1q
    shape average 512 account dot1q
  aal5 snap-rbe-dot1q
  service policy subscriber_classes
```

関連コマンド	コマンド	説明
	bandwidthremainingpercent	クラスレベルまたはサブインターフェイスレベルのキューの帯域幅残量パーセンテージを指定します。この帯域幅残量パーセンテージは、優先トラフィックによって使用されていない余分な帯域幅の量を判断し、非プライオリティキューに割り当てるために輻輳時に使用します。
	showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
	showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、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 packets 統計情報を表示します。

bump

VCバンドルに割り当てることができる仮想回線（VC）クラスのバンピングルールを設定するには、VC-class コンフィギュレーションモードで **bump** コマンドを使用します。このクラスに割り当てられているVCの明示的なバンピングルールを削除し、デフォルトの状態である暗黙的なバンピングに戻すには、**nobumpexplicit** コマンドまたは **bumpimplicit** コマンドを使用します。VCバンドルメンバーがバンピングされたトラフィックを受け入れないように指定するには、このコマンドの **no** 形式を使用します。

バンドルの特定のVCまたは相手先固定接続（PVC）メンバーにバンピングルールを設定するには、**bundle-vc** または **SVC-bundle-member** コンフィギュレーションモードで **bump** コマンドを使用します。VCまたはPVCバンドルメンバーの明示的なバンピングルールを削除し、デフォルトの状態である暗黙的なバンピングに戻すには、**bumpimplicit** コマンドを使用します。VCまたはPVCバンドルメンバーがバンピングされたトラフィックを受け入れないように指定するには、**nobumptraffic** コマンドを使用します。

```
bump {explicit precedence-level|implicit|traffic}
no bump {explicit precedence-level|implicit|traffic}
```

構文の説明

explicit <i>precedence-level</i>	VCまたはPVCが停止した場合に、VCまたはPVC上のトラフィックがバンピングされる優先レベルを指定します。 <i>precedence-level</i> 引数の有効な値は0～7です。
implicit	デフォルトの暗黙的なバンピングルールを単一のVC、PVCバンドルメンバー、またはバンドル内のすべてのVCに適用します（VC-classモード）。暗黙的なバンピングルールは、バンピングされたトラフィックがVCまたはPVCによって低い優先レベルで送信されるように規定します。
traffic	VCまたはPVCがバンピングされたトラフィックを受け入れるように指定します（デフォルトの状態）。 no 形式は、VCまたはPVCがバンピングされたトラフィックを受け入れないように規定します。

コマンドデフォルト

暗黙的なバンピング

バンピングを許可（VCはバンピングされたトラフィックを受け入れます）

コマンドモード

Vc-class コンフィギュレーション（VCクラスの場合）

Bundle-vc コンフィギュレーション（ATM VCバンドルメンバーの場合）

SVC-bundle-member コンフィギュレーション（SVCバンドルメンバーの場合）

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。

リリース	変更箇所
12.2(4)T	このコマンドが、SVC-bundle-member コンフィギュレーションモードで使用できるようになりました。
12.0(23)S	このコマンドが、Cisco 12000 シリーズインターネットルータで8ポートの OC-3 STM-1 ATM ラインカードの VC-class および bundle-vc コンフィギュレーションモードで使用できるようになりました。
12.0(26)S	このコマンドが Cisco IOS Release 12.0(26)S に統合され、Cisco 10000 シリーズルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

使用上のガイドライン

個々の VC または PVC バンドルメンバーに対してバンピングルールを設定するには、`bundle-vc` コンフィギュレーションモード (ATM VC バンドルメンバーの場合) または `SVC-bundle-member` コンフィギュレーションモード (SVC バンドルメンバーの場合) で **bump** コマンドを使用します。バンドルメンバーに割り当てることができる VC クラスを設定するには、`VC-class` コンフィギュレーションモードで **bump** コマンドを使用します。

異なるバンピング設定のアプローチの効果は、次のようになります。

- 暗黙的なバンピング：暗黙的なバンピングを設定すると、バンピングされたトラフィックは、次に低い優先レベルを処理するように設定された VC または PVC に送信されます。トラフィックをバンピングした元の VC または PVC が復帰した場合は、その VC または PVC によって送信するように設定されていたトラフィックが復元されます。他のポジティブな形式の **bump** コマンドが設定されていない場合は、**bumpimplicit** コマンドが有効になります。
- 明示的なバンピング：**bumpexplicit** コマンドを使用して VC または PVC を設定する場合は、VC または PVC が停止したときにトラフィックがバンピングされる優先レベルを指定できます。これにより、トラフィックはその優先レベルでマッピングされた VC または PVC に送信されます。そのトラフィックを引き受け、伝送する VC または PVC が停止した場合、トラフィックはその VC または PVC のバンピングルールに従います。バンピングで指定できる優先レベルは 1 つのみです。
- バンピングを許可：VC または PVC は、デフォルトでバンピングされたトラフィックを受け入れます。VC または PVC がバンピングされたトラフィックを拒否するように以前に設定されていた場合は、**bumptraffic** コマンドを使用して VC または PVC をデフォルトの状態に戻す必要があります。

- バンピングを拒否：個々の VC または PVC に対してバンピングされたトラフィックが送信された場合に拒否するように設定するには、**nobumptraffic** コマンドを使用します。



(注) バンピングされたトラフィックを処理する代替の VC または PVC が見つからない場合は、バンドルは停止したものと宣言されます。これが発生するのを回避するには、最低の優先レベルを持つバンドルメンバーの VC または PVC を明示的に設定します。

このコマンドを **VC-class** コンフィギュレーションモードで使用するには、このコマンドを入力する前に **vc-classatm** グローバル コンフィギュレーション コマンドを入力する必要があります。

このコマンドを使用して **bundle-VC** コンフィギュレーションモードで個々のバンドルメンバーを設定するには、まず **bundle** コマンドを発行し、設定する VC メンバーを追加または変更するバンドルのバンドル コンフィギュレーションモードに入ります。その後、**pvc-bundle** コマンドを使用して、作成または変更する VC を指定し、バンドル VC コンフィギュレーションモードにします。

コマンドを含む VC クラスがスタンドアロン VC (バンドルメンバーではない VC) に付加されている場合、このコマンドは効果がありません。この場合、属性は VC によって無視されます。

VC バンドルの VC は、次の設定継承ガイドラインに従います (2 番目に高い優先順位の順にリストされています)。

- **bundle-VC** モードの VC 設定
- バンドルモードのバンドル設定 (および、割り当てられた **VC-class** コンフィギュレーションの影響)
- サブインターフェイスモードのサブインターフェイス設定

例

次の例では、「five」というクラスを設定し、バンドル内の VC に適用可能なパラメータを定義しています。VC が停止した場合、トラフィックは優先レベル 7 にマッピングされた VC に送信 (明示的にバンピング) されます。

```
vc-class atm five
ubr 5000
precedence 5
bump explicit 7
```

次の例では、「premium-class」というクラスを設定し、バンドル内の VC に適用可能なパラメータを定義しています。**bundle-vc bump** 設定で上書きされない限り、このクラスを使用する VC は他のトラフィックがこの VC にバンピングされることを許可しません。

```
vc-class atm premium-class
no bump traffic
bump explicit 7
```

関連コマンド	Command	Description
	bundle	バンドル コンフィギュレーションモードに入って、バンドルを作成するか、または既存のバンドルを変更します。
	class	PVC または PVC バンドル メンバーにマップ クラスまたは VC クラスを割り当てます。
	class-vc	VC クラスを ATM PVC、SVC、または VC バンドル メンバーに割り当てます。
	dscp(frame-relayvc-bundle-member)	特定のフレーム リレー PVC バンドル メンバーに対して DSCP 値を指定します。
	precedence	VC バンドルまたは PVC バンドルに割り当てることができ、したがって、そのバンドルのすべてのメンバーに適用される、VC クラスまたは PVC クラスの優先レベルを設定します。
	protect	VC または PVC バンドル メンバーに適用するための保護されたグループあるいは保護された VC または PVC ステータスを使用して、VC または PVC クラスを設定します。
	pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーションモードに入ります。
	pvc(frame-relayvc-bundle)	PVC および PVC バンドル メンバーを作成し、frame-relay vc-bundle-member コンフィギュレーションモードに入ります。
	svc-bundle	SVC バンドルのメンバーを作成または変更します。
	ubr	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピークセルレートを指定します。
	ubr+	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピークセルレートと出力最小保証セルレートを指定します。
	vbr-nrt	可変ビットレート非リアルタイム (VBR-NRT) QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピークセルレート、出力平均セルレート、および、出力最大バーストセルサイズを指定します。
	vc-classatm	VC クラス、ATM VC、またはインターフェイスを設定します。

bundle

バンドルを作成するか、既存のバンドルを変更してバンドル コンフィギュレーション モードに入るには、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 **bundle** コマンドを使用します。指定したバンドルを削除するには、このコマンドの **no** 形式を使用します。

bundle *bundle-name*
no bundle *bundle-name*

構文の説明

<i>bundle-name</i>	作成するバンドルの名前。長さの制限は16文字までです。
--------------------	-----------------------------

コマンドデフォルト

バンドルは指定されていません。

コマンドモード

サブインターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.0(26)S	このコマンドが Cisco IOS Release 12.0(26)S に統合され、Cisco 10000 シリーズルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

バンドル コンフィギュレーション モード内から、バンドルとそのメンバーの特性および属性を設定できます。これには、バンドル内のすべての仮想回線 (VC) のカプセル化タイプ、バンドル管理パラメータ、サービス タイプなどがあります。バンドル コンフィギュレーション モードで設定する属性およびパラメータは、バンドルのすべての VC メンバーに適用されます。

VC バンドルの VC は、次の設定継承ガイドラインに従います (2 番目に高い優先順位の順にリストされています)。

- bundle-VC モードの VC 設定
- バンドル モードでのバンドル コンフィギュレーション
- サブインターフェイス モードのサブインターフェイス設定

バンドルのステータスを表示するには、**showatmbundle** コマンドと **showatmbundlestatistics** コマンドを使用します。

例

次に、「**bundle1**」というバンドルを設定する方法の例を示します。この例では、サブインターフェイスの IP アドレスとルータのプロトコル（ルータは IP ルーティングプロトコルとして Intermediate System-to-Intermediate System (IS-IS) を使用）を指定してからバンドルを設定しています。

```
interface atm1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 ip router isis
 bundle bundle1
```

関連コマンド

コマンド	説明
class-bundle	指定された VC クラスに含まれるバンドル レベルのコマンドで VC バンドルを設定します。
oam-bundle	バンドルのすべての VC メンバー、または VC バンドルに適用できる VC クラスに対して、エンドツーエンドの F5 OAM ループバックセル生成と OAM 管理を有効にします。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーションモードに入ります。
showatmbundle	各バンドルの VC メンバに割り当てられたバンドルの属性と、VC メンバの現在の稼働ステータスを表示します。
showatmbundlestatistics	指定されたバンドルの統計を表示します。

bundle svc

相手先選択接続（SVC）バンドルを作成または変更するには、インターフェイスコンフィギュレーションモードで **bundlesvc** コマンドを使用します。指定したバンドルを削除するには、このコマンドの **no** 形式を使用します。

bundle svc *bundle-name* **nsap** *nsap-address*

no bundle svc *bundle-name* **nsap** *nsap-address*

構文の説明

<i>bundle-name</i>	ルータの SVC バンドルを識別する一意のバンドル名。仮想回線（VC）の各終端のバンドル名は同一である必要があります。長さの制限は16文字までです。
nsap <i>nsap-address</i>	SVC バンドルの宛先ネットワーク サービス アクセス ポイント（NSAP）アドレス。

コマンド デフォルト

SVC バンドルは作成または変更されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(4)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

このコマンドにより、システムは SVC バンドル コンフィギュレーション モードを開始します。バンドル名は、VC の両端で同一になっている必要があります。

SVC バンドル コンフィギュレーション モードから、バンドルとそのメンバーの特性および属性を設定できます。これには、バンドル内のすべての仮想回線（VC）のカプセル化タイプ、バンドル管理パラメータ、サービス タイプなどがあります。SVC バンドル コンフィギュレーションモードで設定する属性およびパラメータは、バンドルのすべての VC メンバーに適用されます。

VC バンドルの VC は、次の設定継承ガイドラインに従います（2 番目に高い優先順位の順にリストされています）。

- bundle-VC モードの VC 設定
- バンドル モードでのバンドル コンフィギュレーション

- サブインターフェイス モードのサブインターフェイス設定

バンドルのステータスを表示するには、**showatmbundlesvc** コマンドと **showatmbundlesvcstatistics** コマンドを使用します。

例

次に、「sanfrancisco」という SVC バンドルを設定する方法の例を示します。

```
interface ATM1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 atm esi-address 111111111111.11
 bundle svc sanfrancisco nsap 47.0091810000000003E3924F01.999999999999.99
 protocol ip 10.0.0.2
broadcast
 oam retry 4 3 10
 encapsulation aal5snap
 oam-bundle manage
 svc-bundle seven
 class-vc seven
 svc-bundle six
 class-vc six
 svc-bundle five
 class-vc five
 svc-bundle four
 class-vc four
 svc-bundle three
 class-vc three
 svc-bundle two
 class-vc two
 svc-bundle one
 class-vc one
 svc-bundle zero
 class-vc zero
```

関連コマンド

コマンド	説明
class-bundle	指定された VC クラスに含まれるバンドルレベルのコマンドで VC バンドルを設定します。
oam-bundle	バンドルのすべての VC メンバー、または VC バンドルに適用できる VC クラスに対して、エンドツーエンドの F5 OAM ループバックセル生成と OAM 管理を有効にします。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーション モードに入ります。
showatmbundlesvc	各バンドルの VC メンバに割り当てられたバンドルの属性と、VC メンバの現在の稼働ステータスを表示します。
showatmbundlesvcstatistics	指定されたバンドルの統計を表示します。

class (EtherSwitch)

クラスマップ名またはアクセスグループを使用してポリシーの適用対象となるトラフィック分類を定義するには、ポリシーマップコンフィギュレーションモードでこの **class** コマンドを使用します。既存のクラスマップを削除するには、このコマンドの **no** 形式を使用します。

```
class class-map-name [access-group acl-index-or-name]
no class class-map-name
```

構文の説明

<i>class-map-name</i>	クラスマップの名前。
access-group <i>acl-index-or-name</i>	(任意) IP 標準または拡張アクセスコントロールリスト (ACL) の番号または名前。IP 標準 ACL の場合、インデックス範囲は 1 ~ 99 および 1300 ~ 1999 です。また、IP 拡張 ACL の場合、インデックス範囲は 100 ~ 199 および 2000 ~ 2699 です。

コマンドデフォルト

ポリシーマップクラスマップは定義されません。

コマンドモード

ポリシーマップコンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータプラットフォームに実装されました。
12.3(4)T	このコマンドが、Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズルータ上の Cisco IOS Release 12.3(4)T に統合されました。

使用上のガイドライン

class (EtherSwitch) コマンドを使用する前に、**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ポリシーマップを識別し、ポリシーマップコンフィギュレーションモードを開始します。ポリシーマップを指定すると、ポリシーマップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。インターフェイスにポリシーマップを適用するには、**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ます。ただし、ACL 分類を使用しているポリシーマップを出力方向に適用することはできません。

ポリシーマップで指定したクラス名は、**class-map** グローバルコンフィギュレーションコマンドによる設定に従い、そのクラスの特性をクラスマップおよびその一致基準に連結します。

class (EtherSwitch) コマンドは、**class-map** グローバルコンフィギュレーションコマンドと同一の機能を実行します。他のポートと共有していない新しい分類が必要な場合は、**class (EtherSwitch)** コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用します。



- (注) ポリシー マップでは、「class-default」という名前のクラスがサポートされていません。イーサネットスイッチネットワーク モジュールは、**classclass-default** ポリシーマップ コンフィギュレーション コマンドで定義されるポリシー マップに基づいて、トラフィックをフィルタするわけではありません。

class (EtherSwitch) コマンドを入力すると、ポリシーマップ クラス コンフィギュレーション モードが開始されます。このモードでは、次のコンフィギュレーション コマンドを使用できます。

- **default** : コマンドをデフォルトに設定します。
- **exit** : ポリシーマップ クラス コンフィギュレーション モードを終了して、ポリシーマップ コンフィギュレーション モードに戻ります。
- **no** : コマンドをデフォルト設定に戻します。
- **police** : 分類したトラフィックにポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。詳細については、**police** コマンドを参照してください。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。



- (注) IP ACL の設定の詳細については、『Cisco IOS IP Application Services Configuration Guide』の「Configuring IP Services」の章を参照してください。

例

次の例では、「policy1」という名前のポリシーマップを作成する方法を示します。このコマンドが入力ポートに適用された場合、class1 で定義されたすべての着信トラフィックの照合を行い、平均レート 1 Mbps、バースト 131072 バイトでトラフィックをポリシングします。このプロファイルを超えたトラフィックはドロップされます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police 1000000 131072 exceed-action drop
Router(config-pmap-c)# exit
```

設定を確認するには、**showpolicy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class-map	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(class-mapconfiguration)	トラフィックを分類するための一致条件を定義します。

コマンド	説明
police	トラフィック ポリシングを設定します。
policy-map	サービスポリシーを指定するための、複数のインターフェイスに適用できるポリシー マップを作成または変更します。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showpolicy-map	QoS ポリシー マップを表示します。

class (ポリシー マップ)

ポリシーを作成または変更するクラスの名前を指定するには、またはクラスのポリシーを設定する前にデフォルトクラス（一般に **class-default** クラスとして知られるクラス）を指定するには、ポリシーマップ コンフィギュレーション モードで **class** コマンドを使用します。クラスをポリシー マップから削除するには、このコマンドの **no** 形式を使用します。

```
class {class-name|class-default [fragment fragment-class-name]} [insert-before class-name]
[service-fragment fragment-class-name]
no class {class-name|class-default}
```

構文の説明		
	<i>class-name</i>	設定するクラス、またはポリシーを編集するクラスの名前を指定します。クラス名は、クラス マップに使用するとともに、ポリシー マップのクラスにポリシーを設定する場合にも使用します。
	class-default	ポリシーを設定または変更できるようにデフォルト クラスを指定します。
	fragment f <i>ragment-class-name</i>	(任意) デフォルト トラフィック クラスをフラグメントに指定し、フラグメント トラフィック クラスに名前を付けます。
	insert-before <i>class-name</i>	(任意) 既存の任意の 2 つのクラス マップ間にクラス マップを追加します。 既存の 2 つのクラス マップ間に新しいクラス マップを挿入すると、既存のポリシー マップ コンフィギュレーションの柔軟性が向上します。このオプションを指定しないと、クラス マップはポリシー マップの末尾に追加されます。 このキーワードは、Flexible Packet Matching (FPM) ポリシーでだけサポートされています。
	service-fragment <i>fragment-class-name</i>	(任意) クラスがフラグメントのコレクションを分類するように指定します。このクラスにより分類されるフラグメントは、すべて同じ <i>fragment-class-name</i> を共有する必要があります。

コマンド デフォルト クラスの指定はありません。

コマンド モード

ポリシー マップ コンフィギュレーション (config-pmap)

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。

リリース	変更箇所
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.2(14)SX	このコマンドのサポートが、Cisco 7600 ルータに追加されました。
12.2(17d)SXB	このコマンドが、Cisco 7600 ルータに実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.2(18)SXE	class-default キーワードが Cisco 7600 ルータに追加されました。
12.4(4)T	insert-beforeclass-name オプションが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(31)SB2	このコマンドが、Cisco 10000 シリーズ ルータの PRE3 に追加されました。
12.2(18)ZY	insert-beforeclass-name オプションが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator (PISA) が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。 fragmentfragment-class-name オプションと service-fragmentfragment-class-name オプションが導入されました。

使用上のガイドライン ポリシー マップ コンフィギュレーション モード

ポリシー マップ内で、**class(policy-map)** コマンドを使用すれば、ポリシーを作成または変更するクラスの名前を指定できます。まず、ポリシー マップを指定する必要があります。

ポリシー マップを指定して必要なポリシーマップ コンフィギュレーション モードを開始するには、**class(policy-map)** コマンドを使用する前に **policy-map** コマンドを使用します。ポリシー マップを指定した後は、新しいクラスのポリシーを設定したり、そのポリシーマップ内の任意の既存クラスのポリシーを変更したりできます。

クラス特性

ポリシーマップで指定するクラス名により、そのクラス特性 (つまりポリシー) が、**class-map** コマンドを使用して設定したとおりに、クラス マップおよびその一致基準に関連付けられません。

クラスのポリシーを設定し、その帯域幅を指定し、ポリシーマップをインターフェイスに割り当てると、クラス ベース **Weighted Fair Queueing (CBWFQ)** によって、そのクラスの帯域幅要件が満たされているかどうか判断されます。満たされていれば、CBWFQ がその帯域幅要件のキューを割り当てます。

クラスが削除されると、インターフェイスに使用できる帯域幅が、そのクラスにそれまで割り当てられていた量だけ増加します。

ルータに（つまり 1 つのポリシー マップ内で）設定できるクラスの最大数は、64 個です。

定義済みのデフォルト クラス

`class-default` と呼ばれる定義済みのデフォルト クラスを指定するには、**class-default** キーワードを使用します。`class-default` クラスは、トラフィックがクラス マップ内で設定されているどの一致基準とも一致しない場合に、そのトラフィックが送られるクラスです。

テール ドロップまたは WRED

クラス ポリシーを定義するには、テール ドロップを使用（**queue-limit** コマンドを実行）するか、または重み付けランダム早期検出（WRED）を使用（**random-detect** コマンドを実行）することができます。テール ドロップまたは WRED を使用する場合は、次の点に注意してください。

- **queue-limit** コマンドと **random-detect** コマンドの両方を同じクラス ポリシー内で使用することはできませんが、同じポリシー マップ内の 2 つのクラス ポリシー内で使用することは可能です。
- クラス ポリシーで **queue-limit** コマンドまたは **random-detect** コマンドのいずれかを設定すると、**bandwidth** コマンドを設定できます。**bandwidth** コマンドは、クラスに割り当てられる帯域幅の量を指定します。
- 定義済みのデフォルト クラスでは、**fair-queue (class-default)** コマンドを設定できます。**fair-queue** コマンドは、デフォルト クラスのダイナミック キューの数を指定します。**fair-queue** コマンドは、**queue-limit** コマンドまたは **random-detect** コマンドのいずれかと同じクラス ポリシーで使用できます。**bandwidth** コマンドと一緒に使用することはできません。

Fragments

デフォルト トラフィック クラスは、ポリシー マップ クラス ステートメントで **fragment** キーワードを使用して、フラグメントとしてマークされます。これにより、フラグメントを分類して、複数のフラグメントをまとめて **service-fragment** キーワードを使用して作成した別のポリシー マップに入れることができます。フラグメントが使用されると、フラグメントとしてマークされているデフォルト トラフィック クラスに、デフォルト以外のトラフィック クラスとは別に、QoS が適用されます。

フラグメントを使用する場合は、次のガイドラインに従ってください。

- フラグメントとしてマークできるのは、デフォルト トラフィック クラスだけです。
- デフォルト クラス ステートメントでの **fragment**`fragment-class-name` オプションが、デフォルト クラスをフラグメントとしてマークします。
- ポリシー マップのクラス定義時には **service-fragment**`fragment-class-name` オプションを使用し、同じ `fragment-class-name` を共有するすべてのフラグメントを含む Modular QoS CLI 内のトラフィックのクラスを指定します。
- フラグメントは、同一物理インターフェイス内でしか使用できません。同じ `fragment-class-name` を共有し、異なるインターフェイス上にあるフラグメントを持つポリ

シーマップを、**service-fragment/fragment-class-name** オプションを持つクラスを使用してひとまとめに分類することはできません。

Cisco 10000 シリーズ ルータ

PRE2 では、ポリシー マップで 31 個のクラス キューを設定できます。

PRE3 では、ポリシー マップで優先度レベル 1 のキューを 1 個、優先度レベル 2 のキューを 1 個、クラス キューを 12 個、デフォルト キューを 1 個設定できます。

Cisco ASR 1000 シリーズ ルータ

Cisco ASR 1000 シリーズ ルータに (つまり 1 つのポリシー マップ内で) 設定できるクラスの最大数は、8 個です。

例

次に、**policy1** というポリシー マップに含まれる 3 つのクラス ポリシーを設定する例を示します。**Class1** は、アクセス コントロール リスト 136 に一致するトラフィックのポリシーを指定します。**class2** は、インターフェイス **ethernet101** のトラフィックのポリシーを指定します。3 つ目のクラスは、設定済みの一致基準を満たさないパケットが送られるデフォルトクラスです。

```
! The following commands create class-maps class1 and class2
! and define their match criteria:
class-map class1
  match access-group 136
class-map class2
  match input-interface ethernet101
! The following commands create the policy map, which is defined to contain policy
! specification for class1, class2, and the default class:
policy-map policy1
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```

- **class1** : 輻輳の発生時に、このクラスに最低 2000 kbps の帯域幅が提供されることを予期しています。また、このクラスのために予約されるキューでは、テールドロップを実行して追加のパケットを処理する前に 40 個のパケットまでキューに登録できます。
- **class2** : 輻輳の発生時に、このクラスに最低 3000 Kbps の帯域幅が提供されることを予期しています。また、平均キューサイズの計算に重み係数 10 が使用されます。輻輳回避のために、テールドロップではなく WRED パケットのドロップが使用されます。
- デフォルトクラス : ポリシーがポリシー マップ **policy1** で定義されている他のクラスの一貫条件を満たさないトラフィック用に、16 個のダイナミック キューが予

約されています。また、キューあたり 20 個のパケットを超えると、追加でキューに格納されるパケットを処理するためにテールドロップが実施されます。



(注) このクラスを含むポリシーマップをインターフェイスに付加して、そのインターフェイスのサービスポリシーを規定するとき、設定されるすべてのクラスポリシーおよびリソース予約プロトコル (RSVP) を考慮し、使用可能な帯域幅が評価されます。

次に、`policy8` というポリシー マップに組み込まれるデフォルト クラスのポリシーを設定する例を示します。デフォルトのクラスには、次の特性があります。他のクラスの一致基準を満たさないトラフィックのために 20 個のダイナミック キューが利用でき、また、そのクラスのポリシーは `policy8` というポリシーマップによって定義され、重み係数 14 を使用して平均キュー サイズを計算します。輻輳回避のために、テールドロップではなく WRED パケット ドロップが使用されます。

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

次の例では、`policy1` というポリシー マップに含まれる `acl136` というクラスのためのポリシーを設定する方法を示します。クラス `acl136` には、次の特性があります。輻輳の発生時に、このクラスに最低 2000 kbps の帯域幅が提供されることを予期しています。また、このクラスのために予約されるキューでは、テールドロップを実行して追加のパケットを処理する前に 40 個のパケットまでキューに登録できます。このクラスを含むポリシーマップをインターフェイスに付加して、そのインターフェイスのサービスポリシーを規定するとき、設定されるすべてのクラスポリシーおよび RSVP を考慮し、使用可能な帯域幅が評価されるため、注意してください。

```
Router(config)# policy-map policy1
Router(config-pmap)# class acl136
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
```

次の例では、`policy8` というポリシー マップに含まれる `int101` というクラスのためのポリシーを設定する方法を示します。クラス `int101` には、次のような特性があります。輻輳の発生時に、このクラスに最低 3000 Kbps の帯域幅が提供されることを予期しています。また、平均キュー サイズの計算に重み係数 10 が使用されます。輻輳回避のために、テールドロップではなく WRED パケットのドロップが使用されます。このクラスが含まれているポリシー マップがインターフェイスに付加されて、そのインターフェイスのサービスポリシーが規定される場合、使用可能な帯域幅が評価されることに注意してください。

```
Router(config)# policy-map policy8
Router(config-pmap)# class int101
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
```

次に、**policy1** というポリシーマップに組み込まれる **class-default** デフォルトクラスのポリシーを設定する例を示します。**class-default** デフォルトクラスには、次の特性があります。ポリシーがポリシー マップ **policy1** で定義されている他のクラスの一一致条件を満たさないトラフィック用に、10 個のハッシュ キューが予約されています。また、キューあたり 20 個の packets を超えると、追加でキューに格納される packets を処理するためにテール ドロップが実施されます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config-pmap-c)# queue-limit 20
```

次に、**policy8** というポリシーマップに組み込まれる **class-default** デフォルトクラスのポリシーを設定する例を示します。**class-default** デフォルトのクラスには、次の特性があります。他のクラスの一一致基準を満たさないトラフィックのために 20 個のハッシュ キューが利用でき、また、そのクラスのポリシーは **policy8** というポリシー マップによって定義され、重み係数 14 を使用して平均キュー サイズを計算します。輻輳回避のために、テールドロップではなく WRED パケット ドロップが使用されます。

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

次に、ブラスタ パケット用に FPM を設定する方法の例を示します。クラス マップには、TCP ポート 135、4444 または UDP ポート 69、および IP ヘッダーの先頭から 3 バイトに 0x0030 のパターンが存在するという一致条件が含まれます。

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
  match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
  match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
  match field tcp dest-port eq 135
  match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
  match field tcp dest-port eq 4444
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
  match field udp dest-port eq 69
  match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
  class blaster1
  drop
  class blaster2
  drop
policy-map type access-control fpm-udp-policy
  class blaster3
  drop
policy-map type access-control fpm-policy
  class ip-tcp
  service-policy fpm-tcp-policy
  class ip-udp
```

```

service-policy fpm-udp-policy
interface gigabitEthernet 0/1
  service-policy type access-control input fpm-policy

```

次の例は、**BestEffort** というデフォルトのトラフィック クラスを分類するトラフィックのフラグメント クラスを作成する方法を示しています。**subscriber1** と **subscriber2** というポリシー マップからのすべてのデフォルトのトラフィックは、**BestEffort** というフラグメント デフォルトのトラフィック クラスの一部です。このデフォルトのトラフィックが、**service-fragment** キーワードと **shape** コマンドを使用する、**data** というクラスを作成することによってまとめてシェーピングされます。

この例では、次の点に注意してください。

- 各フラグメントデフォルトのトラフィッククラスの *class-name* は「BestEffort」です。
- *class-name* の「BestEffort」は、**service-fragment** キーワードが入力されるクラスの定義にも使用します。このクラスは、「BestEffort」というフラグメントデフォルトのトラフィッククラスを使用して転送されるすべてのトラフィックにシェーピングポリシーを適用します。

```

policy-map subscriber1
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map subscriber 2
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map input_policy
class class-default
set dscp default
policy-map main-interface
class data service-fragment BestEffort
shape average 400
interface portchannel1.1001
encapsulation dot1q 1001service-policy output subscriber1
service-policy input input_policy
interface portchannel1.1002
encapsulation dot1q 1002
service-policy output subscriber2
service-policy input input_policy
interface gigabitethernet 0/1
description member-link1
port channel 1
service-policy output main-interface
interface gigabitethernet 0/2

```

```

description member-link2
port channel 1

service-policy output main-interface

```

関連コマンド

Command	Description
bandwidth(policy-mapclass)	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
fair-queue(class-default)	デフォルト クラス ポリシーの一部として class-default クラスで使用するために予約するダイナミック キューの数を指定します。
policy-map	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。
queue-limit	キューが保持できる、ポリシー マップ内に設定されるクラス ポリシーのパケットの最大数を指定または変更します。
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detectexponential-weighting-constant	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
random-detectprecedence	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。

class-map arp-peruser

ユーザごとのパケットの Address Resolution Protocol (ARP) に一致するクラス マップを作成するには、グローバルコンフィギュレーションモードで **class-map arp-peruser** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

class-map arp-peruser
no class map arp-peruser

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

クラス マップは設定されません。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。

使用上のガイドライン

CoPP の設定時に ARP クラス マップを作成するには、このコマンドを使用します。

例

ARP クラスマップの作成方法を、次の例に示します。

```
Router(config)# class-map arp-peruser
Router(config-cmap)# match protocol arp
Router(config-cmap)# match subscriber access
```

関連コマンド

コマンド	説明
match protocol arp	ポリシー マップに対する ARP トラフィックに一致します。
match subscriber access	ポリシー マップに対する加入者アクセス トラフィックに一致します。

class-bundle

指定した VC クラスに含まれるバンドルレベル コマンドを使用して仮想回線 (VC) を設定するには、バンドルコンフィギュレーションモードまたは SVC バンドルコンフィギュレーションモードで **class-bundle** コマンドを使用します。VC バンドルから VC クラス パラメータを削除するには、このコマンドの **no** 形式を使用します。

class-bundle *vc-class-name*
no class-bundle *vc-class-name*

構文の説明

<i>vc-class-name</i>	VC バンドルに割り当てる VC クラスの名前です。
----------------------	----------------------------

コマンド デフォルト

VC バンドルに割り当てられている VC クラスはありません。

コマンド モード

バンドル コンフィギュレーション
 SVC バンドル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.0T	このコマンドが導入され、ATM VC バンドルを設定するための class コマンドが置き換えられました。
12.0(26)S	このコマンドが Cisco IOS Release 12.0(26)S に統合され、Cisco 10000 シリーズ ルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.2(4)T	このコマンドが、SVC バンドル コンフィギュレーション モードで使用できるようになりました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

このコマンドを使用するには、まず **bundle** または **bundlesvc** コマンドを入力してバンドルを作成し、バンドルコンフィギュレーションモードまたは SVC バンドルコンフィギュレーションモードを開始する必要があります。

このコマンドを使用して、以前に定義した一連のパラメータ (VC クラスで定義) を ATM VC バンドルに割り当てます。VC クラスに含まれるバンドルレベルコマンドを使用して設定されたパラメータは、バンドルとその VC メンバーに適用されます。

VCバンドルを設定するために使用するVCクラスに、次のコマンドを追加できます。**broadcast、encapsulation、inarp、oam-bundle、oamretry、protocol**

バンドルで直接設定されたコマンドを使用して適用されるバンドルレベルパラメータは、**class-bundle** コマンドによって VC クラスを使用して適用されるバンドルレベルパラメータよりも優先されます。VC クラスを通じて適用されたバンドルレベルパラメータやバンドルに直接適用されたバンドルレベルパラメータの一部は、バンドルVCコンフィギュレーションモードで個々のVCに直接適用されたコマンドによって置き換えることができます。

例

次の例では、「class1」という名前のクラスを作成し、「bundle1」という名前のバンドルに適用しています。

```
! The following commands create the class class1:
vc-class atm class1
  encapsulation aal5snap
  broadcast
  protocol ip inarp
  oam-bundle manage 3
  oam 4 3 10
! The following commands apply class1 to the bundle called bundle1:
bundle bundle1
  class-bundle class1
```

階層化された優先ルールを考慮し、「bundle1」という名前のバンドルに属するVCは、aal5snap、カプセル化、ブロードキャスト対象、IPアドレスを解決するためのInverse Address Resolution Protocol (Inverse ARP) の使用、および有効になった運用管理および保守 (OAM) といったパラメータによって特徴付けられます。

関連コマンド

Command	Description
broadcast	ブロードキャストパケットの複製と、ATM VC クラス、PVC、SVC、またはVCバンドルへの送信を設定します。
bundle	バンドルを作成するか、または既存のバンドルを修正してバンドルコンフィギュレーションモードを開始します。
bundlesvc	SVCバンドルを作成するか、または既存のSVCバンドルを変更します。
class-int	VCクラスをATMメインインターフェイスまたはサブインターフェイスに割り当てます。
class-vc	VCクラスをATMPVC、SVC、またはVCバンドルメンバーに割り当てます。
encapsulation	インターフェイスで使用するカプセル化方式を設定します。
inarp	ATM PVC、VCクラス、またはVCバンドルのInverse ARPの時間を設定します。
oam-bundle	バンドルのすべてのVCメンバー、またはVCバンドルに適用できるVCクラスに対して、エンドツーエンドのF5 OAMループバックセル生成とOAM管理を有効にします。

Command	Description
oamretry	ATM PVC、SVC、VC クラス、または、VC バンドルの OAM 管理に関連するパラメータを設定します。
protocol(ATM)	ATM PVC、SVC、VC クラス、または、VC バンドルのスタティック マップを設定します。PVC、VC バンドルで直接、または VC クラス (IP および IPX プロトコルのみに適用) 内で Inverse ARP を設定することで、ATM PVC で Inverse ARP または Inverse ARP ブロードキャストを有効にします。
pvc-bundle	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドルメンバーを設定するために bundle-vc コンフィギュレーション モードに入ります。

class-map

指定したクラスへのパケットの照合に使用するクラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **class-map** コマンドを使用します。既存のクラス マップをデバイスから削除するには、このコマンドの **no** 形式を使用します。

Cisco 2600、3660、3845、6500、7200、7401、および 7500 シリーズ ルータ

```
class-map [type {stack|access-control|port-filter|queue-threshold|logging log-class}]
[{match-all|match-any}] class-map-name
no class-map [type {stack|access-control|port-filter|queue-threshold|logging log-class}]
[{match-all|match-any}] class-map-name
```

Cisco 7600 シリーズ ルータ

```
class-map class-map-name [{match-all|match-any}]
no class-map class-map-name [{match-all|match-any}]
```

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

```
class-map class-map-name
no class-map class-map-name
```

構文の説明

type	(任意) クラスマップ タイプを指定します。
stack	(任意) Flexible Packet Matching (FPM) 機能を有効にして、調査するプロトコル スタックを決定します。 loadprotocol コマンドを使用し、デバイスで Protocol Header Description File (PHDF) をロードする場合、存在するヘッダーとその順序をフィルタで判定できるように、プロトコルヘッダーのスタックを定義できます。
access-control	(任意) 設定されたプロトコルスタックで検索するパターンを決定します。 (注) スタック クラス マップを指定 (typestack キーワードを使用) してから、アクセス制御クラス マップを指定 (typeaccess-control キーワードを使用) する必要があります。
port-filter	(任意) コントロールプレーンパケットの TCP または UDP ポートポリシングを有効にするポートフィルタクラスマップを作成します。このキーワードが有効になっている場合、コマンドは、コントロールプレーン ホスト サブインターフェイスの特定のポートが宛先になっているトラフィックをフィルタします。
queue-threshold	(任意) 指定されたプロトコルでコントロールプレーン IP 入力キューに入ることができるパケットの総数を制限するキューしきい値を有効にします。このキューしきい値は、コントロールプレーン ホスト サブインターフェイスにしか適用されません。

logging <i>log-class</i>	(任意) コントロールプレーン上のパケットトラフィックのログギングを有効にします。 <i>log-class</i> 引数の値は、ログ クラスの名前です。
match-all	(任意) 複数の一致基準が存在する場合に、どのようにしてパケットを評価するかを決定します。このクラスマップの下の状態メントが、論理 AND 関数に基づいて一致します。パケットが受け入れられるには、すべての状態メントに一致している必要があります。 match-all または match-any キーワードを指定しない場合に使用されるデフォルトキーワードは、 match-all です。
match-any	(任意) 複数の一致基準が存在する場合に、どのようにしてパケットを評価するかを決定します。このクラス マップの下の状態メントが、論理 OR 関数に基づいて一致します。パケットが受け入れられるには、マッチング ステートメントのいずれかに一致している必要があります。 match-any または match-all キーワードを指定しない場合に使用されるデフォルトのキーワードは、 match-all です。
<i>class-map-name</i>	クラスマップのクラスの名前です。クラス名は、クラスマップに使用するとともに、ポリシー マップのクラスにポリシーを設定する場合にも使用します。 (注) 引用符で囲んだ <i>class-map-name</i> 引数の値を入力できます。引用符なしで入力されたクラスマップ名では、スペースが受け入れられません。

コマンド デフォルト

クラス マップは設定されません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.0(5)XE	このコマンドが Cisco IOS Release 12.0(5)XE に統合されました。
12.0(7)S	このコマンドが、Cisco IOS Release 12.0(7)S に統合されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.2(14)SX	このコマンドは、Cisco IOS Release 12.2(14)SX に統合され、Cisco 7600 シリーズ ルータに実装されました。
12.2(17d)SXB	このコマンドが、Cisco IOS Release 12.2(17d)SXB に統合され、Cisco 7600 シリーズ ルータに実装されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更箇所
12.4(4)T	このコマンドが変更されました。FPMをサポートするために stack キーワードと access-control キーワードが追加されました。コントロールプレーン保護機能をサポートするために port-filter キーワードと queue-threshold キーワードが追加されました。
12.4(6)T	このコマンドが変更されました。コントロールプレーンパケットロギングをサポートするために logging log-class キーワードと引数のペアが追加されました。
12.2(18)ZY	このコマンドが変更されました。 stack キーワードと access-control キーワードが、Catalyst 6500 シリーズの Programmable Intelligent Services Accelerator (PISA) が搭載されているスイッチの Cisco IOS Release 12.2(18)ZY に統合されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。
15.1(3)T	このコマンドが、Cisco Performance Monitor 用の Cisco IOS Release 15.1(3)T に統合され、 <i>class-map-name</i> 引数が使用可能な唯一の構文要素となりました。
12.2(58)SE	このコマンドが、 <i>class-map-name</i> 引数とともに Cisco Performance Monitor 用の Cisco IOS Release 12.2(58)SE に統合されました。
12.2(33)SCF	このコマンドが、Cisco IOS リリース 12.2(33)SCF に統合されました。
15.2(3)T	このコマンドが変更されました。引用符なしで入力されたクラスマップ名では、スペースが受け入れられません。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス ルータに統合されました。

Cisco IOS Release 15.1(3)T および 12.2(58)SE の Cisco Performance Monitor

class-map-name 引数のみが利用可能です。

Cisco 2600、3660、3845、6500、7200、7401、7500、および ASR 1000 シリーズ ルータ

class-map コマンドを使用して、クラスマップの一致基準に一致させるために作成または変更するクラスを指定します。このコマンドで QoS クラスマップ コンフィギュレーションモードに入ることができ、そこで1つまたは複数の **match** コマンドを入力して、このクラスの一致基準を設定します。入力インターフェイスまたは出力インターフェイスのいずれか (**service-policy** コマンドの設定により決まります) に到達したパケットが、クラスマップに設定されている一致基準に対して照合され、パケットがそのクラスに属するかどうか判断されます。

クラスマップを設定する際には、1つまたは複数の **match** コマンドを使用して一致基準を指定できます。たとえば、**matchaccess-group** コマンド、**matchprotocol** コマンド、または

matchinput-interface コマンドを使用できます。**match** コマンドは、Cisco のソフトウェア リリースごとに異なります。一致基準および **match** コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Modular Quality of Service Command-Line Interface (CLI) (MQC)」の章を参照してください。

Cisco 7600 シリーズ ルータ

class-map コマンドと、QoS クラスマップ コンフィギュレーション モードで利用できるコマンドをインターフェイス単位ベースで適用し、グローバルに指定されたサービスポリシーの一環として、パケット分類、マーキング、集約、およびフロー ポリシングを定義します。

サービス ポリシーは EtherChannel に付加できます。EtherChannel のメンバーであるポートに、サービス ポリシーを付加しないでください。

デバイスが QoS クラスマップ コンフィギュレーション モードになっている場合、次のコンフィギュレーション コマンドが利用可能です。

- **description** : クラスマップ コンフィギュレーションの記述を指定します。
- **exit** : QoS クラスマップ コンフィギュレーション モードを終了します。
- **match** : 分類基準を設定します。
- **no** : クラス マップからマッチング ステートメントを削除します。

CLI ヘルプには次のコマンドが表示されますが、Optical Service Module (OSM) の LAN インターフェイスまたは WAN インターフェイスではサポートされません。

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **source-address mac** *mac-address*

OSM は、Supervisor Engine 32 が搭載された Cisco 7600 シリーズ ルータではサポートされません。

ポリシー フィーチャ カード (PFC) QoS は、次のコマンドをサポートしません。

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **qos-group** *group-value*
- **source-address mac** *mac-address*

これらのコマンドを入力した場合、インターフェイスにポリシー マップが付加されないと、PFC QoS はサポートされていないキーワードを検出しません。インターフェイスにポリシー マップを付加しようとする、エラー メッセージが生成されます。詳細については、『*Cisco*

『7600 Series Router Cisco IOS Software Configuration Guide』と Cisco IOS コマンド リファレンスを参照してください。

クラスマップ名およびデバイスの設定後、QoS クラスマップ コンフィギュレーション モードで **match access-group** コマンドと **matchipdscp** コマンドを入力できます。これらのコマンドの構文は次のとおりです。

match [**access-group** {*acl-index* | *acl-name*} | **ip dscp** | **precedence**] *value*

match コマンド キーワードの説明については、次の表を参照してください。

表 1: **match** コマンド構文の説明

オプションのコマンド	説明
access-group <i>acl-index</i> <i>acl-name</i>	(任意) アクセス リスト インデックスまたはアクセス リスト名を指定します。有効なアクセス リストのインデックス値は、1 ~ 2699 です。
access-group <i>acl-name</i>	(任意) 名前付きのアクセス リストを指定します。
ipdscp <i>value1 value2 ...value8</i>	(任意) 照合する IP Diffserv コードポイント (DSCP) 値を指定します。有効な値は 0 ~ 63 です。最大 8 つの DSCP 値をスペースで区切って入力できます。
ipprecedence <i>value1 value2 ...value8</i>	(任意) 照合する IP プレシデンス値を指定します。有効な値は 0 ~ 7 です。最大 8 つのプレシデンス値をスペースで区切って入力できます。

例

次に、クラスの名前として **class101** を指定し、そのクラスに対してクラス マップを定義する方法の例を示します。**class101** という名前のクラスは、ACL 101 に一致するトラフィックに対するポリシーを指定します。

```
Device(config)# class-map class101
Device(config-cmap)# match access-group 101
Device(config-cmap)# end
```

次の例は、スラマーおよび UDP パケットの FPM トラフィック クラスを定義する方法を示しています。クラス マップ内で定義されている一致基準は、IP の長さが 404

(0x194) を超えず、UDP ポートが 1434 (0x59A) であり、IP ヘッダーの先頭から 224 バイトでパターン 0x4011010 となるスラマーおよび UDP パケットを対象としています。

```
Device(config)# load protocol disk2:ip.phdf
Device(config)# load protocol disk2:udp.phdf
Device(config)# class-map type stack match-all ip-udp
Device(config-cmap)# description "match UDP over IP packets"
Device(config-cmap)# match field ip protocol eq 0x11 next udp
Device(config-cmap)# exit
Device(config)# class-map type access-control match-all slammer
Device(config-cmap)# description "match on slammer packets"
```



```
Device(config-cmap)# match field udp dest-port eq 0x59A
Device(config-cmap)# match field ip length eq 0x194
Device(config-cmap)# match start 13-start offset 224 size 4 eq 0x 4011010
Device(config-cmap)# end
```

次に、Simple Network Management Protocol (SNMP) 以外の閉じているポート、つまり「リッスンされていない」ポートに宛てられたすべてのトラフィックをドロップするポートフィルタ ポリシーを設定する例を示します。

```
Device(config)# class-map type port-filter pf-class
Device(config-cmap)# match not port udp 123
Device(config-cmap)# match closed-ports
Device(config-cmap)# exit
Device(config)# policy-map type port-filter pf-policy
Device(config-pmap)# class pf-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

次の例は、ipp5 というクラス マップを設定して、IP プレシデンス 5 のマッチング ステートメントを入力する方法を示しています。

```
Device(config)# class-map ipp5
Device(config-cmap)# match ip precedence 5
```

802.1p ドメイン内のクラス マップの設定

次の例は、クラスマップを設定し、802.1p ドメインに対してパケットのサービスクラス (CoS) 値を使用してトラフィック クラスに照合する方法の例を示しています。

```
Device> enable
Device# configure terminal
Device(config)# class-map cos1
Device(config-cmap)# match cos 0
Device(config-pmap-c)# end
```

MPLS ドメイン内のクラス マップの設定

次の例は、クラスマップを設定し、マルチプロトコルラベルスイッチング (MPLS) ドメインに対してパケットの Experimental (EXP) 値を使用してトラフィック クラスに照合する方法の例を示しています。

```
Device> enable
Device# configure terminal
Device(config)# class-map exp7
Device(config-cmap)# match mpls experimental topmost 2
Device(config-pmap-c)# end
```

関連コマンド

コマンド	説明
description	クラス マップまたはポリシー マップのコンフィギュレーションの記述を指定します。

コマンド	説明
drop	特定のクラス マップに属するパケットを廃棄するトラフィック クラスを設定します。
class(policy-map)	ポリシーを作成または変更するクラスの名前を指定し、ポリシーを設定する前にデフォルト クラスを指定します。
load protocol	PHDF をルータにロードします。
match (class-map)	ポート フィルタやプロトコル キュー ポリシーに基づいて、クラス マップの一致基準を設定します。
matchaccess-group	指定した ACL をベースにクラス マップに対して一致基準を設定します。
matchinput-interface	指定された入力インターフェイスを一致基準として使用するクラス マップを設定します。
matchipdscp	1 つまたは複数の DSCP 値、AF 値、および CS 値を一致基準として指定します。
matchmplsexperimental	指定した EXP フィールド値を一致基準として使用するクラス マップを設定します。
matchprotocol	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。
policy-map	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。
protocol	制御インターフェイスのタイマーと認証方法を設定します。
qos-group	クラス マップに対して QoS グループ値を関連付けます。
service-policy	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。
showclass-map	クラス マップ情報を表示します。
showpolicy-mapinterface	インターフェイスに適用された入力および出力ポリシーの統計情報および設定を表示します。
source-address	ポートで送信元アドレスの制御を設定します。

class-map arp-peruser

ユーザごとのパケットの Address Resolution Protocol (ARP) に一致するクラス マップを作成するには、グローバルコンフィギュレーションモードで **class-map arp-peruser** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

class-map arp-peruser
no class map arp-peruser

構文の説明

arpper-user	ユーザごとの Address Resolution Protocol を指定します。
--------------------	--

コマンド デフォルト

有効

コマンド モード

グローバル設定

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。

使用上のガイドライン

CoPP の設定時に ARP クラス マップを作成するには、このコマンドを使用します。

例

ARP クラスマップの作成例を、次に示します。

```
Router(config)#class-map arp-peruser
Router(config-cmap)#match protocol arp
Router(config-cmap)#match subscriber access
```

関連コマンド

コマンド	説明
match protocol arp	ポリシー マップに対する ARP トラフィックに一致します。
match subscriber access	ポリシー マップに対する加入者アクセス トラフィックに一致します。

class type tag

クラスマップをポリシーマップと関連付けるには、ポリシーマップ コンフィギュレーション モードで、**classtypetag** コマンドを使用します。コマンドの関連付けを解除するには、このコマンドの **no** 形式を使用します。

class type tag *class-name* [**insert-before** *class-name*]
no class type tag *class-name* [**insert-before** *class-name*]

構文の説明	<i>class-name</i>	クラス マップの名前。
	insert-before <i>class-name</i>	(任意) 既存の任意の2つのクラスマップ間にクラスマップを追加します。 (注) 既存の2つのクラスマップ間に新しいクラスマップを挿入すると、既存のポリシーマップ設定をより柔軟に変更できるようになります。このオプションを指定しないと、クラスマップはポリシーマップの末尾に追加されます。

コマンド デフォルト クラスマップは、ポリシーマップに関連付けられていません。

コマンド モード ポリシー マップ コンフィギュレーション

コマンド履歴	リリース	変更箇所
	12.4(6)T	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用してもクラスが設定されていない場合は、エラーが発生します。エラーは、「%クラスマップ {名} は設定されていません。(% class map {name} not configured.)」のような内容です。特定のクラスマップの前にクラスを挿入する必要がある場合は、**insert-before** キーワードを使用できます。**insert-before** キーワードは通常、管理者がホストごとのクラスマップを設定し、それを特定のクラスマップの前に挿入する場合に必要となります。**classtypetag** コマンドは、ポリシーマップ クラス コンフィギュレーション モードを作成します。ポリシーマップの下に複数のクラスを配置できます。

例

クラスマップ「`usergroup1_class`」をポリシーマップと関連付ける方法を、次の例に示します。

```
class type tag usergroup1_class
```

関連コマンド

コマンド	説明
policy-map	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。

clear control-plane

コントロールプレーンのインターフェイスまたはサブインターフェイスのカウンタをクリアするには、特権 EXEC モードで **clearcontrol-plane** コマンドを使用します。

clear control-plane [**{*|aggregate|host|transit|cef-exception}**]

構文の説明		
	*	(任意) すべてのコントロールプレーンの機能に対するカウンタをクリアします。
	aggregate	(任意) コントロールプレーンの集約パスのすべての機能に対するカウンタをクリアします。
	host	(任意) コントロールプレーン ホスト機能のパスのすべての機能に対するカウンタをクリアします。
	transit	(任意) コントロールプレーンの中継機能パスのすべての機能に対するカウンタをクリアします。
	cef-exception	(任意) コントロールプレーンの CEF 例外機能パスのすべての機能に対するカウンタをクリアします。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

コントロールプレーンのインターフェイスまたはサブインターフェイスのすべての機能に対するカウンタをクリアするには、**clearcontrol-plane** コマンドを使用します。

例

次の例は、コントロールプレーンホスト機能のパスのすべての機能に対するカウンタをクリアします。

```
Router# clear control-plane host
```

関連コマンド

コマンド	説明
control-plane	コントロールプレーン 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、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。

コマンド	説明
debugcontrol-plane	コントロールプレーンルーチンからのデバッグ出力を表示します。
showcontrol-planecef-exceptioncounters	コントロールプレーン CEF 例外のサブインターフェイスに対するコントロールプレーン パケット カウンタを表示します。
showcontrol-planecef-exceptionfeatures	コントロールプレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-planecounters	集約コントロールプレーン インターフェイスに対するコントロールプレーン パケット カウンタを表示します。
showcontrol-planefeatures	集約コントロールプレーン インターフェイスに対して設定された機能を表示します。
showcontrol-planehostcounters	コントロールプレーン ホスト サブインターフェイスに対するコントロールプレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロールプレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-planehostopen-ports	ポートフィルタデータベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロールプレーン パケット カウンタを表示します。
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

clear ip nbar

Network-Based Application Recognition (NBAR) によって収集されたバッファ、フィルタ、およびポートの統計情報をクリアするには、特権 EXEC モードで **clear ip nbar** コマンドを使用します。

clear ip nbar [**{capture|filter|trace{detail|summary}|statistics|unclassified-port-stats}**]

構文の説明

capture	(任意) パケット キャプチャ バッファを指定します。
filter	(任意) セッション選択フィルタを指定します。
trace	(任意) 状態グラフ トレース バッファを指定します。
detail	(任意) NBAR の詳細な分類情報を指定します。
summary	(任意) NBAR の分類概要を指定します。
unclassified-port-stats	(任意) 未分類パケットのポート統計情報を指定します。
statistics	(任意) パケットの NBAR 統計情報を指定します。

コマンドモード

特権 EXEC (#)

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドは、Cisco IOS Release 12.2(33)SRC よりも前のリリースに統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI よりも前のリリースに統合されました。
15.0(1)M	このコマンドは、Cisco IOS Release 15.0(1)M よりも前のリリースに導入されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズの集約サービス ルータに実装されました。
15.2(4)M	このコマンドが変更されました。 statistics 、 trace 、および detail キーワードが追加されました。

例

次に、NBAR によって収集されたポートの統計情報をクリアする例を示します。

```
Device# clear ip nbar unclassified-port-stats
```

次に、NBAR によって収集された統計情報をクリアする例を示します。

```
Device# clear ip nbar statistics
```


関連コマンド

コマンド	説明
clearipnbarprotocol-discovery	NBAR Protocol Discovery によって収集された統計情報をクリアします。
show ip nbar statistics	NBAR によって収集された統計情報を表示します。

clear ip nbar classification auto-learn top-hosts

ジェネリックとして分類されたネットワークトラフィックの上位ホストの統計およびデータベースをクリアするには、**clear ip nbar classification auto-learn top-hosts** コマンドを使用します。

clear ip nbar custom auto-learn top-hosts {restart | statistics}

構文の説明

restart	表示のクリア後に、ジェネリックとして分類されたトラフィックの上位ホストの統計およびデータベースの表示を再開します。
statistics	統計およびデータベースの表示をクリアします。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
15.5(2)T	このコマンドが導入されました。

例

次の例に、ジェネリックとして分類されたネットワークトラフィックの上位ホストの統計およびデータベースをクリアする方法を示します。

```
Device# clear ip nbar classification auto-learn statistics
```

関連コマンド

コマンド	説明
ipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワークトラフィックの上位ホストの統計およびデータベースを示す NBAR の機能を有効にします。
showipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワークトラフィックの上位ホストの統計およびデータベースを表示します。

clear ip nbar protocol-discovery

Network-Based Application Recognition (NBAR) Protocol Discovery 機能によって収集された統計情報をクリアするには、特権 EXEC モードで **clearipnbarprotocol-discovery** コマンドを使用します。

clear ip nbar protocol-discovery [*interface type number*]

構文の説明

interface	(任意) 設定するインターフェイスのタイプを指定します。
type	(任意) インターフェイスのタイプです。
number	(任意) インターフェイスまたはサブインターフェイスの番号です。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
15.0(1)M	このコマンドは、Cisco IOS Release 15.0(1)M よりも前のリリースに導入されました。
12.2(33)SRC	このコマンドは、Cisco IOS Release 12.2(33)SRC よりも前のリリースに統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI よりも前のリリースに統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズの集約サービス ルータに実装されました。

使用上のガイドライン

NBAR Protocol Discovery 機能によって収集された統計情報をクリアするには、**clearipnbarprotocol-discovery** コマンドを使用します。このコマンドは、デフォルトでは、Protocol Discovery 機能が有効になっているすべてのインターフェイスの統計情報をクリアします。

例

次の例は、NBAR Protocol Discovery 機能によって収集された統計情報をクリアする方法を示しています。

```
Router# clear ip nbar protocol-discovery interface serial 3/1
```

関連コマンド

コマンド	説明
clearipnbar	NBAR 機能によって収集されたバッファ、フィルタ、およびポートの統計情報をクリアします。

clear ip rsvp authentication

ライフタイムの期限が切れる前にリソース予約プロトコル (RSVP) セキュリティ アソシエーションを削除するには、特権 EXEC モードで **clear ip rsvp authentication** コマンドを使用します。

clear ip rsvp authentication [*{ip-addresshostname}*]

構文の説明

<i>ip-address</i>	(任意) 特定のネイバーとのセキュリティ アソシエーションを解除します。
<i>hostname</i>	(任意) 特定のホストとのセキュリティ アソシエーションを解除します。



(注) *ip-address* 引数と *hostname* 引数の違いは、ネイバーを IP アドレスで指定するか、その名前指定するかの違いです。

コマンド デフォルト

デフォルトの動作では、すべてのセキュリティ アソシエーションがクリアされます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

次の場合に、**clear ip rsvp authentication** コマンドを使用します。

- ライフタイムの期限が切れる前にセキュリティ アソシエーションを削除する場合
- メモリを解放する場合
- 一部の独立ステートにあるセキュリティ アソシエーションの問題を解決する場合
- ネイバーの再認証を強制する場合

IP アドレスまたはホスト名を入力しないことで、すべての RSVP セキュリティ アソシエーションを削除できます。また、特定の RSVP ネイバーまたはホストのみを入力して削除することができます。

セキュリティ アソシエーションを削除すると、信頼された RSVP ネイバーが RSVP メッセージをさらに送信しはじめたとき、必要に応じて再度作成されます。

例

次のコマンドは、期限切れになる前にすべてのセキュリティアソシエーションを削除する方法を示します。

```
Router# clear ip rsvp authentication
```

関連コマンド

コマンド	説明
iprsvpauthenticationlifetime	信頼できる他の RSVP ネイバーとのセキュリティアソシエーションを RSVP が保持する期間を制御します。
showiprsvpauthentication	RSVP によって他の RSVP ネイバーとの間で確立されたセキュリティアソシエーションを表示します。

clear ip rsvp counters

保持されているすべての IP リソース予約プロトコル (RSVP) カウンタをクリア (0 に設定) するには、特権 EXEC モードで **cleariprsvpcounters** コマンドを使用します。

clear ip rsvp counters [confirm]

構文の説明

confirm	(任意) すべての IP RSVP カウンタがクリアされたことの確認を要求します。
----------------	---

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(14)ST	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

このコマンドを使用すると、変更を容易に確認できるように、すべての IP RSVP カウンタを 0 に設定できます。

例

次の例では、保持しているすべての IP RSVP のカウンタをクリアしています。

```
Router# clear ip rsvp counters
Clear rsvp counters [confirm]
```

関連コマンド

コマンド	説明
showiprsvpcounters	送受信された RSVP メッセージのカウンタを表示します。

clear ip rsvp hello instance counters

hello インスタンス カウンタの値をクリア（更新）するには、特権 EXEC モードで **cleariprsvphelloinstancecounters** コマンドを使用します。

clear ip rsvp hello instance counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(31)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

例

showiprsvphelloinstancedetail コマンドと、**cleariprsvphelloinstancecounters** コマンドからの出力例を、次に示します。「Statistics」フィールドがクリアされ、0 になっていることに注意してください。

```
Router# show ip rsvp hello instance detail
Neighbor 10.0.0.2 Source 10.0.0.1
State: UP (for 2d18h)
Type: PASSIVE (responding to requests)
I/F: Et1/1
LSPs protecting: 0
Refresh Interval (msec) (used when ACTIVE)
Configured: 100
Statistics: (from 2398195 samples)
  Min:      100
  Max:      132
  Average:  100
  Waverage: 100 (Weight = 0.8)
  Current:  100
Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
Counters:
Communication with neighbor lost:
Num times: 0
Reasons:
  Missed acks:          0
  Bad Src_Inst received: 0
  Bad Dst_Inst received: 0
```

clear ip rsvp hello instance counters

```

I/F went down:          0
Neighbor disabled Hello: 0
Msgs Received:    2398194
Sent:             2398195
Suppressed:       0
Router# clear ip rsvp hello instance counters
Neighbor 10.0.0.2 Source 10.0.0.1
State: UP          (for 2d18h)
Type: PASSIVE     (responding to requests)
I/F: Et1/1
LSPs protecting: 0
Refresh Interval (msec) (used when ACTIVE)
Configured: 100
Statistics:
Min:              0
Max:              0
Average:          0
Waverage:         0
Current:          0
Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
Counters:
Communication with neighbor lost:
Num times: 0
Reasons:
Missed acks:      0
Bad Src_Inst received: 0
Bad Dst_Inst received: 0
I/F went down:   0
Neighbor disabled Hello: 0
Msgs Received:    2398194
Sent:             2398195
Suppressed:       0

```

関連コマンド

Command	説明
iprsvpsignallinghello(configuration)	ルータで hello をグローバルに有効にします。
iprsvpsignallinghello(interface)	Fast Reroute の保護が必要なインターフェイスでの hello を有効にします。
iprsvpsignallinghelloworldstatistics	ルータで hello 統計を有効にします。
showiprsvphellostatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

clear ip rsvp hello instance statistics

インスタンスの hello 統計をクリアするには、特権 EXEC モードで **cleariprsvphelloinstancestatistics** コマンドを使用します。

clear ip rsvp hello instance statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

インスタンスに対して Hello 統計はクリアされません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(31)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

例

次の例は、**showiprsvphellostatistics** コマンドからの出力例と、**cleariprsvphelloinstancestatistics** コマンドの入力後のフィールド内の値を示していません。

```
Router# show ip rsvp hello statistics
Status: Enabled
Packet arrival queue:
  Wait times (msec)
    Current:0
    Average:0
    Weighted Average:0 (weight = 0.8)
    Max:4
  Current length: 0 (max:500)
  Number of samples taken: 2398525
```

```
Router# clear ip rsvp hello instance statistics
Status: Enabled
Packet arrival queue:
  Wait times (msec)
    Current:0
    Average:0
    Weighted Average:0 (weight = 0.8)
```

clear ip rsvp hello instance statistics

```

Max:0
Current length: 0 (max:500)
Number of samples taken: 0

```

関連コマンド

コマンド	説明
iprsvpsignallinghello(configuration)	ルータで hello をグローバルに有効にします。
iprsvpsignallinghello(interface)	Fast Reroute の保護が必要なインターフェイスでの hello を有効にします。
iprsvpsignallinghelloworldstatistics	ルータで hello 統計を有効にします。
showiprsvphelloworldstatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

clear ip rsvp hello statistics

hello 統計をグローバルにクリアするには、特権 EXEC モードで **cleariprsvphellostatistics** コマンドを使用します。

clear ip rsvp hello statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

Hello 統計はグローバルにクリアされません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB2s	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(31)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

hello インプットキューに hello パケットが入っていた時間に関するすべての情報を削除するには、このコマンドを使用します。

例

showiprsvphellostatistics コマンドと **cleariprsvphellostatistics** コマンドからの出力例を、次に示します。「Packet arrival queue」フィールドの値がクリアされていることに注意してください。

```
Router# show ip rsvp hello statistics
Status: Enabled
Packet arrival queue:
  Wait times (msec)
    Current:0
    Average:0
    Weighted Average:0 (weight = 0.8)
    Max:4
  Current length: 0 (max:500)
Number of samples taken: 2398525
Router# clear ip rsvp hello statistics
Status: Enabled
Packet arrival queue:
  Wait times (msec)
    Current:0
```

```
Average:0  
Weighted Average:0 (weight = 0.8)  
Max:0  
Current length: 0 (max:500)  
Number of samples taken: 16
```

関連コマンド

コマンド	説明
iprsvpsignallinghellostatistics	ルータで hello 統計を有効にします。
showiprsvphellostatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

clear ip rsvp high-availability counters

ルータプロセッサ (RP) によって保持されているリソース予約プロトコル (RSVP) トラフィック エンジンアリング (TE) 高可用性 (HA) カウンタをクリア (0 に設定) するには、特権 EXEC モードで **cleariprsvphigh-availabilitycounters** コマンドを使用します。

clear ip rsvp high-availability counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(33)SRA	このコマンドが導入されました。
12.2(33)SRB	インサービス ソフトウェア アップグレード (ISSU) のサポートが追加されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

状態、リソース障害、および履歴情報を含む HA カウンタをクリア (0 に設定) するには、**cleariprsvphigh-availabilitycounters** コマンドを使用します。

例

次の例は、現在 RP が保持しているすべての HA 情報をクリアします。

```
Router# clear ip rsvp high-availability counters
```

関連コマンド

コマンド	説明
showiprsvphigh-availabilitycounters	RP によって保持されている RSVP TE HA カウンタを表示します。

clear ip rsvp msg-pacing



(注) Cisco IOS Release 12.4(20)T では、Cisco IOS ソフトウェアで **cleariprsvmsg-pacing** コマンドを使用できません。このコマンドが、**cleariprsvsignallingrate-limit** コマンドによって置き換えられました。

showiprsvneighbor コマンドからのリソース予約プロトコル (RSVP) メッセージペーシング出力をクリアするには、特権 EXEC モードで **cleariprsvmsg-pacing** コマンドを使用します。

clear ip rsvp msg-pacing

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(14)ST	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.2(13)T	このコマンドが、 cleariprsvsignallingrate-limit コマンドによって置き換えられました。
12.4(20)T	このコマンドは削除されました。

例

次の例は、RSVP メッセージペーシング出力をクリアします。

```
Router# clear ip rsvp msg-pacing
```

関連コマンド

コマンド	説明
showiprsvpcounters	送受信された RSVP メッセージの数を表示します。

コマンド	説明
showiprsvpneighbor	現在の RSVP ネイバーを表示し、指定されたインターフェイスまたはすべてのインターフェイスに対して、そのネイバーが IP カプセル化と UDP カプセル化のどちらを使用しているのかを示します。

clear ip rsvp reservation

現在データベースに格納されているリソース予約プロトコル (RSVP) RESV 関連の受信側情報を削除するには、EXEC モードで **cleariprsvreservation** コマンドを使用します。

```
clear ip rsvp reservation {session-ip-address sender-ip-address {tcp|udp|ip-protocol} session-dport sender-sport[*]}
```

構文の説明	
<i>session-ip-address</i>	ユニキャストセッションの場合、これは目的の受信者のアドレスです。また、マルチキャストセッションの場合、これはセッションの IP マルチキャストアドレスです。
<i>sender-ip-address</i>	送信者の IP アドレス。
tcp udp ip-protocol	TCP、User Datagram Protocol (UDP)、または IP プロトコル (0 ~ 65535 の範囲) です。
<i>session-dport</i>	宛先ポート。 (注) ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先が 0 の場合は送信元も 0 でなくてはなりません。また、これはポートがチェックされていない可能性を示します。宛先が 0 以外の場合、送信元も 0 以外でなくてはなりません (送信元ポートが常に無視され、0 となるワイルドカードフィルタ (wf) 予約を除く)。
<i>sender-sport</i>	送信元ポート。 (注) ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先が 0 の場合は送信元も 0 でなくてはなりません。また、これはポートがチェックされていない可能性を示します。宛先が 0 以外の場合、送信元も 0 以外でなくてはなりません (送信元ポートが常に無視され、0 となるワイルドカードフィルタ (wf) 予約を除く)。
*	すべての送信者をクリアするためにワイルドカードが使用されます。

コマンドモード

EXEC

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。

リリース	変更箇所
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

予約要求を受信した場合に、RSVP アドミッションポリシーに基づいて関連するものを再確立できるよう、現在データベースに格納されている RESV 関連の送信者情報を削除するには、**cleariprsvppreservation** コマンドを使用します。

クロックレートやインターフェイスの帯域幅を変更するたびに、RSVP が変更を反映してデータベースを更新することはありません。これは、新しいクロックレートまたは帯域幅の値に基づき、このような変更で RSVP が予約を再確立する必要があるためです。また、一部の予約を任意で破棄してその他を保持することが好ましくないためです。解決策は、**cleariprsvppreservation** コマンドを発行することで RESV 状態をクリアすることです。

cleariprsvppreservation コマンドは、コマンドを発行したルータから RESV 状態をクリアし、ルータから PATH TEAR メッセージを上流に位置するルータに送信させ、その上流に位置するすべてのルータの予約に対する RESV 状態をクリアします。

例

次の例は、現在データベースに格納されている RESV 関連の受信側情報のすべてをクリアします。

```
Router# clear ip rsvp reservation *
```

次の例は、現在データベースに格納されている特定の予約に対する RESV 関連の受信側情報のすべてをクリアします。

```
Router# clear ip rsvp reservation 10.2.1.1 10.1.1.2 udp 10 20
```

関連コマンド

コマンド	説明
cleariprsvpsender	現在データベースに存在する RSVP PATH 関連の送信者情報を削除します。

clear ip rsvp sender

現在データベースに格納されているリソース予約プロトコル (RSVP) PATH 関連の送信者情報を削除するには、EXEC モードで **cleariprvpsender** コマンドを使用します。

```
clear ip rsvp sender {session-ip-address sender-ip-address {tcp|udp|ip-protocol} session-dport sender-sport[*]}
```

構文の説明	
<i>session-ip-address</i>	ユニキャストセッションの場合、これは目的の受信者のアドレスです。また、マルチキャストセッションの場合、これはセッションの IP マルチキャストアドレスです。
<i>sender-ip-address</i>	送信者の IP アドレス。
tcp udp ip-protocol	TCP、User Datagram Protocol (UDP)、または IP プロトコル (0 ~ 65535 の範囲) です。
<i>session-dport</i>	宛先ポート。 (注) ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先が 0 の場合は送信元も 0 でなくてはなりません。また、これはポートがチェックされていない可能性を示します。宛先が 0 以外の場合、送信元も 0 以外でなくてはなりません (送信元ポートが常に無視され、0 となるワイルドカードフィルタ (wf) 予約を除く)。
<i>sender-sport</i>	送信元ポート。 (注) ポート番号は、すべてのケースで指定します。IP ヘッダーに続く 16 ビット ポートの使用は、UDP または TCP に限定されるものではないためです。宛先が 0 の場合は送信元も 0 でなくてはなりません。また、これはポートがチェックされていない可能性を示します。宛先が 0 以外の場合、送信元も 0 以外でなくてはなりません (送信元ポートが常に無視され、0 となるワイルドカードフィルタ (wf) 予約を除く)。
*	すべての送信者をクリアするためにワイルドカードが使用されます。

コマンドモード

EXEC

コマンド履歴

リリース	変更箇所
11.2	このコマンドが導入されました。

リリース	変更箇所
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

予約要求を受信した場合に、RSVP アドミッションポリシーに基づいて関連するものを再確立できるよう、現在データベースに格納されている PATH 関連の送信者情報を削除するには、**cleariprsvpsender** コマンドを使用します。

クロックレートやインターフェイスの帯域幅を変更するたびに、RSVP が変更を反映してデータベースを更新することはありません。これは、新しいクロックレートまたは帯域幅の値に基づき、このような変更で RSVP が予約を再確立する必要があるためです。また、一部の予約を任意で破棄してその他を保持することが好ましくないためです。解決策は、**cleariprsvpsender** コマンドを発行することで PATH 状態をクリアすることです。

cleariprsvpsender コマンドは、コマンドを発行したルータから PATH 状態をクリアし、ルータから PATH TEAR メッセージを下流に位置するルータに送信させ、その下流に位置するすべてのルータの予約に対する PATH 状態をクリアします。

例

次の例は、現在データベースに格納されている PATH 関連の送信者情報のすべてをクリアします。

```
Router# clear ip rsvp sender *
```

次の例は、現在データベースに格納されている特定の予約に対する PATH 関連の送信者情報のすべてをクリアします。

```
Router# clear ip rsvp sender 10.2.1.1 10.1.1.2 udp 10 20
```

関連コマンド

コマンド	説明
cleariprsvppreservation	現在データベースに存在する RSVPRESV 関連の受信側情報を削除します。

clear ip rsvp signalling fast-local-repair statistics

リソース予約プロトコル (RSVP) 高速ローカル修復 (FLR) カウンタをクリア (0に設定) するには、ユーザ EXEC モードまたは特権 EXEC モードで **cleariprsvpsignallingfast-local-repairstatistics** コマンドを使用します。

clear ip rsvp signalling fast-local-repair statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、すべての RSVP FLR カウンタをクリアします。

コマンド モード

ユーザ EXEC (>) 特権 EXEC (#)

コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

すべての RSVP FLR カウンタを 0 に設定するには、**cleariprsvpsignallingfast-local-repairstatistics** コマンドを使用します。統計には、現在の状態、開始時刻、および修復レートなど、FLR 手順に関する情報が含まれます。

例

次の例は、データベースで保持されているすべての RSVP FLR カウンタをクリアします。

```
Router# clear ip rsvp signalling fast-local-repair statistics
```

関連コマンド

コマンド	説明
showiprsvpsignallingfast-local-repair	FLR 関連情報を表示します。

clear ip rsvp signalling rate-limit

キューがいっぱいのため破棄されたリソース予約プロトコル (RSVP) メッセージの数をクリア (0 に設定) するには、特権 EXEC モードで **cleariprsvpsignallingrate-limit** コマンドを使用します。

clear ip rsvp signalling rate-limit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。このコマンドは cleariprsvpsmsg-pacing コマンドを置き替えます。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

破棄されたメッセージを記録しているカウンタをクリアするには、**cleariprsvpsignallingrate-limit** コマンドを使用します。

例

次のコマンドで、すべての破棄されたメッセージをクリアする方法を示します。

```
Router# clear ip rsvp signalling rate-limit
```

関連コマンド

コマンド	説明
debugiprsvprate-limit	RSVP レート制限イベントのデバッグメッセージを表示します。
iprsvpsignallingrate-limit	指定の期間中に隣接ルータに送信される RSVP メッセージの伝送レートを制御します。
showiprsvpsignallingrate-limit	RSVP メッセージのレート制限パラメータを表示します。

clear ip rsvp signalling refresh reduction

再送信回数および誤った順序のリソース予約プロトコル（RSVP）メッセージの番号に関連付けられたカウンタをクリア（0 に設定）するには、EXEC モードで **cleariprsvpsignallingrefreshreduction** コマンドを使用します。

clear ip rsvp signalling refresh reduction

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

EXEC

コマンド履歴

リリース	変更箇所
12.2(13)I	このコマンドが導入されました。

使用上のガイドライン

再送信や誤った順序の RSVP メッセージを記録しているカウンタをクリアするには、**cleariprsvpsignallingrefreshreduction** コマンドを使用します。

例

次のコマンドは、すべての再送信および誤った順序のメッセージをクリアする方法を示しています。

```
Router# clear ip rsvp signalling refresh reduction
```

関連コマンド

コマンド	説明
iprsvpsignallingrefreshreduction	リフレッシュ削減をイネーブルにします。
showiprsvpsignallingrefreshreduction	RSVP メッセージのリフレッシュ削減パラメータを表示します。

clear mls qos

マルチレイヤスイッチング (MLS) 集約の Quality of Service (QoS) 統計をクリアするには、特権 EXEC モードで **clearmlsqos** コマンドを使用します。

```
clear mls qos [{ip|ipx|mac|mpls|ipv6|arp} [{interface-type interface-number|null
interface-number|port-channel number|vlan vlan-id}]]
```

構文の説明	
ip	(任意) MLS の IP 集約 QoS 統計情報をクリアします。
ipx	(任意) MLS の IPX 集約 QoS 統計情報をクリアします。
mac	(任意) MLS の MAC 集約 QoS 統計情報をクリアします。
mpls	(任意) MLS の MPLS 集約 QoS 統計情報をクリアします。
ipv6	(任意) MLS の IPv6 集約 QoS 統計情報をクリアします。
arp	(任意) MLS の ARP 集約 QoS 統計情報をクリアします。
<i>interface-type</i>	(任意) インターフェイスタイプ。可能な有効値は、 ethernet 、 fastethernet 、 gigabitethernet 、および tengigabitethernet です。その他の有効値については、「使用上のガイドライン」を参照してください。
<i>interface-number</i>	(任意) モジュールおよびポート番号。有効値については、「使用上のガイドライン」を参照してください。
null <i>interface-number</i>	(任意) null インターフェイスを指定します。有効値は0です。
port-channel <i>number</i>	(任意) チャンネルインターフェイスを指定します。有効な値は、1～256の範囲の最大64個の値です。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。有効値の範囲は1～4094です。

コマンドデフォルト このコマンドには、デフォルト設定がありません。

コマンドモード 特権 EXEC

コマンド履歴	リリース	変更箇所
	12.2(14)SX	このコマンドのサポートが Supervisor Engine 2 に追加されました。
	12.2(17a)SX	このコマンドが変更され、 mpls キーワードが追加されました。
	12.2(17d)SXB	スーパーバイザエンジン2上のこのコマンドのサポートが Release 12.2(17d)SXB に拡張されました。

リリース	変更箇所
12.2(18)SXD	このコマンドが変更され、 arp キーワードが追加されました。
12.2(18)SXE	このコマンドが変更され、 ipv6 および arp キーワードが Supervisor Engine 2 のみで追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

使用上のガイドライン

interface-type の有効値には、**ge-wan**、**atm**、および **pos** キーワードがあり、Supervisor Engine 2 で設定された Cisco 7600 シリーズルータでサポートされています。

ipx キーワードは、Supervisor Engine 2 で設定された Cisco 7600 シリーズルータでのみサポートされます。

ipv6 および **arp** キーワードは、Supervisor Engine 720 で設定された Cisco 7600 シリーズルータでのみサポートされます。

interface-number 引数では、モジュールおよびポート番号を指定します。*interface-number* の有効な値は、指定するインターフェイスタイプと、使用するシャーシおよびモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネットモジュールが搭載されている場合に、ギガビットイーサネットインターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

引数なしで **clearmlsqos** コマンドを入力すると、すべてのプロトコルでグローバルおよびインターフェイス単位の集約 QoS カウンタがクリアされます。

インターフェイスタイプを入力しない場合、すべてのインターフェイスのプロトコル集約 QoS カウンタがクリアされます。



(注) **clearmlsqos** コマンドを入力すると、ポリシングのトークンバケットカウンタが影響を受け、ポリシングされるはずのトラフィックがわずかに転送される可能性があります。

例

次に、すべてのプロトコルでグローバルおよびインターフェイス単位の集約 QoS カウンタをクリアする例を示します。

```
Router# clear mls qos
```

次に、すべてのインターフェイスで特定プロトコルの集約 QoS カウンタをクリアする例を示します。

```
Router# clear mls qos ip
```


関連コマンド

コマンド	説明
<code>showmlsqos</code>	MLS QoS 情報を表示します。

clear service-group traffic-stats

サービスグループのいずれか、またはすべてに対するトラフィック統計情報をクリアするには、特権 EXEC モードで **clearservice-grouptraffic-stats** コマンドを使用します。

clear service-group traffic-stats [group service-group-identifier]

構文の説明	group	(任意) サービスグループ。
	<i>service-group-identifier</i>	(任意) サービスグループ番号。統計をクリアするサービスグループ番号を入力します。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(33)SRE	このコマンドが導入されました。

使用上のガイドライン

サービスグループ番号を指定しない場合は、すべてのサービスグループの統計がクリアされます。



- (注) サービスグループのトラフィック統計情報をクリアしてもグループメンバーのトラフィック統計情報はクリアされません。グループメンバーのトラフィック統計情報をクリアするには、**clearethernetserviceinstance** コマンドを使用します。**clearethernetserviceinstance** コマンドの詳細については、『Cisco IOS Carrier Ethernet Command Reference』を参照してください。

例

すべてのサービスグループのトラフィック統計情報をクリアする方法を、次に示します。

```
Router> enable
Router# clear service-group traffic-stats
```

関連コマンド

コマンド	説明
clearethernetserviceinstance	MAC アドレスなどのイーサネット サービス インスタンス属性と統計をクリアし、イーサネットサービスインスタンスのエラーを消去します。

compression header ip

特定のクラスに対して Real-time Transport Protocol (RTP) または TCP/IP ヘッダー圧縮を設定するには、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 **compressionheaderip** コマンドを使用します。特定のクラスに対して RTP または TCP/IP ヘッダー圧縮を削除するには、このコマンドの **no** 形式を使用します。

compression header ip [{rtp|tcp}]
no compression header ip

構文の説明

rtp	(任意) RTPヘッダー圧縮を設定します。
tcp	(任意) TCPヘッダー圧縮を設定します。

コマンドデフォルト

RTP または TCP ヘッダー圧縮を指定しない (つまり、コマンド名の後で Enter キーを押す) 場合、RTP と TCP ヘッダー圧縮の両方が設定されます。これは「全体で圧縮を使用する」というシナリオに対応することを目的としています。

コマンドモード

ポリシーマップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが導入されました。

使用上のガイドライン

すべての形式の **compressionheaderip** コマンドは、以前に入力された形式を上書きします。

compressionheaderip コマンドは、モジュラ Quality of Service (QoS) コマンドライン インターフェイス (CLI) (MQC) 機能を使用して設定されたポリシーマップ階層の任意のレベルで使用できます。

例

次の例では、「class1」というクラスに対して RTP ヘッダー圧縮を使用するように **compressionheaderip** コマンドが設定されています。class1 は、「policy1」というポリシーマップの一部です。

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# compression header ip rtp
Router(config-pmap-c)# end
```

関連コマンド

コマンド	説明
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapclass	指定されたポリシーマップの指定されたクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定のPVCに対し、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 packets 統計情報を表示します。

control-plane

コントロールプレーン コンフィギュレーションモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータ（サービスポリシーなど）の関連付けまたは変更を実行できます。このモードを開始するには、グローバル コンフィギュレーション モードで **control-plane** コマンドを使用します。既存のコントロールプレーン コンフィギュレーションをルータから削除するには、このコマンドの **no** 形式を使用します。

T リリースの構文

```
control-plane [{host|transit|cef-exception}]
no control-plane [{host|transit|cef-exception}]
```

12.0S リリースの構文

```
control-plane [slot slot-number] [{host|transit|cef-exception}]
no control-plane [slot slot-number] [{host|transit|cef-exception}]
```

Cisco 7600 シリーズ ルータ用 12.2S リリースの構文

```
control-plane
no control-plane
```

ASR 1000 シリーズ ルータの構文

```
control-plane [host]
no control-plane [host]
```

構文の説明

host	(任意) ホスト コントロールプレーン トラフィックにポリシーを適用します。
transit	(任意) 中継コントロールプレーン トラフィックにポリシーを適用します。
cef-exception	(任意) CEF 例外コントロールプレーン トラフィックにポリシーを適用します。
slot <i>slot-number</i>	(任意) QoS ポリシーをアタッチして、分散コントロールプレーン (CP) サービスを設定するラインカードのスロット番号を指定します。

コマンド デフォルト

コントロールプレーン サービス ポリシーは定義されません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更箇所
12.2(18)S	このコマンドが導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.0(29)S	このコマンドが、Cisco IOS Release 12.0(29)S に統合されました。

リリース	変更箇所
12.0(30)S	slotslot-number パラメータが、分散コントロールプレーン (CP) サービスを設定するために追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.4(4)T	host,transit および cef-exception キーワードが追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.2	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

control-plane コマンドの入力後、コントロールプレーン ポリシング (CoPP)、ポートフィルタ、またはキューしきい値ポリシーを適用し、コントロールプレーン宛のトラフィックをポリシングできます。ルート プロセッサ (RP) に対する集約 CoPP を定義し、サービス ポリシーを設定してコントロールプレーン宛のすべてのトラフィックを次のようにポリシングできます。

- ルータ (集計 CP サービス) のすべてのラインカードから
- ラインカードのすべてのインターフェイスから (分散 CP サービス)

集約 CP サービスは、コントロールプレーン宛のトラフィックと、ルータのすべてのラインカードから中央のスイッチ エンジンで受信したトラフィックを管理します。

分散 CP サービスは、集計 CP サービスが適用される中央のスイッチ エンジンに対して CP パケットが転送される前に、指定したラインカード上のインターフェイスから CP トラフィックを管理します。



- (注) Cisco 12000 シリーズ インターネット ルータでは、分散 CP サービスと集約 CP サービスを組み合わせ、DoS 攻撃からコントロールプレーンを保護し、パケットの QoS を提供できます。**slotslot-number** パラメータは、分散 CP サービス設定にのみ使用します。

コントロールプレーン ポリシングには、強化されたコントロールプレーン機能が含まれています。ルータ上の閉じたまたはリスンされていない Cisco IOS TCP/UDP ポート宛てにダイレクトされたパケットを早期にドロップするメカニズムを提供します。また、正常に動作していない単一のプロトコルプロセスがコントロールプレーンインターフェイス ホールドキューに割り込みをしないように、プロトコル キューの使用率を制限する機能を提供します。



- (注) **control-plane** コマンドは、Cisco IOS Release 12.2S により、Cisco 7600 ルータに対してのみサポートされています。その他の Cisco IOS リリースでは、Cisco 7600 は **nocontrol-plane** コマンドのみをサポートし、以前の既存の設定条件は廃止されました。

この機能強化により、コントロールプレーントラフィックを異なるカテゴリのトラフィックに分類できます。これらのカテゴリは次のとおりです。

- **コントロールプレーンホストサブインターフェイス**：ルータインターフェイスのいずれかが直接の宛先となるすべてのコントロールプレーン IP トラフィックを受信するサブインターフェイス。コントロールプレーンホスト IP トラフィックの例には、トンネル終端トラフィック、管理トラフィック、ルーティングプロトコルなど（SSH、SNMP、BGP、OSPF、EIGRP など）があります。すべてのホストトラフィックは、ルータによって終端し、処理されます。ほとんどのコントロールプレーン保護機能とポリシーは、コントロールプレーンホストサブインターフェイス上で厳格に運用されます。ほとんどの重要なルータコントロールプレーンサービス（ルーティングプロトコルや管理トラフィックなど）がコントロールプレーンホストサブインターフェイス上で受信されるため、ポリシーングおよび保護ポリシーによってこのトラフィックを保護することは不可欠です。CoPP 機能、ポートフィルタリング機能、およびプロトコルごとのキューしきい値保護機能をコントロールプレーンホストサブインターフェイスに適用できます。
- **コントロールプレーン中継サブインターフェイス**：ルートプロセッサによってソフトウェアスイッチングされるすべてのコントロールプレーン IP トラフィックを受信するサブインターフェイス。つまり、パケットは、ルータ自体を直接の宛先とするのではなく、ルータを経由して移動します。ルータによって処理される非終端トンネルは、このタイプのコントロールプレーントラフィックの一例です。コントロールプレーン保護機能では、このサブインターフェイスで受信されるすべてのトラフィックに特定の集約ポリシーングを適用できます。
- **コントロールプレーン CEF 例外サブインターフェイス**：プロセススイッチング用に CEF パケット転送パスで設定された入力機能の結果としてリダイレクトされるか、インターフェイスドライバによってコントロールプレーン入力キューに直接追加されるすべてのトラフィック（ARP、L2 キープアライブ、および非 IP ホストトラフィック）を受信するサブインターフェイス。コントロールプレーン保護機能を使用すると、この特定のタイプのコントロールプレーントラフィックに対する特定の集約ポリシーングを実行できます。

例

次の例では、送信元アドレス 10.1.1.1 および 10.1.1.2 を持つ信頼できるホストを設定し、制約を設けずに Telnet パケットをコントロールプレーンに転送する方法を示します。残りのすべての Telnet パケットは、指定したレートでポリシーングされるようにします。次に、集約 CP サービスに対し、ルータのすべてのラインカードからコントロールプレーンに入るすべてのパケットに QoS ポリシーが適用されます。

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
```

```

! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control-plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end

```

次の例では、送信元アドレス 10.1.1.1 および 10.1.1.2 を持つ信頼できるホストを設定し、制約を設けずに Telnet パケットをコントロールプレーンに転送する方法を示します。スロット 1 経由で入る残りのすべての Telnet パケットは、指定したレートでポリシングされるようにします。QoS ポリシーは、分散 CP サービスに対し、スロット 1 のラインカードのインターフェイスを経由して入り、コントロールプレーンを宛先とするすべてのパケットに適用されます。

```

! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control-plane service for the active route processor.
Router(config)# control-plane slot 1
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end

```

次の例は、集約 CoPP ポリシーをホストコントロールプレーン機能パスに適用することで、ホストコントロールプレーントラフィックに適用する方法を示しています。

```

Router(config)# control-plane host
Router(config-cp)# service-policy input cpp-policy-host

```

次の例は、集約 CoPP ポリシーを中継コントロールプレーン機能パスに適用することで、中継コントロールプレーントラフィックに適用する方法を示しています。

```

Router(config)# control-plane transit
Router(config-cp)# service-policy input cpp-policy-transit

```

次の例は、集約 CoPP ポリシーを CEF 例外コントロールプレーン機能パスに適用することで、例外コントロールプレーントラフィックに適用する方法を示しています。


```
Router(config)# control-plane cef-exception
Router(config-cp)# service-policy input cpp-policy-cef-exception
```

関連コマンド

コマンド	説明
class(policy-map)	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルトクラス（一般に class-default クラスといます）を指定します。
class-map	QoS クラス マップ コンフィギュレーションモードにアクセスして QoS クラス マップを設定します。
drop	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
matchaccess-group	指定した ACL をベースにクラスマップに対して一致基準を設定します。
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーションモードにアクセスします。
service-policy(control-plane)	集約コントロールプレーンサービスまたは分散コントロールプレーンサービス用に、ポリシーマップをコントロールプレーンにアタッチします。
showpolicy-mapcontrol-plane	コントロールプレーンにアタッチされたポリシー マップのあるクラス、またはすべてのクラスの設定を表示します。

copy interface

コマンドで指定されているインターフェイスに対し、特定のクラスに属するパケットをコピーするトラフィック クラスを設定するには、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 **copyinterface** コマンドを使用します。パケットがコピーされるのを防ぐには、このコマンドの **no** 形式を使用します。

copy interface interface type number

no copy interface interface type number

構文の説明

<i>interface type number</i>	パケットを送信する必要があるインターフェイスのタイプおよび数です。
------------------------------	-----------------------------------

コマンド デフォルト

このコマンドを指定しないと、パケットはインターフェイスにコピーされません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション (config-pmap-c)

コマンド履歴

リリース	変更箇所
12.2(18)ZYA1	このコマンドが導入されました。

使用上のガイドライン

定義済みのインターフェイスにパケットをコピーするには、このコマンドを使用します。元のパケットは定義済みの宛先に送信され、コピーされたパケットはコピー先のインターフェイスに送信されます。**copyinterface** コマンドは **log** コマンドとともに設定することもできますが、**drop** コマンドまたは **redirectinterface** コマンドとともに設定することはできません。スタッククラスのサービスポリシーを使用して、このコマンドを構成することはできません。パケットは、次のインターフェイスにのみコピーできます。

- Ethernet
- ファストイーサネット
- ギガビットイーサネット
- Ten Gigabit Ethernet

例

次の例では、**cmtest** というトラフィック クラスを作成し、**pmtest** というポリシー マップで使用できるように設定しています。ポリシー マップ (サービス ポリシー) は、FastEthernet インターフェイス 4/18 に適用されます。**cmtest** クラスのすべてのパケットは、FastEthernet インターフェイス 4/15 にコピーされます。

```
Router(config)# policy-map type access-control pmtest
Router(config-pmap)# class cmtest
Router(config-pmap-c)# copy interface FastEthernet 4/15
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
```

```
Router(config)# interface FastEthernet 4/18
Router(config-if)#
service-policy input pmtest
```

関連コマンド

コマンド	説明
log	ポリシーマップクラスコンフィギュレーションモードまたはクラスマップコンフィギュレーションモードでログメッセージを生成します。
showclass-map	すべてのクラス マップおよびその一致基準を表示します。
showpolicy-map	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定のPVCに対し、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 packets 統計情報を表示します。

custom-queue-list



- (注) Cisco IOS XE Release 2.6 および Cisco IOS Release 15.1(3)T 以降では、**custom-queue-list** コマンドは表示されません。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンドラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンドシーケンス）を使用する必要があります。詳細（代替コマンドのリストを含む）については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。



- (注) Cisco IOS XE Release 3.2S では、**custom-queue-list** コマンドは、モジュラ QoS CLI (MQC) コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンドシーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

インターフェイスにカスタムキューリストを割り当てるには、インターフェイスコンフィギュレーションモードで **custom-queue-list** コマンドを使用します。特定のリストまたはすべてのリストの割り当てを削除するには、このコマンドの **no** 形式を使用します。

custom-queue-list [*list-number*]
no custom-queue-list [*list-number*]

構文の説明

<i>list-number</i>	カスタムキューリストのための 1～16 の番号です。
--------------------	----------------------------

コマンド デフォルト

カスタム キュー リストは割り当てられていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更箇所
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレーンでサポートされます。このトレーンの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

使用上のガイドライン

1 つのインターフェイスに 1 つのキュー リストのみを割り当てることができます。**priority-listinterface** コマンドの代わり（追加はせず）に、このコマンドを使用してください。カスタム キューイングでは、プライオリティ キューイングで提供されない均等性が実現されます。カスタム キューイングを使用すると、インターフェイスでキューに入れられた集約トラフィックに対応できない場合に、インターフェイスで利用可能な帯域幅を制御できます。それぞれの出力キューに関連付けられるのは設定可能なバイトカウントであり、これによりシステムが次のキューに移動する前に現在のキューから送信するバイト数が指定されます。特定のキューが処理されている間は、パケットは、送信されたバイト数がキューのバイトカウントを超えるまで、またはキューが空になるまで送信されます。

カスタム出力キューの現在の状態を表示するには、**showqueueingcustom** コマンドと **showinterfaces** コマンドを使用します。

例

次の例では、シリアル インターフェイス 0 にカスタム キュー リスト番号 3 が割り当てられています。

```
interface serial 0
 custom-queue-list 3
```

関連コマンド

Command	Description
priority-listinterface	特定のインターフェイスから着信するパケットのキューイングプライオリティを確立します。
queue-listdefault	キュー リストの他のルールに一致しないパケット用にプライオリティ キューを割り当てます。
queue-listinterface	インターフェイスに着信するパケットのキューイング プライオリティを確立します。

Command	Description
queue-listqueuebyte-count	特定のサイクル中に特定のキューからシステムが配信できるバイト数を指定します。
queue-listqueuelimit	キューに対してキューの長さ制限を指定します。
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
showqueue	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。