QoS：パケット フロー制御のコンフィギュレーション ガイド

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

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

CiscoおよびCisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/go/trademarks でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

トラフィック シェーピングを使用したパケット フローの制御 3

機能情報の確認 3

トラフィック シェーピングに関する情報 4

ネットワーク上でのトラフィック シェーピングの利点 4

トークン バケットとトラフィック シェーピング 4

トラフィック シェーピングと転送レート 5

トラフィック シェーピングによるトラフィックの制御方法 6

トラフィック シェーピングとトラフィック ポリシング 7

その他の参考資料 8

クラスベース トラフィック シェーピングを使用したクラス単位のパケット フローの制御 11

機能情報の確認 11

クラスベース トラフィック シェーピングの設定の前提条件 12

クラスベース トラフィック シェーピングの設定の制約事項 12

クラスベース トラフィック シェーピングに関する情報 13

クラスベース トラフィック シェーピングの機能 13

クラスベース トラフィック シェーピングの利点 13

クラスベース トラフィック シェーピングの階層型ポリシー マップ構造 14

クラスベース トラフィック シェーピングの設定方法 15

第 1 レベル ポリシー マップ内でのクラスベース トラフィック シェーピングの設定 15

次の作業 17

第 2 レベル ポリシー マップの設定 18

クラスベース トラフィック シェーピングの設定例 20

例：クラスベース トラフィック シェーピングの設定 20

次の作業 20

その他の参考資料 20

クラスベース トラフィック シェーピングの機能情報 **22**

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

有効な Cisco IOS XE Release 3.7.0E（Catalyst スイッチング向け）および Cisco IOS XE Release 3.17S（アクセスおよびエッジ ルーティング向け）の 2 つのリリースは、コンバージド リリースの 1 つのバージョン（Cisco IOS XE 16）へと進化（マージ）しました。本リリースでは、スイッチングおよびルーティング ポートフォリオにおける幅広いアクセス製品およびエッジ製品をカバーしています。

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

第 2 章

トラフィック シェーピングを使用したパケット フローの制御

このモジュールでは、ネットワーク上でのパケット フローの制御の概要について説明します。ネットワーク上のパケット フロー（つまり、トラフィックのフロー）は、トラフィック シェーピングともいいます。トラフィック シェーピングでは、インターフェイスから出るトラフィックの速度を制御できます。このようにして、トラフィックのフローとパケットを受信するインターフェイスの速度を合わせることができます。シスコでは、クラスベース トラフィック シェーピングと呼ばれるトラフィック制御メカニズムを提供しています。このメカニズムを設定する前に、このモジュールに記載された概要を理解しておくことが重要です。

- 機能情報の確認，3 ページ
- トラフィック シェーピングに関する情報，4 ページ
- その他の参考資料，8 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

トラフィック シェーピングに関する情報

ネットワーク上でのトラフィック シェーピングの利点

- トラフィック シェーピングにより、インターフェイスから出力されるトラフィックを制御して、トラフィック フローとインターフェイスの速度を合わせることができます。
- トラフィックが、適用されたポリシーに従うことが保証されます。
- トラフィック シェーピングは、パケットが規定された要件を満たすように支援し、パケットに適用すべき適切な QoS を決定します。
- また、ボトルネックとデータレートの不一致を排除します。この例が、中央サイトとリモート サイト間のデータ速度の不一致です。
- パケット損失を防止します。

ここで、トラフィック シェーピングを使用したいくつかのシナリオを紹介します。

- たとえば、ポリシーによって、アクセス レートがインターフェイス速度を上回っていても、そのインターフェイスのレートが平均で特定のレートを上回るべきではないとされている場合に、帯域幅へのアクセスを制御します。
- ネットワークのアクセス レートが複数存在する場合に、インターフェイス上でトラフィック シェーピングを設定します。ネットワーク上でリンクの一方の端が 256 kbps で動作し、もう一方の端が 128 kbps で動作しているとします。256 kbps でパケットを送信すると、そのリンクを使用しているアプリケーションで障害が発生する可能性があります。

同様に、さらに複雑なケースでは、アクセス レートが異なる複数のデータ端末装置（DTE）が接続されたリンク層ネットワークで輻輳が発生する場合があります。ネットワークによっては、一度に 1 台の DTE 装置に対して他の装置よりも速い転送速度を提供できる場合があります（このシナリオでは、トークン バケットが抽出され、そのレートが維持されることが保証されます）。

- サブレート サービスを提供します。この場合は、トラフィック シェーピングを使用すれば、ルータで T1 または T3 リンクをより小さなチャネルに分割できます。

トークン バケットとトラフィック シェーピング

トラフィック シェーピングでは、トークン バケット メタファーを使用してトラフィックを調整します。トークンバケットは、転送レートの正式な定義です。バーストサイズ、平均レート、時間間隔（Tc）という 3 つの構成要素があります。通常は中間レートがビット/秒の単位で表されますが、次に示す関係式によって、2 つの値が残る 3 つめの値から導き出される場合もあります。

```
mean rate = burst size / time interval
```

これらの用語の定義は次のとおりです。

- 平均レート：認定情報レート（CIR）とも呼ばれ、単位時間に送信または転送できるデータ量の平均値を指定します。
- バーストサイズ：認定バースト（Bc）サイズとも呼ばれ、スケジューリングの問題を発生させることなく単位時間内に送信できるトラフィックの量を、バーストあたりのビット数（またはバイト数）で指定します。（トラフィック シェーパーの場合は、バースト当たりのビット数を意味します）。
- 時間間隔：測定間隔とも呼ばれ、バーストあたりの時間量を秒単位で指定します。

定義では、間隔が整数倍の場合は、インターフェイスのビット レートは中間レートを超えません。ただし、ビット レートは間隔内で任意に早くなる場合があります。

トークン バケットは、フロー内のデータを規制するデバイスの管理に使用されます。たとえば、トラフィック シェーパーがこのような調整デバイスとして使用されている場合があります。トークン バケット自体には、廃棄ポリシーまたはプライオリティ ポリシーはありません。むしろ、トークン バケットは、フローによって規制機能が過剰に働く場合に、トークンを廃棄し、送信キューの管理の問題はフローに任せます。

トークン バケットのたとえで言えば、トークンは特定のレートでバケットに入れられます。バケット自体には指定された容量があります。バケットがいっぱいになると、新しく到着するトークンは廃棄されます。各トークンは、送信元が一定の数のビットをネットワークに送信するための権限です。パケットを送信するため、規制機能はパケット サイズに等しい数のトークンをバケットから削除する必要があります。

パケットを送信するために必要なトークンがバケット内に存在しない場合は、パケットは、バケットに十分な量のトークンが蓄積されるまで送信待ちの状態になります。バケットがすでにトークンで満たされている場合、着信トークンはオーバーフローし、以降のパケットには使用できません。したがって、いつでも、送信元がネットワークに送信できる最大のバーストは、バケットのサイズにほぼ比例します。

トラフィック シェーピングに使用されるトークン バケット メカニズムは、トークン バケットとデータ バッファ、またはキューの両方を持つことに注意してください。データ バッファを持たない場合は、トラフィック ポリサーである可能性があります。トラフィック シェーピングの場合、到着したパケットですぐに送信できないものは、データ バッファで遅延されます。

トラフィック シェーピングでは、トークン バケットはバースト性を許可する一方で、それを抑制します。トークン バケットは、（トークン バケットの容量）+（トークンをバケット内に配置するための設定レート x 時間間隔）よりも速くフローが送信されないようにバースト性が制限されることを保証します。また、長期転送レートが、トークンをバケット内に配置するための設定レートを超えないことを保証します。

トラフィック シェーピングと転送レート

トラフィック シェーピングは、データの転送レートを制限します。データ転送を次のいずれかに制限できます。

- 特定の設定レート
- 輻輳レベルに基づいて抽出されたレート

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

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

超過バースト（Be）サイズという新しい変数がトラフィック シェーピングに適用されます。Be サイズは、非認定ビットの数に相当します。非認定ビットは、CIR から外れたビットで、スイッチで受け入れられますが、破棄適性（DE）としてマークされます。

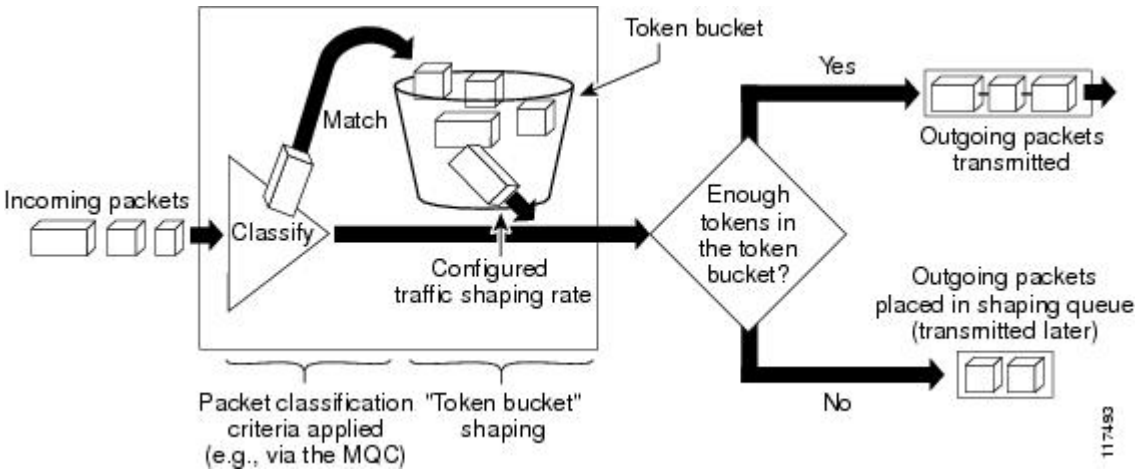
つまり、Be サイズは、特定の状況下の時間間隔中に送信されるバースト サイズを上回ることができます。スイッチでは、超過バーストに属するパケットの通過を許可しますが、DE ビットを設定することで、これらのパケットをマークします。パケットが送信されるかどうかは、スイッチの設定方法に依存します。

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

トラフィック シェーピングによるトラフィックの制御方法

次の図に、トラフィック シェーピング メカニズムによるトラフィック制御方法を示します。

図 *1*：トラフィック シェーピング メカニズムによるトラフィックの制御方法



上の図では、着信パケットがインターフェイスに到着します。パケットは、アクセス コントロール リスト（ACL）やモジュラ QoS コマンドライン インターフェイス（MQC）などの「分類エン

ジン」を使用して分類されます。パケットが、指定された分類と一致した場合は、トラフィック シェーピング メカニズムが継続されます。そうでない場合は、それ以上の処理が行われません。

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

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

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

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

トラフィック シェーピングとトラフィック ポリシング

トラフィック シェーピングとトラフィック ポリシングは、同一ネットワーク上で同時に実行できますが、次の表に示すように、2 つの機能には明らかな違いがあります。

表 *1*：トラフィック シェーピングとトラフィック ポリシングの違い

	トラフィック シェーピング	トラフィック ポリシング
トリガーイベント	• 一定の間隔（Tc）で自動的に実行されます。 または、パケットがインターフェイスに到達するたびに実行されます。	• パケットがインターフェイスに到達するたびに実行されます。

	トラフィック シェーピング	トラフィック ポリシング
処理の内容	• パケットを分類します。 • パケットが一致基準を満たしていない場合は、それ以上の処理が行われません。 • 一致基準を満たしているパケットが送信されます（トークンバケット内に十分なトークンが存在する場合）。 または、パケットが後で転送するためにキュー内に配置されます。 • キュー内のパケット数がキュー制限を超えている場合は、パケットが破棄されます。	• パケットを分類します。 • パケットが一致基準を満たしていない場合は、それ以上の処理が行われません。 • 一致基準を満たしており、指定されたレートに対して適合、超過、または違反しているパケットには、設定されたポリシング処理（破棄、送信、マーク後に送信など）が行われます。 • パケットは、後で転送するためにキュー内に配置されません。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
パケット分類	「Classifying Network Traffic」モジュール
MQC、ポリシー マップ、クラス マップ、および階層型ポリシー マップ	「Applying QoS Features Using the MQC」モジュール
WFQ、CBWFQ、PQ、CQ、FIFO およびその他のキューイング メカニズム	「Congestion Management Overview」モジュール
クラスベース トラフィック シェーピング	「Regulating Packet Flow on a Per-Class Basis -- Using Class-Based Traffic Shaping」モジュール

関連項目	マニュアル タイトル
GTS	「Regulating Packet Flow on a Per-Interface Basis Using Generic Traffic Shaping」モジュール
FRTS	「MQC-Based Frame Relay Traffic Shaping」モジュール

標準規格

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

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 3 章

クラスベース トラフィック シェーピングを使用したクラス単位のパケット フローの制御

ネットワーク上のパケット フローは、トラフィック シェーピング メカニズムを使用して制御できます。このようなトラフィック シェーピング メカニズムの 1 つがクラスベース トラフィック シェーピングと呼ばれるシスコの機能です。クラスベース トラフィック シェーピングを使用すれば、インターフェイスから出力されるパケット フローをインターフェイスの速度に合わせて（トラフィック クラス単位で）制御できます。このモジュールでは、クラスベース トラフィック シェーピングの設定に関する概念とタスクについて説明します。

- 機能情報の確認，11 ページ
- クラスベース トラフィック シェーピングの設定の前提条件，12 ページ
- クラスベース トラフィック シェーピングの設定の制約事項，12 ページ
- クラスベース トラフィック シェーピングに関する情報，13 ページ
- クラスベース トラフィック シェーピングの設定方法，15 ページ
- クラスベース トラフィック シェーピングの設定例，20 ページ
- 次の作業，20 ページ
- その他の参考資料，20 ページ
- クラスベース トラフィック シェーピングの機能情報，22 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

クラスベーストラフィックシェーピングの設定の前提条件

「トラフィック シェーピングを使用したパケット フローの制御」モジュールに記載された概念をよく理解しておく必要があります。

ご使用のプラットフォームでクラスベース トラフィック シェーピングがサポートされているかどうかを確認するには、Feature Navigator を使用してください。http://www.cisco.com/go/fn から、Cisco Feature Navigator にアクセスしてください。

顧客がルータ上で Versatile Interface Processor（VIP）を使用している場合は、分散型シスコ エクスプレス フォワーディング（dCEF）をイネーブルにする必要があります。

ポリシー マップとクラス マップを初めて作成する場合は、モジュラ Quality of Service（QoS）コマンドライン インターフェイス（MQC）を使用する必要があります。

クラスベーストラフィックシェーピングの設定の制約事項

フレームリレー ネットワーク用の適応型トラフィック シェーピングは、フレームリレー ネットワーク以外ではサポートされません。

クラスベース トラフィック シェーピングはアウトバウンド トラフィックにのみ適用されます。

クラスベース トラフィック シェーピングでサポートされていないコマンドは次のとおりです。

- **traffic-shapeadaptive**
- **trafficshapefecn-adaptive**
- **traffic-shapegroup**
- **traffic-shaperate**

クラスベース トラフィック シェーピングに関する情報

クラスベース トラフィック シェーピングの機能

クラスベース トラフィック シェーピングは、トラフィック シェーピング メカニズムです（「トラフィック シェーパー」とも呼ばれています）。トラフィック シェーパーは、通常、バッファ、またはキューイング メカニズムを使用し、過剰なトラフィックを遅延してパケットを保持し、データ レートが予想より高い場合にフローをシェーピングします。トークン バケット メカニズムを使用して、トラフィックを保持し、特定のビット レートに調整します。トークンバケットとトラフィック シェーピングに関する詳細については、「トラフィック シェーピングを使用したパケット フローの制御」モジュールを参照してください。

クラスベース トラフィック シェーピングは、シスコ推奨のトラフィック シェーピング メカニズムです。

（注） クラスベース トラフィック シェーピングは、従来の分散トラフィック シェーピング（DTS）の代用として使用する必要があります。また、クラスベース トラフィック シェーピングは、VIP2-40、VIP2-50、またはそれ以上のプロセッサを搭載した Cisco 7500 シリーズ ルータ上で使用できます。

クラスベース トラフィック シェーピングを使用すれば、次のタスクを実行できます。

- トラフィック クラス単位でトラフィック シェーピングを設定します。1 つまたは複数のクラスのトラフィック シェーピングを微調整したり、より高い粒度でトラフィック シェーピングを設定したりできます。
- 平均レートまたはピーク レートのトラフィック シェーピングを指定します。ピーク レート シェーピングを指定すれば、帯域幅に余裕がある場合に、設定されたトラフィック シェーピング レートより多くのデータを送信可能にすることによって、帯域幅の有効利用を促進できます。
- 階層型ポリシーマップ構造でトラフィック シェーピングを設定します。つまり、トラフィック シェーピングは第 1 レベル（親）ポリシーマップ内で設定し、その他の QoS 機能（CBWFQ やトラフィック ポリシングなど）は第 2 レベル（子）ポリシー マップ内で設定することができます。詳細については、クラスベース トラフィック シェーピングの階層型ポリシーマップ構造，（14 ページ）を参照してください。

クラスベース トラフィック シェーピングの利点

トラフィック シェーピングに関連した利点のすべてがクラスベース トラフィック シェーピングにも適用されますが、粒度は高くなります。トラフィック シェーピングの利点に関する詳細につ

いては、「トラフィック シェーピングを使用したパケットフローの制御」モジュールを参照してください。

クラスベース トラフィック シェーピングの階層型ポリシー マップ構造

クラスベース トラフィック シェーピング メカニズムを使用すれば、トラフィック シェーピングを階層型ポリシー マップ構造で設定できます。つまり、トラフィック シェーピングは第 1 レベル（親）ポリシーマップ内でイネーブルにし、トラフィック シェーピングと一緒に使用されるその他の QoS 機能（CBWFQ やトラフィック ポリシングなど）は第 2 レベル（子）ポリシー マップ内でイネーブルにできます。

トラフィック シェーピングは、ポリシー マップ内の **shape** コマンドを使用して（およびレートを指定して）イネーブルにします。トラフィック シェーピングがイネーブルになっている場合は、次のいずれかの処理が行われます。

- 指定されたレートを上回るパケットは、該当するキューイング メカニズムを使用してキュー内に配置されます。
- 指定されたレートに準拠しているパケットは転送されます。

パケットがキュー内に配置されているときに使用されるデフォルトキューイング メカニズムは、重み付け均等化キューイング（WFQ）です。ただし、クラスベース トラフィック シェーピングを使用すれば、クラスベース WFQ（CBWFQ）を代替キューイング メカニズムとして設定できます。

CBWFQ を使用すれば、トラフィックをキュー内に配置する方法を微調整できます。たとえば、音声トラフィックはすべて高優先度キューに配置し、指定されたクラスからのトラフィックはすべて低優先度キューに配置するように指定できます。

クラスベース トラフィック シェーピング メカニズムと一緒に CBWFQ を使用するには、次の条件を満たす必要があります。

- 第 2 レベル（子）ポリシー マップを作成する必要があります。作成した第 2 レベル（子）ポリシー マップは、**bandwidth** コマンドをイネーブルにすることで、CBWFQ の設定に使用されます。
- トラフィック シェーピングを第 1 レベル（親）ポリシー マップ内で設定する必要があります。

（注） CBWFQ は、第 1 レベル（親）ポリシー マップと第 2 レベル（子）ポリシー マップの両方でサポートされます。ただし、第 2 レベル（子）ポリシー マップで CBWFQ を使用するには、トラフィック シェーピングを第 1 レベル（親）ポリシーマップ内で設定する必要があります。

次のサンプル設定は、クラスベース トラフィック シェーピング メカニズムを階層型ポリシー マップ構造で設定する方法を示しています。

```
enable
configure terminal
 policy-map policy_parent        ! This is the primary-level policy map.
  class class-default
   shape average 1000000         ! This enables traffic shaping.
   service-policy policy_child   ! This associates the policy maps.
```

トラフィック シェーピングを第 1 レベル（親）ポリシー マップ内で設定する必要があります。この設定では、WFQ がすべてのトラフィックをキュー内に配置するためのデフォルト キューイング メカニズムとして使用されます。

次の第 2 レベル（子）ポリシー マップでは、代替キューイング メカニズムの CBWFQ が設定されます。

```
enable
configure terminal
 policy-map policy_child     ! This is the secondary-level policy map.
  class class-default
   bandwidth percent 50      ! This enables CBWFQ.
```

第 2 レベル（子）ポリシー マップでは、通常、トラフィック シェーピングとともに使用される QoS の追加機能（CBWFQ やトラフィック ポリシングなど）が設定されます。クラスベース トラフィック シェーピングの場合は、第 2 レベル（子）ポリシー マップでサポートされる QoS 機能が CBWFQ とトラフィック ポリシングの 2 つだけです。

クラスベース トラフィック シェーピングの設定方法

第 1 レベル ポリシー マップ内でのクラスベース トラフィック シェーピングの設定

トラフィック シェーピングはポリシーマップ内で設定されます。ポリシーマップによって、ネットワーク上のトラフィックに適用される Quality of Service（QoS）機能が決定されます。このモジュールで適用される QoS 機能は、トラフィック シェーピングです。

トラフィック シェーピングは、階層の第 1 レベル（親）ポリシー マップ内で設定されます。

はじめる前に

トラフィック シェーピングを設定する前に、MQC を使用してポリシー マップとクラス マップを作成する必要があります。

（注） トラフィック シェーピングは、第 1 レベル（親）ポリシー マップ内でのみサポートされます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **shape** [**average** | **peak**] *mean-rate* [*burst-size*] [*excess-burst-size*]
6. **service-policy***policy-map-name*
7. **end**
8. **showpolicy-map**
9. **showpolicy-mapinterface***typenumber*
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map***policy-map-name* 例： `Router(config)# policy-map policy_parent`	事前に作成したポリシーマップの名前を指定して、ポリシーマップ コンフィギュレーション モードに入ります。詳細については、「第 1 レベル ポリシー マップ内でのクラスベース トラフィック シェーピングの設定」を参照してください。 • ポリシー マップ名を入力します。
ステップ 4	**class** {*class-name* | **class-default**} 例： `Router(config-pmap)# class class-default`	作成するポリシーのクラス名を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。 • クラス名を入力するか、**class-default** キーワードを入力します。

	コマンドまたはアクション	目的
ステップ 5	**shape** [**average** | **peak**] *mean-rate* [*burst-size*] [*excess-burst-size*] 例： `Router(config-pmap-c)# shape average 1000000`	指定されたキーワードおよびレートに従ってトラフィックを調整します。 • キーワードとレートを入力します。
ステップ 6	**service-policy***policy-map-name* 例： `Router(config-pmap-c)# service-policy policy_child`	サービス ポリシーをポリシー マップに含まれる QoS ポリシー（階層型サービス ポリシー）として使用します。 • ポリシー マップ名を入力します。
ステップ 7	**end** 例： `Router(config-pmap-c)# end`	特権 EXEC モードに戻ります。
ステップ 8	**showpolicy-map** 例： `Router# show policy-map`	（任意）すべての設定済みポリシー マップを表示します。
ステップ 9	**showpolicy-mapinterface***typenumber* 例： `Router# show policy-map interface serial4/0`	（任意）指定されたインターフェイスまたはサブインターフェイス、またはインターフェイス上の特定の PVC のどちらかで、すべてのポリシーに対して設定されたすべてのクラスのパケット統計値を表示します。 • インターフェイス タイプと番号を入力します。
ステップ 10	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

次の作業

階層型ポリシーマップ構造で第2レベル（子）ポリシーマップを設定するには（任意のタスク）、「第 2 レベル ポリシー マップの設定」に記載された指示に従って進めます。

第 2 レベル ポリシー マップの設定

（注） CBWFQ は、第 1 レベル（親）ポリシー マップと第 2 レベル（子）ポリシー マップの両方でサポートされます。ただし、第2 レベル（子）ポリシーマップ内でCBWFQを使用するには、トラフィック シェーピングを第1 レベル（親）ポリシーマップ内で設定する必要があります。第 2 レベル（子）ポリシー マップ内の CBWFQ の詳細については、クラスベース トラフィック シェーピングの階層型ポリシー マップ構造, （14 ページ）を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}
6. **end**
7. **showpolicy-map**
8. **showpolicy-mapinterface***typenumber*
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map***policy-map-name* 例： `Router(config)# policy-map policy1`	事前に作成したポリシー マップの名前を指定して、ポリシー マップ コンフィギュレーション モードに入ります。詳細については、「第 2 レベル ポリシー マップの設定」を参照してください。 ポリシー マップ名を入力します。

	コマンドまたはアクション	目的
ステップ 4	**class** {*class-name* | **class-default**} 例： `Router(config-pmap)# class class-default`	作成するポリシーのクラス名を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。 • クラス名を入力するか、**class-default** キーワードを入力します。
ステップ 5	**bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*} 例： `Router(config-pmap-c)# bandwidth percent 50` 例：	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。 • kbpsの数値、帯域幅の相対的な割合、または帯域幅合計の絶対値として、帯域幅の合計を入力します。 （注） ここで使用した **bandwidth** コマンドは、設定可能なQoS機能の一例に過ぎません。**bandwidth** コマンドを使用してCBWFQを設定します。また、**police** コマンドを使用して、トラフィック ポリシングを設定することもできます。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showpolicy-map** 例： `Router# show policy-map`	（任意）すべての設定済みポリシー マップを表示します。
ステップ 8	**showpolicy-mapinterface***typenumber* 例： `Router# show policy-map interface serial4/0`	（任意）指定されたインターフェイスまたはサブインターフェイス、またはインターフェイス上の特定のPVCのどちらかで、すべてのポリシーに対して設定されたすべてのクラスのパケット統計値を表示します。 • インターフェイス タイプと番号を入力します。
ステップ 9	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

クラスベース トラフィック シェーピングの設定例

例：クラスベース トラフィック シェーピングの設定

階層型ポリシー マップ構造で設定されたクラスベース トラフィック シェーピングの例を示します。この例では、「policy_parent」と呼ばれる第 1 レベル（親）ポリシーマップと、「policy_child」と呼ばれる第 2 レベル（子）ポリシー マップの 2 つのポリシー マップが作成されています。トラフィック シェーピングは policy_parent ポリシー マップ内で設定され、CBWFQ は policy_child ポリシー マップ内で設定されています。

service-policy コマンドが、階層型ポリシー マップ構造で 2 つのポリシー マップを関連付けます。

```
enable
configure terminal
 policy-map policy_parent
  class class-default
   shape average 1000000         ! This enables traffic shaping.
   service-policy policy_child   ! This associates the policy maps.
   exit
  exit
 policy-map policy_child
  class class-default
   bandwidth percent 50   ! This enables CBWFQ.
   end
```

次の作業

汎用トラフィック シェーピング（GTS）を設定するには、「Regulating Packet Flow on a Per-Interface Basis Using Generic Traffic Shaping」モジュールを参照してください。

フレーム リレー トラフィック シェーピング（FRTS）を設定するには、「MQC-Based Frame Relay Traffic Shaping」モジュールを参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
パケット分類	「Classifying Network Traffic」モジュール

関連項目	マニュアル タイトル
MQC、ポリシー マップ、クラス マップ、および階層型ポリシー マップ	「Applying QoS Features Using the MQC」モジュール
CBWFQ とその他のキューイング メカニズム	「Configuring Weighted Fair Queueing」モジュール
トラフィック シェーピングを使用してネットワーク上のパケット フローを制御する方法に関する概要	「Regulating Packet Flow Using Traffic Shaping」モジュール
GTS	「Regulating Packet Flow on a Per-Interface Basis Using Generic Traffic Shaping」モジュール
FRTS	「MQC-Based Frame Relay Traffic Shaping」モジュール

標準規格

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

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

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

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

クラスベース トラフィック シェーピングの機能情報

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

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

表 *2*：クラスベース トラフィック シェーピングの機能情報

機能名	ソフトウェア リリース	機能の設定情報
分散トラフィック シェーピング	12.2(8)T	分散トラフィック シェーピング（DTS）は、インターフェイスから出力されるパケット フローを制御するための従来の方式です。DTS の代わりにクラスベース トラフィック シェーピングを使用する必要があります。
汎用トラフィック シェーピング（GTS）	15.0(1)S	GTS 機能は、Cisco IOS リリース 15.0(1)S に統合されました。