



クラスベースのポリシング

- 機能情報の確認 (1 ページ)
- 機能の概要 (1 ページ)
- 前提条件 (3 ページ)
- 設定作業 (3 ページ)
- トラフィック ポリシングのモニタリングと保守 (4 ページ)
- 設定例 (4 ページ)
- その他の参考資料 (6 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。

機能の概要

クラスベースポリシングでは、インターフェイスでのトラフィックの最大送受信レートを制御できます。クラスベース ポリシング設定を含むトラフィック ポリシーをインターフェイスに適用すると、クラスベース ポリシング機能が適用されます。

クラスベース ポリシングは、次のように機能します。

- ユーザ定義の基準に基づいて、トラフィックのクラスの入力転送速度を制限します。
- COS、QoS グループ、および DSCP を設定してパケットをマークします。

利点

レート制限による帯域幅管理

クラスベースポリシングでは、インターフェイスでのトラフィックの最大送受信レートを制御できます。クラスベースポリシングは、多くの場合、ネットワークの端のインターフェイスで、ネットワークを出入りするトラフィックを制限するように設定されます。ほとんどのクラスベースポリシング設定では、レートパラメータ内に収まるトラフィックは送信されますが、パラメータを超えるトラフィックはドロップされるか、異なる優先度で送信されます。

パケットのマーキング

パケットのマーキングにより、ネットワークを複数のプライオリティ レベルまたはサービスクラス (CoS) に区分することができます。パケットにマークが付けられると、これらのマーキングを使用して、ダウストリームデバイスでのトラフィックを識別および分類できます。

- クラスベースポリシングを使用して、ネットワークに入るパケットの IP プレシデンスを設定します。その後、ネットワーク内のネットワークング デバイスは、調整された IP precedence 値を使用してトラフィックの処理方法を決定できます。
- クラスベースポリシングを使用して、パケットを QoS グループに割り当てます。ルータは QoS グループを使用して、ルータ内のパケットに優先順位を付ける方法を決定します。

トラフィックには、クラスベースポリシング機能を使用せずにマークを付けることができます。クラスベースポリシングを使用せずにトラフィックにマークを付けるには、「Marking Network Traffic」モジュールを参照してください。

機能制限

- Cisco NCS 520 ルータでは、クラスベースポリシングを使用して監視できるのはシスコ エクスプレス フォワーディング (CEF) スイッチングパスだけです。クラスベースポリシング機能を使用するには、パケットを受信するインターフェイスとパケットを送信するインターフェイスの両方でシスコ エクスプレス フォワーディングを設定する必要があります。
- Cisco NCS 520 ルータでは、クラスベースポリシングはデバイスから送信されるパケットまたはデバイス宛てに送信されるパケットには適用できません。
- クラスベースポリシングは、インターフェイスまたはサブインターフェイスで設定できます。
- クラスベースポリシングは、物理インターフェイスまたはサービスインスタンスに適用できます。

前提条件

Cisco NCS 520 ルータでは、クラスベースポリシングを使用するには、その前にインターフェイスでシスコ エクスプレス フォワーディング (CEF) を設定する必要があります。

設定作業

トラフィック ポリシングの設定

コマンド	目的
<pre>Device(config-pmap-c)# police bps burst-normal burst-max conform-action action exceed-action action violate-action action</pre>	<p>トラフィック クラスによる最大帯域幅の使用を指定します。</p> <p>(注) クラスベース ポリシング機能は、トークンバケットメカニズムと連動します。現在、トークンバケットアルゴリズムには、シングルトークンバケットアルゴリズムとツー トークンバケットアルゴリズムの2種類があります。シングルトークンバケットシステムは、violate-action オプションが指定されない場合に使用されます。ツー トークンバケットシステムは、violate-action オプションが指定される場合に使用されます。</p>

トラフィック ポリシングの確認

クラスベースポリシング機能がインターフェイスで設定されていることを確認するには、**show policy-map interface EXEC** コマンドを使用します。この機能がインターフェイスで設定されている場合、**show policy-map interface** コマンド出力にポリシング統計情報が表示されます。

```
Device# show policy-map interface
Ethernet1/7
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

トラブルシューティングのヒント

- インターフェイスタイプをチェックします。インターフェイスが、このモジュールの[機能制限 \(2 ページ\)](#) のサポートされていないインターフェイスの説明に記載されていないことを確認してください。
- Cisco NCS 520 シリーズ ルータでの入力クラスベースポリシングの場合は、クラスベースポリシングが設定されているインターフェイスで CEF が設定されていることを確認してください。
- Cisco NCS 520 シリーズ ルータでの出力クラスベースポリシングの場合は、着信トラフィックが CEF 交換であることを確認してください。クラスベース ポリシングは、CEF スイッチングがイネーブルになっていない限り、スイッチング パスで使用できません。

トラフィック ポリシングのモニタリングと保守

コマンド	目的
Device# show policy-map	設定されたすべてのポリシー マップを表示します。
Device# show policy-map <i>policy-map-name</i>	ユーザ指定ポリシー マップを表示します。
Device# show policy-map interface	インターフェイスに適用されたすべての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。
Device# show policy-map interface service instance	ポートチャネルにおける特定のサービスインスタンスに関するポリシー マップ情報を表示します。

設定例

例：トラフィックポリシングを含むサービスポリシーの設定

次の例では、ファストイーサネットインターフェイス 0/0 から出るすべてのパケットに関して、平均レートを 8000 ビット/秒、ノーマルバーストサイズを 1000 バイト、超過バーストサイズを 1000 バイトに指定したクラスベースポリシングを設定します。

```
class-map access-match
match access-group 1
exit
policy-map police-setting
class access-match
police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1
violate-action drop
exit
```

```
exit
service-policy input police-setting
```

ファストイーサネットインターフェイス 0/0 から出る一連のパケットの処理方法は、パケットのサイズ、および準拠トークンバケットと超過トークンバケットに残っているバイト数に応じて異なります。一連のパケットは、次のルールに基づいてポリシングされます。

- 前のパケットが T1 に到達し、現在のパケットが T に到達した場合、バケットはトークン到達レートに基づいて T-T1 に相当するビット数で更新されます。リフィルトークンは、準拠バケットに置かれます。トークンが準拠バケットでオーバーフローになると、超過バケットにオーバーフロートークンが置かれます。トークンの到達レートは次のように計算されます。

(パケット間の時間 (= T - T1) X ポリシング レート) / 8 バイト

- 準拠バケット B のバイト数が 0 以上の場合、パケットは準拠し、パケットで準拠処理が実行されます。パケットが準拠している場合、B バイトが準拠バケットから削除され、準拠処理が実行されます。このシナリオでは、超過バケットには影響ありません。
- 準拠バケット B のバイト数が 0 未満の場合、超過トークンバケットでパケットによるバイトがチェックされます。超過バケット B のバイト数が 0 以上の場合、超過処理が実行され、超過トークンバケットから B バイトが削除されます。このシナリオでは、準拠バケットからバイトは削除されません。
- 超過バケット B のバイト数が 0 未満の場合、パケットはレートに違反しているため、違反処理が実行されます。パケットに対する処理が完了します。

この例では、初期トークンバケットはフルの 1000 バイトで開始します。450 バイトのパケットを受信すると、準拠トークンバケットに使用可能なバイトが十分あるため、パケットは準拠しています。パケットにより準拠処理（送信）が実行され、450 バイトが準拠トークンバケットから削除されます（残り 550 バイト）。

次のバケットが 0.25 秒後に到達し、準拠トークンバケットに 250 バイト追加された場合

$((0.25 \times 8000)/8)$ 、準拠トークンバケットには 800 バイト残ります。次のパケットが 900 バイトの場合、準拠トークンバケットでは 800 バイトしか使用できないため、パケットは準拠していません。

フルの 1000 バイトで始まる超過トークンバケット（超過バーストサイズで指定）に使用可能なバイトがあるかどうかチェックされます。超過トークンバケットには使用可能なバイトが十分あるため、超過処理（QoS 送信値を 1 に設定）が実行され、超過バケットから 900 バイトが取られ、超過トークンバケットの残りは 100 バイトになります。

次のパケットが 0.40 秒後に到達し、トークンバケットに 400 バイトが追加されます ($(.40 \times 8000)/8$)。これで、準拠トークンバケットには 1000 バイトあり（準拠バケットで使用可能な最大トークン数）、200 バイトが準拠トークンバケットをオーバーフローします（準拠トークンバケットの容量を満たすために必要なのは 200 バイトだけのため）。これらのオーバーフローバイトは、超過トークンバケットに置かれ、超過トークンバケットに 300 バイト与えられます。

着信パケットが 1000 バイトの場合、準拠トークンバケットで使用可能なバイト数が十分あるため、パケットは準拠します。パケットにより準拠処理（送信）が実行され、1000 バイトが準拠トークンバケットから削除されます（残り 0 バイト）。

次のパケットが 0.20 秒後に到達し、トークンバケットに 200 バイトが追加されます（ $(.20 \times 8000)/8$ ）。これで、準拠バケットの中身は 200 バイトになります。着信パケットが 400 バイトの場合、準拠トークンバケットでは 200 バイトしか使用できないため、パケットは準拠していません。同様に、超過バケットで使用可能なバイト数は 300 バイトだけなので、パケットは超過しません。したがって、パケットは違反となり、違反処理（ドロップ）が実行されます。

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
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』
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)、階層型ポリシー、ポリシーマップ	「Applying QoS Features Using the MQC」モジュール
トラフィックのポリシングとシェーピング	「Policing and Shaping Overview」モジュール

標準

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

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェアリリース、およびフィチャーセットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
<p>★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。</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

