



クラスベースのポリシング

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。

- [機能情報の確認, 1 ページ](#)
- [クラスベース ポリシングの概要, 2 ページ](#)
- [クラスベース ポリシングに関する制約事項, 3 ページ](#)
- [クラスベース ポリシングの設定方法, 3 ページ](#)
- [クラスベース ポリシングの設定例, 8 ページ](#)
- [その他の関連資料, 11 ページ](#)
- [クラスベース ポリシングの機能情報, 13 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、[バグ検索ツール](#)とプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

クラスベース ポリシングの概要

クラスベース ポリシング機能

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または出力送信レートを制限します。
- ATMセル損失率優先度 (CLP) ビット、フレームリレー廃棄特性 (DE) ビット、IP Precedence 値、IP Diffserv コードポイント (DSCP) 値、MPLS EXP 値、Quality of Service (QoS) グループを設定することによりパケットにマーク付けします。

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 ポリシング機能は、トークン バケット メカニズムで動作します。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てい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ている場合に使用されます。

クラスベース ポリシングの利点

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クラス サービス (CoS) に区切ることができます。パケットがマーキングされ、ダウンストリーム デバイスのトラフィックを識別および分類するためにこれらのマーキングが使用できます。

- 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 precedence または DSCP 値を設定します。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、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場合は、「ネットワークトラフィックのマーキング」モジュールを参照してください。

クラスベース ポリシングに関する制約事項

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が、EtherChannel インターフェイスまたはトンネル インターフェイスではサポートされません。

Cisco ASR 903 ルータに関する制約事項

- サブインターフェイスでのクラスベース ポリシングはサポートされません。
- ポリシングは、入力ポリシー マップでのみサポートされています。
- 階層型ポリシング（親レベルと子レベルの両方でのポリシング）はサポートされません。

クラスベース ポリシングの設定方法

トラフィック ポリシング サービス ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match ip precedence** *precedence-value*
5. **exit**
6. **policy-map** *policy-map-name*
7. **class** {*class-name* | **class-default**}
8. **police** *bps burst-normal burst-max conform-action action exceed-action action violate-action action*
9. **exit**
10. **exit**
11. **interface** *interface-type interface-number*
12. **service-policy** {**input** | **output**} *policy-map-name*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Router> enable</pre>	<p>特権 EXEC モードなど、高位の権限レベルをイネーブルにします。</p> <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	<p>configure terminal</p> <p>例 :</p> <pre>Router# configure terminal</pre>	<p>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。</p>
ステップ 3	<p>class-map [match-all match-any] <i>class-map-name</i></p> <p>例 :</p> <pre>Router(config)# class-map match-any MATCH_PREC</pre>	<p>作成するクラス マップの名前を指定し、QoS クラス マップ コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> クラスマップは、トラフィックを差別化するために使用する条件を定義します。たとえば、クラスマップを使用して、match コマンドを使用して定義した一連の一致基準に基づき、音声トラフィックをデータトラフィックから差別化できます。 <p>(注) match-all または match-any キーワードを指定しない場合、トラフィックがそのトラフィッククラスに分類されるためには、すべての一致基準を満たさなければなりません。</p>
ステップ 4	<p>match ip precedence precedence-value</p> <p>例 :</p> <pre>Router(config-cmap)# match ip precedence 0</pre>	<p>ユーザが指定する IP precedence 値に基づいて一致するパケットをイネーブルにします。</p> <p>(注) 数字の省略形 (0~7) または基準名 (critical、flash など) で、単一の match 文で最大 4 つの一致基準を入力できます。</p>
ステップ 5	<p>exit</p> <p>例 :</p> <pre>Router(config-cmap)# exit</pre>	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 6	<p>policy-map policy-map-name</p> <p>例 :</p> <pre>Router(config)# policy-map POLICE-SETTING</pre>	<p>サービス ポリシーを指定するために 1 つ以上のインターフェイスに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、QoS ポリシー マップ コンフィギュレーション モードを開始します。</p>

	コマンドまたはアクション	目的
ステップ 7	<p>class <i>{class-name class-default}</i></p> <p>例 :</p> <pre>Router(config-pmap)# class MATCH_PREC</pre>	<p>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 クラスとして知られるクラス）を指定し、ポリシーマップコンフィギュレーション モードを開始します。</p>
ステップ 8	<p>police <i>bps burst-normal burst-max conform-action action exceed-action action violate-action action</i></p> <p>例 :</p> <pre>Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1 violate-action drop</pre>	<p>指定されたバースト サイズと任意選択アクションに基づいてトラフィック ポリシングを設定します。</p>
ステップ 9	<p>exit</p> <p>例 :</p> <pre>Router(config-pmap-c)# exit</pre>	<p>(任意) ポリシーマップクラスコンフィギュレーションモードを終了します。</p>
ステップ 10	<p>exit</p> <p>例 :</p> <pre>Router(config-pmap)# exit</pre>	<p>(任意) QoS ポリシーマップコンフィギュレーションモードを終了します。</p>
ステップ 11	<p>interface <i>interface-type interface-number</i></p> <p>例 :</p> <pre>Router(config)# interface GigabitEthernet 0/0/1</pre>	<p>インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> • インターフェイスタイプとインターフェイス番号を入力します。
ステップ 12	<p>service-policy <i>{input output} policy-map-name</i></p> <p>例 :</p> <pre>Router(config-if)# service-policy input POLICE-SETTING</pre>	<p>ポリシー マップをインターフェイスに付加します。</p> <ul style="list-style-type: none"> • input キーワードまたは output キーワードとポリシーマップ名を入力します。
ステップ 13	<p>end</p> <p>例 :</p> <pre>Router(config-if)# end</pre>	<p>(任意) インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p>

トラフィック ポリシングのモニタリングと保守

はじめる前に



(注)

手順の概要

1. **enable**
2. **show policy-map**
3. **show policy-map *policy-map-name***
4. **show policy-map interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	show policy-map 例： Router# 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。
ステップ 3	show policy-map <i>policy-map-name</i> 例： Router# show policy-map pmap	ユーザ指定ポリシー マップを表示します。
ステップ 4	show policy-map interface 例： Router# show policy-map interface	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します。機能がインターフェイスで設定されている場合 • コマンド出力はポリシング統計値を表示します。

クラスベースのトラフィック 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** コマンドを使用します。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** コマンド出力はポリシング統計値を示します。

手順の概要

1. **enable**
2. **show policy-map interface**
3. **show policy-map interface type interface**
4. **show policy-map interface type interface service instance service-instance number**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	show policy-map interface 例： Router# show policy-map interface	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します。機能がインターフェイスで設定されている場合 • コマンド出力はポリシング統計値を表示します。
ステップ 3	show policy-map interface type interface 例： Router# show policy-map interface GigabitEthernet 0/0/1	特定のインターフェイスに適用されたポリシーの表示 トラフィック統計情報を表示します。
ステップ 4	show policy-map interface type interface service instance service-instance number 例： Router# show policy-map interface GigabitEthernet 0/0/1 service instance 1	ポートチャネル下の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。

	コマンドまたはアクション	目的
ステップ 5	exit 例： Router# exit	(任意) 特権 EXEC モードを終了します。

例：クラスベースのトラフィック ポリシングの確認

```
Router# show policy-map interface
FastEthernet1/1/1
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。クラスベース ポリシングがインターフェイスでサポートされていることを確認します。 [クラスベース ポリシングに関する制約事項](#), (3 ページ) を参照してください。

クラスベース ポリシングの設定例

トラフィック ポリシングを含むサービス ポリシーの設定例

次の例では、インターフェイスから離れるすべてのパケットについて、クラスベース ポリシングは 8,000 ビット/秒の平均レート、通常バースト サイズは 1000 バイト、超過バースト サイズは 1000 バイトが設定されています。

```
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 output police-setting
```


FastEthernet インターフェイス 1/1/1 から離れる一連のパケットについての処理は、準拠および超過トークンバケットで残っているパケットのサイズとバイト数によって異なります。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

- 準拠バケットのバイト数がパケット (B など) の長さよりも大きい場合、パケットは準拠しており、バケットから B バイトを削除する必要があります。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。
- 準拠バケットのバイト数がパケット長よりも小さく、超過バケットのバイト数がパケット (B など) の長さよりも大きい場合、パケットは超過しており、B バイトがバケットから削除されます。
- 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)。

次のパケットが 0.25 秒後に到着すると、250 バイトが適合トークンバケットに追加され ((0.25 × 8000) / 8)、適合トークンバケットには 800 バイトが残ります。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 ((0.40 X 8000) / 8)。これにより、準拠トークンバケットは 1000 バイト (準拠バケットで使用可能な最大トークン数) となり、準拠トークンバケットを 200 バイトオーバーフローします (準拠トークンバケットを容量分まで満たすために必要なのがちょうど 200 バイトであるためです)。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 X 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。

クラスベースのトラフィック 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** コマンドを使用します。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** コマンド出力はポリシング統計値を示します。

```
Router# show policy-map interface
FastEthernet1/1/1
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
```

特定のインターフェイスに適用されているポリシーのトラフィック統計情報を表示するには、**show policy-map interface type number** コマンドを使用します。

```
Router# show policy-map interface gigabitethernet 0/0/1
GigabitEthernet0/0/1

Service-policy input: TUNNEL_MARKING

Class-map: MATCH_PREC (match-any)
  72417 packets, 25418367 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: ip precedence 0
QoS Set
  ip precedence tunnel 3
  Marker statistics: Disabled

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

Class-map: class-default (match-any)
  346462 packets, 28014400 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any

Service-policy output: POLICE-SETTING

Class-map: MATCH_PREC (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: ip precedence 0
police:
  cir 8000 bps, bc 1000 bytes, be 1000 bytes
  conformed 0 packets, 0 bytes; actions:
```

```

transmit
exceeded 0 packets, 0 bytes; actions:
  set-qos-transmit 1
violated 0 packets, 0 bytes; actions:
  drop
conformed 0000 bps, exceed 0000 bps, violate 0000 bps

Class-map: class-default (match-any)
  31 packets, 2019 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
    
```

特定のインターフェイスに適用されているポリシーのトラフィック統計情報を表示するには、**show policy-map interface service instance** コマンドを使用します。

```

Router# show policy-map interface gigabitethernet 0/0/1 service instance 1
Service-policy input: p

Class-map: precl (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: ip precedence 1
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 packets, 0 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    drop
  conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
    
```

その他の関連資料

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』
トラフィック マーキング	「ネットワークトラフィックのマーキング」モジュール
トラフィック ポリシング	「トラフィック ポリシング」モジュール
トラフィック ポリシングとシェーピングの概念と概要	「ポリシングとシェーピングの概要」
モジュラ QoS コマンドライン インターフェイス (MQC)	「MQCを使用した QoS 機能の適用」モジュール

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
クラスベース <i>Quality of Service MIB</i> <ul style="list-style-type: none"> • CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB 	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャセットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2697	『 <i>A Single Rate Three Color Marker</i> 』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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 ポリシングの機能情報

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 1: クラスベース ポリシングの機能情報

機能名	リリース	機能情報
クラスベースのポリシング	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータ用にサポートが追加されました。 この機能により、 police コマンドが導入または変更されました。

