クラスベースのポリシング

クラスベース ポリシングを使用すると、インターフェイスでやり取りされる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、ネットワークのエッジにあるインターフェイスで設定され、ネットワークを出入りするトラフィックを制限します。

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、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース 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 ポリシングについて

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、および Quality of Service（QoS）グループを設定することで、パケットにマークを付けます。

クラスベース ポリシングを使用すると、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関連付けると、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われます。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われます。

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 ポリシングを使用すると、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、ネットワークのエッジにあるインターフェイスで設定され、ネットワークを出入りするトラフィックを制限します。 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、ダウンストリーム 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 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キング 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には、「Marking Network Traffic」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 ポリシングを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 インターフェイスやトンネル インターフェイスではサポートされていません。

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ていません。
- 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）はサポートされていません。

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	**enable** 例： `Router> enable`	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。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Router(config)# class-map match-any MATCH_PREC`	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。 • 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。 （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。
ステップ 4	**match ip precedence** *precedence-value* 例： `Router(config-cmap)# match ip precedence 0`	指定する IP precedence 値に基づくパケット照合をイネーブルにします。 （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。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map** *policy-map-name* 例： `Router(config)# policy-map POLICE-SETTING`	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関連付けることができるポリシー マップを作成または変更し、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。

	コマンドまたはアクション	目的
ステップ 7	**class** {*class-name* | **class-default**} 例： `Router(config-pmap)# class MATCH_PREC`	クラスのポリシーを設定する前に、ポリシーの作成/変更対象となるクラスの名前を指定するか、（一般に class-default クラスと呼ばれる）デフォルト クラスを指定してから、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。
ステップ 8	**police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action* 例： `Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1 violate-action drop`	指定したバースト サイズと任意のアクションに基づくトラフィック ポリシングを設定します。
ステップ 9	**exit** 例： `Router(config-pmap-c)# exit`	（オプション）ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 10	**exit** 例： `Router(config-pmap)# exit`	（オプション）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。
ステップ 11	**interface** *interface-type interface-number* 例： `Router(config)# interface GigabitEthernet 0/0/1`	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。 • 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	**service-policy** {**input** | **output**} *policy-map-name* 例： `Router(config-if)# service-policy input POLICE-SETTING`	ポリシー マップをインターフェイスに付加します。 • **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	**end** 例： `Router(config-if)# end`	（オプション）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。

トラフィック ポリシングのモニタリングと保守

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** *policy-map-name* 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。 この機能がインターフェイスで設定されている場合は、 • コマンド出力にポリシング統計情報が表示されます。

クラスベース 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。 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。

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。 この機能がインターフェイスで設定されている場合は、 • コマンド出力にポリシング統計情報が表示されます。
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るポリシーの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。

	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 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

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、インターフェイス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 output police-setting
```

FastEthernet インターフェイス 1/1/1 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（つまり T - T1）x ポリシング レート）/8 バイト

- 準拠バケット内のバイト数がパケットの長さを超えている場合（たとえば B とする）、パケットは準拠しているため、B バイトがバケットから削除されます。 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。
- 準拠バケット内のバイト数がパケットの長さに満たない一方、超過バケット内のバイト数がパケットの長さを超えている場合（たとえば B とする）、パケットは超過しているため、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 バイトが準拠トークン バケットに追加され（（0.25 × 8000）/8）、準拠トークン 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。

（超過バースト サイズで指定された）フルの 1000 バイトで始まる超過トークン バケットに、使用可能なバイトがあるかどうかがチェックされます。 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 X 8000)/8）。 これで、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）になり、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のに 200 バイトだけが必要であったため）。 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 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 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。 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。

```
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
```

その特定のインターフェイスに適用され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 nummber* 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
```

その特定のインターフェイスに適用され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: prec1 (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	「Marking Network Traffic」モジュール
トラフィック ポリシング	「Traffic Policing」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	「Policing and Shaping Overview」
モジュラ QoS コマンドライン インターフェイス（MQC）	「Applying QoS Features Using the MQC」 モジュール

規格

規格	タイトル
なし	--

MIB

MIB	MIB のリンク
クラスベース *Quality of Service MIB* • 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	『*A Single Rate Three Color Marker*』

テクニカル サポート

説明	リンク
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 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、特定のソフトウェア 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

のみを示しています。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 ルータのサポートが追加されました。 次のコマンドが導入または変更されました。**police**。