

クラスベースのポリシングおよび専用アクセスレートの比較

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[トラフィック ポリシングとは](#)

[CAR およびクラスベース ポリシングの比較](#)

[マッチング基準](#)

[準拠および超過アクション](#)

[RFC 2697 および違反アクション](#)

[関連情報](#)

概要

このドキュメントでは、Cisco のレガシートラフィック ポリシング機能である Committed Access Rate (CAR; 専用アクセスレート) と、Cisco の新しいトラフィック ポリサーであるクラスベース ポリシングとの違いを明らかにしています。クラスベース ポリシングは、モジュラ Quality of Service (QoS) Command-Line Interface (CLI; コマンドライン インターフェイス) (MQC) でサービス ポリシーを設定することにより実装されます。トラフィックポリシングとも呼ばれるクラスベースポリシングは、Cisco IOS®ソフトウェア12.1(5)Tで導入されました。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

表記法

ドキュメントの表記法の詳細は、「[シスコ テクニカル ティップスの表記法](#)」を参照してください。

トラフィック ポリシングとは

トラフィック ポリシングにより、インターフェイスで送受信されるトラフィックの最大レートが制御されます。トークン バケットの測定結果に基づいて、パケットのマーキングを行い、パケットをサービスに関する複数のクラスまたはレベルに分けるように、アクションを設定できます。

トラフィック ポリシング機能には、2 つの主要な利点があります。

- **レート制限による帯域幅管理**：インターフェイスで送受信するトラフィックの最大レートを制御できます。トラフィック ポリシングは、通常、ネットワークのエッジにあるインターフェイスに設定され、ネットワークへ出入りするトラフィックを制限します。レート パラメータ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廃棄されるか、または異なるプライオリティで送信されます。
- **IP 優先順位、QoS グループ、または DSCP 値の設定によるパケット マーキング**：パケット 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 Class of Service (CoS; サービス クラス) に分割できます。

トラフィック ポリシングを使用して、IP precedence または Differentiated Services Code Point (DSCP; DiffServ コード ポイント) の値をネットワークに入るパケットに設定します。ネットワーク内にあるネットワーク デバイスでは、調整された IP precedence の値を使用して、トラフィックをどのように取り扱うかが決定されます。たとえば VIP 分散 Weighted Random Early Detection (WRED; 重み付けランダム早期検出) 機能では、『[輻輳回避の概要](#)』で説明されているように、IP precedence の値を使用してパケットが廃棄される確率が決定されます。

CAR およびクラスベース ポリシングの比較

Cisco では、可能な場合は、ネットワークに QoS を実装するためにモジュラ QoS CLI 機能を使用することを推奨しています。バッファリングやキューイングを行わずにレート制限を行うには、サービス ポリシーの police コマンドを介してクラスベース ポリシングを使用します。新しい機能や機能性の計画がない CAR の使用は避けてください。Cisco では、この方式を使用している既存の実装については、CAR のサポートを継続します。

次の表は、クラスベース ポリシングと CAR の機能的な違いをリストしたものです。

機能	クラスベース ポリシング機能	CAR
イネーブル方式	MQC を使用したサービス ポリシー内でイネーブル	インターフェイス上で明示的にイネーブル
コンフィギュレーション コマンド	MQC での police コマンド	インターフェイスまたはサブインターフェイス上での rate-limit コマンド
分類 (トラフィ	Required	必要なし。すべての

ッククラスへの)		IPトラフィックに対して、インターフェイスごとのレート制限をサポート
準拠および非準拠トラフィックについてのアクション	3つのアクション：準拠、超過、および違反	2つのアクション：準拠および超過、違反アクションなし
トークン測定方式	通常バーストおよび最大バーストのための分散トークンバケット	通常バーストおよび最大バーストのための単一トークンバケット
RFC 2697 に対するサポート	あり (Cisco IOS ソフトウェア リリース 12.1(5)T 現在)	No

注：詳細は、このドキュメントの「RFC 2697」および「違反行為」セクションを参照してください。

マッチング基準

CAR とクラスベースのポリシングでは、トラフィックを分類するための照合でサポートされるパケットヘッダー値が異なります。トラフィックの照合では、レート制限やパケットマーキングでトラフィックを識別するプロセスが定義されます。

パケットヘッダー値	サポートレベル	
	クラスベースポリシング機能	CAR
着信または発信インターフェイス	Yes	Yes
すべての IP トラフィックまたは IP パケットが標準または拡張アクセスリストに一致する	Yes	Yes
IP 優先値	Yes	Yes
DSCP	Yes	—
QoS グループ ID	Yes	Yes
MAC Address	Yes	Yes
IP リアルタイムプロトコル (RTP) ポート番号	Yes	—
レイヤ 2 の CoS 値	Yes	—
事前に定義されたクラスマップ	Yes	—
MPLS 経験値	Yes	—

Network-Based Application Recognition (NBAR) プロトコル	Yes	—
--	-----	---

準拠および超過アクション

次の表では、各トラフィックポリシング メカニズムについて、適合するトラフィックおよび適合しないトラフィックに対してサポートされるアクションをリストしています。

アクション	サポート レベル	
	クラスベース ポリシング機能	CAR
continue	—	Yes
drop	Yes	Yes
set-clp-transmit	Yes	Yes
set-dscp-continue	—	Yes
set-dscp-transmit	Yes	Yes
set-frde-transmit	Yes	—
set-mpls-exp-continue	—	Yes
set-mpls-exp-transmit	Yes	Yes
set-prec-continue	—	Yes
set-prec-transmit	Yes	Yes
set-qos-continue	—	Yes
set-qos-transmit	Yes	Yes
送信	Yes	Yes

上の表で示すように、continue アクションがサポートされているのは CAR だけです。このアクションでは、一連のレート制限コマンドで、パケットを次のレート ポリシーに転送するようにルータが設定されます。CAR とクラスベースのポリシングでは、異なるアルゴリズムが使用されます。クラスベースのポリシングでは RFC 2697 および 2698 に基づくアルゴリズムが使用され、continue 文は不要です。詳細については、次のセクションを参照してください。

RFC 2697 および違反アクション

CAR とは異なり、クラスベース ポリシングでは次の 2 つの RFS で指定されるアルゴリズムを使用しています。

- [RFC 2697](#) 「A Single Rate Three Color Marker」 - Cisco IOSリリース12.1(5)T
- [RFC 2698](#) 「A Two Rate Three Color Marker」 - Cisco IOSリリース12.2(4)T

また重要点として、クラスポリシングでは、Cisco IOS のリリースに応じて 2 つのアルゴリズムが使用されていることに注意してください。Cisco IOS ソフトウェア リリース 12.1(5)T では新しいアルゴリズムが導入されており、違反アクションを使用する 2 バケット ポリサーがサポートされています。この 2 バケットのメカニズムにより、CAR とクラスベース ポリシング間の顕著な機能上の違いが示されています。

トークン バケット アルゴリズムでは、それぞれのパケットに対し 3 つのアクションを提供します。適合アクション、超過アクション、および違反アクション。トラフィック ポリシングが設定されているインターフェイスに入るトラフィックは、これらのカテゴリの 1 つに置かれます。こ

これらの3つのカテゴリ内で、ユーザはパケットの処理を決定できます。たとえば、準拠パケットを送信するように設定できます。を超えるパケットは、優先順位を下げて送信されるように設定できます。そして違反をするパケットはドロップするよう設定できます。

違反アクションのオプションを指定すると、トークンバケットアルゴリズムでは適合および超過バーストに対して別々のトークンバケットが使用されます。次の例では、2つのトークンバケットによるトークンバケットアルゴリズムが使用されています。

```
policy-map POLICE
  class twobucket
    police 8000 1000 1000 conform-action transmit exceed-action
      set-dscp-transmit 4 violate-action drop

interface fastethernet 0/0
  service-policy output POLICE
```

違反アクションの設定に関する詳細な説明についてはトラフィックポリシングの「機能の概要」の項を参照してください。

[関連情報](#)

- [クラスベースポリシング](#)
- [QoSに関するサポートページ](#)
- [IPルーティングプロトコルに関するサポートページ](#)
- [IPルーティングに関するサポートページ](#)
- [テクニカルサポート - Cisco Systems](#)