ポリシングとシェーピングの概要

Cisco IOS XE QoS は、ポリシングとシェーピングという 2 種類のトラフィック規制メカニズムを提供します。

これらのトラフィック規制メカニズム（ポリサーおよびシェーパー）をネットワーク全体に展開することで、パケットまたはデータ ソースを規定の契約に確実に準拠させ、パケットをレンダリングする QoS を決定することができます。 ポリシングとシェーピングのメカニズムは、準拠およびサービスを確実に行うために、いずれもパケットの分類によって示されるトラフィック記述子をパケットに使用します。

ポリサーとシェーパーは、通常、トラフィック記述子の違反を同一の方法で識別します。 ただし、通常、違反に対処する方法が異なります。たとえば、

- 通常、ポリサーはトラフィックをドロップしますが、パケットの設定や「マーキング」を変更することもできます。 （たとえば、ポリサーはパケットをドロップするか、またはパケットの IP precedence 値を書き換えて、パケット ヘッダーでのサービス ビットのタイプをリセットします）。
- 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 （たとえば、クラスベース シェーピングではフローをシェーピングするために、重み付け均等化キューを使用してパケットを遅延させます）。

トラフィック シェーピングとトラフィック ポリシングは連携して機能します。 たとえば、優れたトラフィック シェーピング スキームを使用すると、ネットワーク内のノードは動作の不正なフローを簡単に検出できます。 このアクティビティは、フローのトラフィックのポリシングと呼ばれる場合もあります。

この章では、Cisco IOS XE QoS トラフィック ポリシングおよびシェーピングのメカニズムについて簡単に説明します。 ポリシングとシェーピングはいずれもトークン バケット メカニズムを使用するため、この章ではまずトークンバケットがどのように機能するかについて説明します。この章は、次の項で構成されています。

- トークン バケットとは，2 ページ
- トラフィック ポリシング，3 ページ

• トラフィック シェーピングによるパケット フローの規制，3 ページ

トークン バケットとは

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（GTS などのシェーパーの場合はバースト当たりのビット数を指定し、CAR などのポリサーの場合はバーストおよび1秒当たりのバイト数を指定します）。
- 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。調整デバイスは、たとえば CAR のようなトラフィック ポリサーの場合もあれば、FRTS や GTS のようなトラフィック シェーパーの場合もあります。 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。 （CAR、FRTS、および GTS は、真のトークン バケットまたは真のリーキー バケットを実装しません）。

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。

パケットを送信できるだけの十分なトークンがバケット内に存在しない場合、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るか（GTS の場合）、廃棄またはマークダウンされます（CAR の場合）。 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っています。データ バッファを持たない場合は、ポリシング機能になります。 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。特定の速度（バケットの容量を時間間隔で割り、それにトークンバケットへのトークン格納レートを加えた値）を超える速度でフローが送信されないように、バースト性が確実に抑制されます。 次の式を参照してください。

```
(token bucket capacity in bits / time interval in seconds) + established rate in bps =
maximum flow speed in bps
```

このようなバースト性抑制方法は、長期的な送信レートが設定されているバケットへのトークン格納レートを超えないことも保証します。

トラフィック ポリシング

トラフィック ポリシングでは、インターフェイス上で送受信するトラフィックの最大レートを制御し、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）に区切ります。

トラフィック ポリシングでは、トークン バケット アルゴリズムを介して、トラフィックの最大レートを管理します。 トークン バケット アルゴリズムでは、ユーザが設定した値を使用して、特定の瞬間にインターフェイス上で許可されるトラフィックの最大レートを決定できます。 トークン バケット アルゴリズムは、（トラフィック ポリシングを使用するトラフィック ポリシーがどこに設定されているかに応じて）出入りするすべてのトラフィックによる影響を受けます。したがって、同じトラフィック ストリームで複数の大きなパケットが送信される場合、ネットワーク帯域幅を管理するうえで役立ちます。

トークンバケットアルゴリズムは、ユーザに各パケットに対する、準拠（conform）アクション、超過（exceed）アクション、およびオプションの違反（violate）アクションの 3 つを提供します。トラフィック ポリシングが設定されたインターフェイスに入ってくるトラフィックは、これらのカテゴリのいずれかに分類されます。 これら 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、適合したパケットは送信するように設定し、超過したパケットはプライオリティを下げて送信するように設定し、違反したポリシーはドロップするように設定できます。

トラフィック ポリシングは、多くの場合、ネットワークに出入りするトラフィックのレートを制限するためにネットワークのエッジのインターフェイスで設定されます。最も一般的なトラフィック ポリシングの設定では、適合したトラフィックは送信され、超過したトラフィックはプライオリティを下げて送信されるかドロップされます。 ユーザはネットワークのニーズに合わせてこれらの設定オプションを変更できます。

トラフィックシェーピングによるパケットフローの規制

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一致させることができます。