GRE トンネル インターフェイスでの QoS オプション

目次

概要

このドキュメントでは、generic routing encapsulation（GRE; 総称ルーティング カプセル化）を使用したトンネル インターフェイスに設定できる Quality of Service（QoS）機能について検討しています。 IP Security（IPSec; IP セキュリティ）で設定されているトンネルは、このドキュメントの対象範囲外です。

前提条件

要件

このドキュメントに関する固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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 こ

のドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『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。

GRE の概要

GRE トンネルでの QoS について学習する前に、まずトンネル化パケットの形式について理解しておく必要があります。

トンネル インターフェイスは、Cisco IOS(R) ソフトウェアが実行されているルータ上にある、仮想的または論理的なインターフェイスです。 このインターフェイスによって、IP インターネットワークを使用したリモート ポイントにある 2 台の Cisco ルータ間に、仮想的なポイントツーポイント リンクが作成されます。

GRE は IOS でサポートされているカプセル化プロトコルで、RFC 1702sで定義されています。 トンネリング プロトコルは、トランスポート プロトコルの内部でパケットをカプセル化します。

トンネル インターフェイスでは、次の項目に対するヘッダーがサポートされています。

- パッセンジャ プロトコルまたはカプセル化されたプロトコル。IP、AppleTalk、DECnet、IPX など。
- キャリア プロトコル（この場合、GRE）。
- トランスポート プロトコル（この場合、IP のみ）。

トンネル パケットのフォーマットを次に示します。

GRE トンネルの設定についての詳細は、『論理インターフェイスの設定』を参照してください。

GRE トンネルに対するシスコの QoS

トンネル インターフェイスでは、物理インターフェイスと同じ QoS 機能を数多くサポートしています。 以降のセクションでは、サポートされている QoS 機能について説明しています。

シェーピング

Cisco IOS ソフトウェア リリース 12.0(7)T では、トンネル インターフェイスで Generic Traffic Shaping（GTS; ジェネリック トラフィック シェーピング）を直接適用する機能のサポートが導入されています。 次の設定例では、トンネル インターフェイスを整形して、全体の出力レートを 500 Kbps にしています。 詳細は、『ジェネリック トラフィック シェーピングの設定』を参照してください。

```
interface Tunnel0
  ip address 130.1.2.1 255.255.255.0
  traffic-shape rate 500000 125000 125000 1000
  tunnel source 10.1.1.1
  tunnel destination 10.2.2.2
```

Cisco IOS ソフトウェア リリース 12.1(2)T では、modular QoS command-line interface（MQC;

モジュラ QoS コマンドライン インターフェイス) を使用したクラスベース シェーピングのサポートが追加されています。 次の設定例では、MQC コマンドを使用して同じシェーピング ポリシーをトンネル インターフェイスに適用する方法を示しています。 詳細は、『クラスベース シェーピングの設定』を参照してください。

```
policy-map tunnel
  class class-default
    shape average 500000 125000 125000
interface Tunnel0
  ip address 130.1.2.1 255.255.255.0
  service-policy output tunnel
  tunnel source 130.1.35.1
  tunnel destination 130.1.35.2
```

ポリシング

インターフェイスで輻輳が発生するようになり、パケットがキューイングされ始めたら、伝送を待機しているパケットにキューイング方法を適用することができます。 Cisco IOS の論理インターフェイスでは、本質的な理由で輻輳状態をサポートせず、キューイング方法を適用するサービス ポリシーの直接的な適用もサポートしていません。 その代わりに、次のようにして階層ポリシーを適用する必要があります。

1. **priority** コマンドによる低遅延キューイングや、**bandwidth** コマンドによる class-based weighted fair queueing (CBWFQ; クラスベース均等化キューイング) など、キューイング メカニズムを構成する「子」または低レベルのポリシーを作成します。 詳細は、『輻輳管理』を参照してください。`policy-map child`
   ```
   class voice
    priority 512
   ```
2. クラスベース シェーピングを適用する「親」またはトップレベルのポリシーを作成します。 子クラスに対するアドミッション制御は、親クラスに対するシェーピング レートをベースとして行われるため、親ポリシーの下でコマンドとして子ポリシーを適用します。`policy-map tunnel`
   ```
   class class-default
    shape average 2000000
    service-policy child
   ```
3. 親ポリシーをトンネル インターフェイスに適用します。`interface tunnel0`
   ```
   service-policy tunnel
   ```

シェーピングを使用しないキューイングを適用するサービス ポリシーによってトンネル インターフェイスが設定されている場合、ルータから次のログ メッセージが出力されます。

```
router(config)# interface tunnel1 router(config-if)# service-policy output child Class Based
Weighted Fair Queueing not supported on this interface
```

トンネル インターフェイスでは、クラスベース ポリシングもサポートされていますが、committed access rate (CAR; 専用アクセス レート) はサポートされていません。

注: 7500 のトンネル インターフェイスでは、サービス ポリシーはサポートされていません。

輻輳回避

Cisco IOS ソフトウェア リリース 11.3T は GREトンネル トンネルか GRE IP ヘッダーに内部パケットをカプセル化する TOS バイトの IP優先順位ビット値をコピーするためにルータを設定する IP 優先順位 値もたらしました、またはマーキングおよび DSCP を。 これらのビット値は、あらかじめゼロに設定されています。 トンネルのエンドポイントの間にある中間ルータでは、IP 優先順位の値を使用して、ポリシー ルーティング、WFQ、および weighted random early detection (WRED; 重み付けランダム早期検出) などの QoS 機能のためのパケットを分類するこ

とができます。

qos pre-classify コマンド

パケットがトンネルまたは暗号化ヘッダーによってカプセル化されている場合は、QoS 機能によって元のパケット ヘッダーを検査したり、正しくパケットを分類することができなくなります。同じトンネルを行き来するパケットは同じトンネル ヘッダーを持つため、物理インターフェイスが輻輳している場合は、これらのパケットは全く同様に処理されます。 仮想私設ネットワーク（VPN）の QoS 機能の導入により、現在では、パケットはトンネリングや暗号化が行われる前に分類できるようになりました。

この例では、tunnel0 がトンネル名になっています。 **qos pre-classify** コマンドを使用すると、tunnel0 で VPN に対する QoS 機能が有効になります。

```
Router(config)# interface tunnel0 Router(config-if)# qos pre-classify
```

注: qos pre-classify コマンドは IP 優先順位か DSCP 以外値に基づいてトラフィックを分類するために使用することができます。 たとえば、このコマンドが使用することができる送信元 および宛先 IPアドレスのような IP フローかレイヤ3 情報に、基づいてパケットを分類したいと思うかもしれません。 IP、プロトコル、またはポートのトラフィックを分類するときだけ **qos pre-classify コマンドが**必要となります。 分類が DSCP コードに基づいている場合、**qos pre-classify が**必要となりません。

QoS ポリシーのためのトラフィックの識別

サービス ポリシーを設定する際には、最初にトンネルを通過するトラフィックを識別することが必要な場合があります。 Cisco IOS では、トンネルのような論理インターフェイスでの、Netflow および IP の Cisco Express Forwarding（CEF; Cisco エクスプレス転送）アカウンティングをサポートしています。 詳細は、『NetFlow サービス ソリューション ガイド』を参照してください。

サービス ポリシーの適用先

サービス ポリシーは、トンネル インターフェイスまたは基礎となる物理インターフェイスのいずれにも適用できます。 ポリシーの適用先の決定は、QoS の目的によって異なります。 また、分類に使用するヘッダーによっても異なります。

- パケットをトンネリング前のヘッダーに基づいて分類したい場合は、**qos-preclassify** を使用しないでトンネル インターフェイスにポリシーを割り当てます。
- パケットをトンネリング後のヘッダーに基づいて分類したい場合は、**qos-preclassify** を使用しないで**物理**インターフェイスにポリシーを割り当てます。 さらに、トンネルに属するすべてのトラフィック、および複数のトンネルをサポートする物理インターフェイスの整形またはポリシングを行いたい場合は、ポリシーを物理インターフェイスに適用します。
- プリトンネルヘッダーに基づいてパケットを分類したいと思うときポリシーを*物理*インターフェイスに適用し、トンネルインターフェイスの **QoS の事前分類を**有効に して下さい。

マルチポイント トンネル インターフェイス

CBWFQ 内部のクラスベース シェーピングは、マルチポイント インターフェイスではサポートされていません。 Cisco Bug ID CSCds87191 では、ポリシーが拒否された際にルータからエラー

メッセージが出力されるように設定されています。

既知の問題

まれな条件において、**shape** コマンドを使用して設定されたサービス ポリシーを適用すると、CPU の利用率が高くなり、アライメント エラーが生じます。 CPU負荷は不正確にアウトプットインターフェイスおよび隣接関係 の リライト情報を設定 する CEF によってそれから引き起こされるアラインメント エラーの記録によって引き起こされます。 この問題は非 RSP プラットフォーム (ローエンド) と、パーティクルベースの CEF スイッチングを使用しているプラットフォームにのみ影響が及ぶもので、Cisco Bug ID CSCdu45504 と CSCuk30302 で解決されています。また、次の回避策を検討することもできます。

- GRE カプセル化を **tunnel mode ipip** で置き換える。
- **shape** コマンドを **police** コマンドで置き換える。
- トンネルをサポートしている物理インターフェイスにシェーピングを設定する。

関連情報

- 仮想私設ネットワークの QoS
- ケーブルを介した GRE トンネルの設定
- QoS に関するサポート ページ
- OSPF を使用した GRE トンネル over IPSec の設定
- テクニカルサポートとドキュメント - Cisco Systems