



QoS

衛星接続を使用した長距離電話では、会話が、短い間ですが認識できる程度に割り込みされ、不定期に中断されることがあります。このような中断は、ネットワークで送信されるパケットが到着する間隔の時間で、遅延と呼ばれます。音声やビデオなどのネットワークトラフィックでは、長時間の遅延は許容されません。Quality of Service (QoS) 機能を使用すると、重要なトラフィックのプライオリティを高くし、帯域幅の過剰な使用を防ぎ、ネットワーク ボトルネックを管理してパケットのドロップを防止できます。



(注)

ASASM については、ASASM の代わりにスイッチで QoS を実行することを推奨します。スイッチの方が、この領域においては多機能です。一般的に、QoS は、ASA よりも広範な機能を持つ傾向がある、ネットワーク内のルータおよびスイッチで実行するのが最適です。

この章では、QoS ポリシーの適用方法について説明します。

- 「QoS について」 (P.13-1)
- 「QoS のガイドライン」 (P.13-3)
- 「QoS の設定」 (P.13-4)
- 「QoS のモニタ」 (P.13-10)
- 「プライオリティ キューイングとポリシングの設定例」 (P.13-12)
- 「QoS の履歴」 (P.13-14)

QoS について

常に変化するネットワーク環境では、QoS は 1 回限りの構成ではなく、ネットワーク設計の継続的で不可欠な要素であることを考慮する必要があります。

この項では、ASA で使用できる QoS 機能について説明します。

- 「サポートされる QoS 機能」 (P.13-2)
- 「トークン バケットとは」 (P.13-2)
- 「ポリシング」 (P.13-2)
- 「プライオリティ キューイング」 (P.13-3)
- 「DSCP (DiffServ) の保存」 (P.13-3)

サポートされる QoS 機能

ASA は、次の QoS の機能をサポートしています。

- **ポリシング**：分類されたフローがネットワーク帯域幅を大量に使用することを防ぐため、クラスごとの最大使用帯域幅を制限できます。詳細については、「[ポリシング](#)」(P.13-2)を参照してください。
- **プライオリティ キューイング**：Voice over IP (VoIP) のような遅延を許されない重要なトラフィックについて、トラフィックを低遅延キューイング (LLQ) に指定することで、常に他のトラフィックより先に送信できます。「[プライオリティ キューイング](#)」(P.13-3)を参照してください。

トークン バケットとは

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（トラフィック ポリサーなど）の管理に使用されます。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。

トークン バケットは、転送レートの正式な定義です。トークン バケットには、バースト サイズ、平均レート、時間間隔という 3 つのコンポーネントがあります。平均レートは通常 1 秒間のビット数で表されますが、次のような関係によって、任意の 2 つの値を 3 番目の値から求めることができます。

平均レート = バースト サイズ / 時間間隔

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、スケジューリングに関する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、バーストあたりのバイト数で指定します。
- **時間間隔**：測定間隔とも呼ばれ、バーストごとの時間を秒単位で指定します。

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。

パケットを送信するための十分なトークンがバケットにない場合、パケットは、パケットが廃棄されるか、ダウン状態とマークされるまで待機します。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。

ポリシング

ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1 つのトラフィック クラスが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超過すると、ASA は超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

プライオリティ キューイング

LLQ プライオリティ キューイングを使用すると、特定のトラフィックフロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。プライオリティ キューイングでは、インターフェイスで LLQ プライオリティ キューが使用されます（「[インターフェイスのプライオリティ キューの設定](#)」(P.13-6) を参照してください）。一方、他のトラフィックはすべて「ベストエフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降の packets はキューに入ることができず、すべてドロップされます。これはテールドロップと呼ばれます。キューがいっぱいになることを避けるには、キューのバッファサイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。

QoS 機能の相互作用のしくみ

ASA で必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能を ASA に設定します。次のことを設定できます。

プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

DSCP (DiffServ) の保存

DSCP (DiffServ) のマーキングは、ASA を通過するすべてのトラフィックで維持されます。ASA は、分類されたトラフィックをローカルにマーク/再マークすることはありません。たとえば、すべてのパケットの完全優先転送 (EF) DSCP ビットを受け取り、「プライオリティ」処理が必要かどうかを判断し、ASA にそれらのパケットを LLQ に入れさせることができます。

QoS のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。マルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

モデルのガイドライン

- (ASA 5512-X ~ ASA 5555-X) プライオリティ キューイングは、Management 0/0 インターフェイスでサポートされていません。
- (ASASM) ポリシングだけがサポートされます。

その他のガイドラインと制限事項

- QoS は単方向に適用されます。ポリシー マップを適用するインターフェイスに出入りする (QoS 機能によって異なります) トラフィックだけが影響を受けます。詳細については、「機能の方向」(P.1-4) を参照してください。
- プライオリティ トラフィックに対しては、**class-default** クラス マップは使用できません。
- プライオリティ キューイングの場合、プライオリティ キューは物理インターフェイス用または ASASM の場合には VLAN 用に設定する必要があります。
- ポリシングでは、to-the-box トラフィックはサポートされません。
- ポリシングでは、VPN トンネルとの間で送受信されるトラフィックはインターフェイスのポリシングをバイパスします。
- ポリシングでは、トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。

QoS の設定

ASA に QoS を実装するには、次の手順を使用します。

-
- ステップ 1 「プライオリティ キューのプライオリティ キューおよび TX リング制限の決定」(P.13-4)。
 - ステップ 2 「インターフェイスのプライオリティ キューの設定」(P.13-6)。
 - ステップ 3 「プライオリティ キューイングとポリシング用のサービス ルールの設定」(P.13-7)。
-

プライオリティ キューのプライオリティ キューおよび TX リング制限の決定

プライオリティ キューおよび TX リング制限を決定するには、次のワークシートを使用します。

- 「キュー制限のワークシート」(P.13-5)
- 「TX リング制限のワークシート」(P.13-5)

キュー制限のワークシート

次のワークシートは、プライオリティキューのサイズを計算する方法を示しています。キューは無限度ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（テールドロップと呼ばれます）。キューがいっぱいになることを避けるには、「[インターフェイスのプライオリティキューの設定](#)」(P.13-6)に従ってキューのバッファサイズを調節します。

ワークシートに関するヒント:

- アウトバウンド帯域幅：たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
- 平均パケットサイズ：この値は、コーデックまたはサンプリング サイズから決定します。たとえば、VoIP over VPN の場合は、160 バイトなどを使用します。使用するサイズがわからない場合は、256 バイトにすることをお勧めします。
- 遅延：遅延はアプリケーションによって決まります。たとえば、VoIP の場合の推奨される最大遅延は 200 ミリ秒です。使用する遅延がわからない場合は、500 ミリ秒にすることをお勧めします。

表 13-1 キュー制限のワークシート

1	$\frac{\text{アウトバウンド帯域幅 (Mbps または Kbps)}}{\text{Mbps} \times 125} = \frac{\text{バイト数}}{\text{ミリ秒}}$	
	$\frac{\text{アウトバウンド帯域幅 (Mbps または Kbps)}}{\text{Kbps} \times .125} = \frac{\text{バイト数}}{\text{ミリ秒}}$	
2	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;"> $\frac{\text{ステップ1からのバイト数}}{\text{ミリ秒}} \div \frac{\text{平均パケットサイズ}}{\text{バイト}} \times \text{遅延 (ミリ秒)} = \text{キュー制限 (パケット数)}$ </td> </tr> </table>	$\frac{\text{ステップ1からのバイト数}}{\text{ミリ秒}} \div \frac{\text{平均パケットサイズ}}{\text{バイト}} \times \text{遅延 (ミリ秒)} = \text{キュー制限 (パケット数)}$
$\frac{\text{ステップ1からのバイト数}}{\text{ミリ秒}} \div \frac{\text{平均パケットサイズ}}{\text{バイト}} \times \text{遅延 (ミリ秒)} = \text{キュー制限 (パケット数)}$		

TX リング制限のワークシート

次のワークシートは、TX リング制限の計算方法を示しています。この制限により、イーサネット送信ドライバが受け入れるパケットの最大数が決まります。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。

ワークシートに関するヒント:

- アウトバウンド帯域幅：たとえば、DSL のアップリンク速度は 768 Kbps などです。プロバイダーに確認してください。
- 最大パケットサイズ：通常、最大サイズは 1538 バイト、またはタグ付きイーサネットの場合は 1542 バイトです。ジャンボフレームを許可する場合（プラットフォームでサポートされている場合）、パケットサイズはさらに大きくなる場合があります。
- 遅延：遅延はアプリケーションによって決まります。たとえば、VoIP のジッタを制御するには、20 ミリ秒を使用します。

表 13-2 TX リング制限のワークシート

1	_____ Mbps × 125 = _____
	アウトバウンド帯域幅 (Mbps または Kbps) _____ バイト数/ミリ秒
2	_____ Kbps × 0.125 = _____
	_____ ÷ _____ × _____ = _____
	ステップ1からのバイト数/ミリ秒 最大パケットサイズ (バイト) 遅延 (ミリ秒) TX リング制限 (パケット数)

インターフェイスのプライオリティ キューの設定

物理インターフェイスでトラフィックに対するプライオリティ キューイングをイネーブルにする場合は、各インターフェイスでプライオリティ キューを作成する必要があります。各物理インターフェイスは、プライオリティトラフィック用と、他のすべてのトラフィック用に、2つのキューを使用します。他のトラフィックについては、必要に応じてポリシングを設定できます。

はじめる前に

- (ASASM) ASASM では、プライオリティ キューイングはサポートされません。
- (ASA 5512-X ~ ASA 5555-X) プライオリティ キューイングは、Management 0/0 インターフェイスでサポートされていません。

手順

ステップ 1 インターフェイスのプライオリティ キューを作成します。

```
priority-queue interface_name
```

例：

```
hostname(config)# priority-queue inside
```

interface_name 引数には、プライオリティキューをイネーブルにする物理インターフェイスの名前、または ASASM の場合は VLAN インターフェイス名を指定します。

ステップ 2 プライオリティ キューのサイズを変更します。

```
queue-limit number_of_packets
```

例：

```
hostname(config-priority-queue)# queue-limit 260
```

デフォルトのキューの制限は 1024 パケットです。キューは無量大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます（テールドロップと呼ばれます）。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファサイズを大きくします。

queue-limit コマンドの値の範囲の上限は、実行時に動的に決まります。この制限を表示するには、コマンドラインで **queue-limit ?** と入力します。主な決定要素は、キューのサポートに必要なメモリと、デバイス上で使用可能なメモリの量です。

指定した **queue-limit** は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。

ステップ 3 プライオリティ キューの深さを指定します。

```
tx-ring-limit number_of_packets
```

例：

```
hostname(config-priority-queue)# tx-ring-limit 3
```

デフォルトの **tx-ring-limit** は 128 パケットです。このコマンドは、イーサネット送信ドライバが受け入れる低遅延パケットまたは通常プライオリティ パケットの最大数を設定します。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。この設定により、ハードウェアベースの送信リングがプライオリティの高いパケットに対して制限以上の余分な遅延を発生させないことが保証されます。

tx-ring-limit コマンドの値の範囲の上限は、実行時に動的に決まります。この制限を表示するには、コマンドラインで **tx-ring-limit ?** と入力します。主な決定要素は、キューのサポートに必要なメモリと、デバイス上で使用可能なメモリの量です。

指定した **tx-ring-limit** は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。

例

次の例は、デフォルトの **queue-limit** と **tx-ring-limit** を使用して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティ キューを構築します。

```
hostname(config)# priority-queue outside
```

次の例は、**queue-limit** を 260 パケット、**tx-ring-limit** を 3 に設定して、インターフェイス「outside」（GigabitEthernet0/1 インターフェイス）にプライオリティ キューを構築します。

```
hostname(config)# priority-queue outside  
hostname(config-priority-queue)# queue-limit 260  
hostname(config-priority-queue)# tx-ring-limit 3
```

プライオリティ キューイングとポリシング用のサービス ルールの設定

同じポリシー マップ内の異なるクラス マップに対し、プライオリティ キューイングとポリシングを設定できます。有効な QoS 設定については、「[QoS 機能の相互作用のしくみ](#)」(P.13-3)を参照してください。

はじめる前に

- プライオリティトラフィックに対しては、**class-default** クラス マップは使用できません。
- (ASASM) ASASM はポリシングだけをサポートします。
- ポリシングでは、**to-the-box** トラフィックはサポートされません。
- ポリシングでは、VPN トンネルとの間で送受信されるトラフィックはインターフェイスのポリシングをバイパスします。
- ポリシングでは、トンネルグループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。
- プライオリティトラフィックの場合は、遅延が問題になるトラフィックだけを指定します。
- ポリシングトラフィックの場合は、他のすべてのトラフィックをポリシングすることも、トラフィックを特定のタイプに制限することもできます。

手順

ステップ 1 プライオリティ キューイングを実行するトラフィックを識別するためのクラス マップを作成します。

```
class-map priority_map_name
```

例：

```
hostname(config)# class-map priority_traffic
```

ステップ 2 クラス マップにトラフィックを指定します。

```
match parameter
```

例：

```
hostname(config-cmap)# match access-list priority
```

詳細については、「[トラフィックの特定 \(レイヤ 3/4 クラス マップ\)](#)」(P.1-14) を参照してください。

ステップ 3 ポリシングを実行するトラフィックを識別するためのクラス マップを作成します。

```
class-map policing_map_name
```

例：

```
hostname(config)# class-map policing_traffic
```

ステップ 4 クラス マップにトラフィックを指定します。

```
match parameter
```

例：

```
hostname(config-cmap)# match access-list policing
```

詳細については、「[トラフィックの特定 \(レイヤ 3/4 クラス マップ\)](#)」(P.1-14) を参照してください。



ヒント トラフィック照合に ACL を使用する場合、ポリシングは ACL で指定された方向にのみ適用されます。つまり、送信元から宛先に向かうトラフィックがポリシングされ、宛先から送信元に向かうトラフィックはポリシングされません。

ステップ 5 ポリシー マップを追加または編集します。

```
policy-map name
```

例：

```
hostname(config)# policy-map QoS_policy
```

ステップ 6 優先されるトラフィック用に作成したクラス マップを指定します。

```
class priority_map_name
```

例：

```
hostname(config-pmap)# class priority_class
```

ステップ 7 クラスのプライオリティ キューイングを設定します。

```
priority
```

例：

```
hostname(config-pmap-c)# priority
```

ステップ 8 ポリシングされるトラフィック用に作成したクラス マップを指定します。

```
class policing_map_name
```

例：

```
hostname(config-pmap)# class policing_class
```

ステップ 9 クラスのポリシングを設定します。

```
police {output | input} conform-rate [conform-burst] [conform-action [drop | transmit]]  
[exceed-action [drop | transmit]]
```

例：

```
hostname(config-pmap-c)# police output 56000 10500
```

次のオプションがあります。

- *conform-burst argument* : 適合レート値にスロットリングするまでに、持続したバーストで許可された最大瞬間バイト数を 1000 ~ 512000000 バイトの範囲で指定します。
- **conform-action** : レートが *conform_burst* 値を下回ったときに実行するアクションを設定します。
- *conform-rate* : このトラフィック クラスのレート制限を 8000 ~ 2000000000 ビット/秒の範囲で設定します。
- **drop** : パケットをドロップします。
- **exceed-action** : レートが *conform-rate* 値 ~ *conform-burst* 値の範囲にあるときに実行するアクションを設定します。
- **input** : 入力方向のトラフィック フローのポリシングをイネーブルにします。
- **output** : 出力方向のトラフィック フローのポリシングをイネーブルにします。
- **transmit** : パケットを送信します。

ステップ 10 1つまたは複数のインターフェイスでポリシー マップをアクティブにします。

```
service-policy policymap_name {global | interface interface_name}
```

例：

```
hostname(config)# service-policy QoS_policy interface inside
```

global オプションはポリシー マップをすべてのインターフェイスに適用し、**interface** は1つのインターフェイスに適用します。グローバルポリシーは1つしか適用できません。インターフェイスのグローバルポリシーは、そのインターフェイスにサービスポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを1つだけ適用できます。

QoS のモニタ

- ・「QoS ポリシーの統計情報」(P.13-10)
- ・「QoS プライオリティの統計情報」(P.13-11)
- ・「QoS プライオリティ キューの統計情報」(P.13-11)

QoS ポリシーの統計情報

トラフィック ポリシングの QoS 統計情報を表示するには、**show service-policy police** コマンドを使用します。

```
hostname# show service-policy police
```

```
Global policy:
```

```
Service-policy: global_fw_policy
```

```
Interface outside:
```

```
Service-policy: qos
```

```
Class-map: browse
```

```
police Interface outside:
```

```
cir 56000 bps, bc 10500 bytes
```

```
conformed 10065 packets, 12621510 bytes; actions: transmit
```

```
exceeded 499 packets, 625146 bytes; actions: drop
```

```
conformed 5600 bps, exceed 5016 bps
```

```
Class-map: cmap2
```

```
police Interface outside:
```

```
cir 200000 bps, bc 37500 bytes
```

```
conformed 17179 packets, 20614800 bytes; actions: transmit
```

```
exceeded 617 packets, 770718 bytes; actions: drop
```

```
conformed 198785 bps, exceed 2303 bps
```

QoS プライオリティの統計情報

priority コマンドを実装するサービス ポリシーの統計情報を表示するには、**show service-policy priority** コマンドを使用します。

```
hostname# show service-policy priority
Global policy:
  Service-policy: global_fw_policy
Interface outside:
  Service-policy: qos
  Class-map: TGI-voice
  Priority:
    Interface outside: aggregate drop 0, aggregate transmit 9383
```

「Aggregate drop」は、このインターフェイスでの合計ドロップ数を示しています。「aggregate transmit」は、このインターフェイスで送信されたパケットの合計数を示しています。

QoS プライオリティ キューの統計情報

インターフェイスのプライオリティ キュー統計情報を表示するには、**show priority-queue statistics** コマンドを使用します。ベストエフォート (BE) キューと低遅延キュー (LLQ) の両方の統計情報が表示されます。次の例に、**test** という名前のインターフェイスに対する **show priority-queue statistics** コマンドの使用方法を示します。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length    = 0

Queue Type      = LLQ
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length    = 0
hostname#
```

この統計情報レポートの内容は次のとおりです。

- 「Packets Dropped」は、このキューでドロップされたパケットの合計数を示します。
- 「Packets Transmit」は、このキューで送信されたパケットの合計数を示します。
- 「Packets Enqueued」は、このキューでキューイングされたパケットの合計数を示します。
- 「Current Q Length」は、このキューの現在の深さを示します。
- 「Max Q Length」は、このキューで発生した最大の深さを示します。

プライオリティ キューイングとポリシングの設定例

次の項では、プライオリティ キューイングとポリシングを設定する例を示します。

VPN トラフィックのクラス マップの例

次の例で、**class-map** コマンドは `tcp_traffic` という ACL を使用して、すべての非トンネル TCP トラフィックを分類します。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

次の例では、より限定的な一致基準を使用して、特定のセキュリティ関連のトンネル グループにトラフィックを分類します。これらの特定の一致基準では、トラフィックが特定のトンネルに分類されるために、最初の一致特性としてトンネルグループ（この例では、すでに定義されている `Tunnel-Group-1`）に一致する必要があります。次に、別の照合行でトラフィックを分類できます（IP DiffServ コード ポイント、緊急転送）。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

次の例では、**class-map** コマンドはトンネル トラフィックと非トンネル トラフィックの両方をトラフィック タイプに従って分類します。

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0
192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L

hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for
tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for
tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

次の例は、クラス トラフィックがトンネルとして指定されておらず、トンネルを通過する場合に、トンネル内のトラフィックをポリシングする方法を示します。この例では、192.168.10.10 がリモート トンネルのプライベート側のホスト マシンのアドレスで、ACL の名前は「`host-over-121`」です。クラスマップ（名前は「`host-specific`」）を作成すると、LAN-to-LAN 接続によるトンネルのポリシングの前に、「`host-specific`」クラスをポリシングできます。この例では、トンネルの前で「`host-specific`」トラフィックのレートが制限され、次にトンネルのレートが制限されます。

```
hostname(config)# access-list host-over-121 extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-121
```

プライオリティとポリシングの例

次の例は、前の項で作成したコンフィギュレーションで構築されています。前の例と同様に、tcp_traffic と TG1-voice という 2 つのクラスマップがあります。

```
hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

第 3 のクラス マップを追加することで、次のように、トンネルおよび非トンネル QoS ポリシーを定義する基本が提供されます。トンネルおよび非トンネルトラフィックに対する単純な QoS ポリシーが作成され、クラス TG1-voice のパケットが低遅延キューに割り当てられ、tcp_traffic および TG1-best-effort フローにレート制限が設定されます。

この例では、tcp_traffic クラスのトラフィックの最大レートは 56,000 ビット/秒で、最大バーストサイズは 10,500 バイト/秒です。TC1-BestEffort クラスの最大レートは 200,000 ビット/秒で、最大バーストは 37,500 バイト/秒です。TC1-voice クラスのトラフィックは、プライオリティクラスに属しているため、最大速度またはバースト レートでポリシングされません。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

```
hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

```
hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500
```

```
hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority
```

```
hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500
```

```
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500
```

```
hostname(config-pmap-c)# service-policy qos global
```

QoS の履歴

機能名	プラットフォームリリース	説明
プライオリティ キューイングとポリシング	7.0(1)	QoS プライオリティ キューイングとポリシングが導入されました。 priority-queue 、 queue-limit 、 tx-ring-limit 、 priority 、 police 、 show priority-queue statistics 、 show service-policy police 、 show service-policy priority 、 show running-config priority-queue 、 clear configure priority-queue の各コマンドが導入されました。
シェーピングおよび階層型プライオリティ キューイング	7.2(4)/8.0(4)	QoS シェーピングおよび階層型プライオリティ キューイングが導入されました。 shape 、 show service-policy shape の各コマンドが導入されました。
ASA 5585-X での 10 ギガビット イーサネットによる標準プライオリティ キューのサポート	8.2(3)/8.4(1)	ASA 5585-X の 10 ギガビット イーサネット インターフェイスでの標準プライオリティ キューのサポートが追加されました。