# Quality of Serviceの実装

## 内容



## 概要

このドキュメントでは、遅延の影響を受けやすいアプリケーションや帯域幅を大量に消費するアプリケーションを含む、さまざまなアプリケーション向けのトランスポートとして機能するネットワークに Quality of Service ( QoS ) を実装するためのいくつかの基本的なガイドラインを示します。これらのアプリケーションによって業務処理は改善しますが、ネットワーク リソースを酷使する可能性があります。QoS を実装することで、ネットワーク内の遅延、遅延変動 ( ジッタ ) 、帯域幅、およびパケットの損失が管理されます。その結果、安全性が高い保証された品質のサービスをアプリケーションに提供することができます。

## QoS を必要とするアプリケーション

まず、ビジネスに不可欠で、保護が必要なアプリケーションを特定します。これには、ネットワーク リソースの取り合いをしているすべてのアプリケーションを検討しなければならない場合があります。この場合、「Netflow Accounting」、「Network-based Application Recognition ( NBAR ) 」、または「QoS Device Manager ( QDM ) 」を使用して、ネットワーク内のトラフィック パターンを分析してください。

NetFlow Accounting を使用すると、ネットワーク トラフィックの詳細が提供されるので、各フローに関連するトラフィックの分類や優先順位を知ることができます。

NBAR は、アプリケーション層までのトラフィックを識別するための分類ツールです。このツールを使用すると、インターフェイスを通過するトラフィック フローごとに、インターフェイス単位、プロトコル単位、および双方向の統計情報が提供されます。NBARはサブポート分類も行います。つまり、アプリケーション ポートよりも詳細な検索と識別が行われます。

QDM は、Web ベースのネットワーク管理アプリケーションであり、ルータ上の IP ベースの QoS 拡張機能を設定または管理するための操作性の優れたグラフィカル ユーザ インターフェイスを提供します。

## アプリケーションの特性の理解

保護を必要とするアプリケーションの特性を理解することが重要です。遅延やパケット損失によって大きな影響を受けるアプリケーションもあれば、バースト性があったり使用する帯域幅が大きいために、「アグレッシブ」と見なされるアプリケーションもあります。アプリケーションがバースト性の場合は、一定のバーストまたは小さなバーストがあるかどうかを判別します。このアプリケーションのパケット サイズは大きいか小さいか、アプリケーションは TCP ベースまたは UDP ベースのどちらかなのかを判断してください。

| 特性 | ガイドライン |
|---|---|
| 遅延またはパケット損失の影響を受けやすいアプリケーション（音声およびリアルタイム ビデオ） | weighted random early detection（WRED; 重み付けランダム早期検出）、トラフィック シェーピング、断片化（FRF-12）、またはポリシングは使用しないでください。この種のトラフィックには Low Latency Queuing（LLQ; 低遅延キューイング）を実装して、遅延の影響を受けやすいトラフィックにプライオリティ キューイングを使用する必要があります。 |
| バースト性が常にあり、帯域幅を占有するアプリケーションFTP および HTTP） | 帯域幅を確保するには、WRED、ポリシング、トラフィック シェーピング、または class-based weighted fair queueing（CBWFQ; クラスベース重み付け均等化キューイング）を使用します。 |
| TCP ベースのアプリケーション | パケットの損失により TCP がスピードを落とした後、スロースタート アルゴリズムを使って再度速度を上げるので、WREDを使用します。トラフィックがUDPベースで、パケットがドロップされても動作が変更されない場合は、WREDを使用しないでください。アプリケーションのレート制限が必要な場合は、ポリシングを使用します。それ以外の場合は、パケットのテールドロップだけを行います。 |

# ネットワーク トポロジに関する知識

デバイスによっては、実装する QoS 機能を活用できるように、IOS をアップグレードする必要があります。ネットワーク トポロジの図、ルータの設定、および各デバイスに装備されたソフトウェア バージョンを確認すると、IOS をアップグレードする必要のあるデバイス数を予測できます。ネットワーク図の作成時に役立つアイコンについては、「Cisco アイコン ライブラリ」を参照してください。

- ビジーの期間に、各ルータで CPU の利用率にアクセスすると、デバイス間にどのように QoS 機能を分散したら負荷を共有できるのかを判断しやすくなります。
- 業務に不可欠なトラフィックのタイプと、このトラフィックが通過するインターフェイスを分類します。ネットワークの QoS の目標を実現するには、どのプライオリティ グループまたはプライオリティ クラスを作成するかを判断します。
- 業務に不可欠なアプリケーションの大半が処理できる最大の遅延を確認するとともに、この遅延に対応できるように、トラフィック調整機能（トラフィック シェーピング機能やポリシング機能）によってバースト パラメータを調整します。
- 各インターフェースでサポートされるレートを確認します。サポートされている速度を確認し、帯域幅が一致するように設定します。
- 低速リンクを特定して、ネットワーク内のボトルネックが存在する場所を特定し、適切なインターフェイスでリンク効率メカニズムを適用する方法を決定します。
- 業務に不可欠なトラフィックを転送するメディア タイプごとに、レイヤ 2 およびレイヤ 3 のオーバーヘッドを計算します。この結果、クラスごとに必要な正しい総帯域幅を計算できます。
- もう 1 つの重要な情報は、アプリケーションか、IP の発信元または送信先のいずれか、またはその両方に基づいて、トラフィックを保護するかどうかです。

### リンク層のヘッダー サイズ

| メディア タイプ | リンク層のヘッダー |
|---|---|
| イーサネット | 14 バイト |
| PPP | 6 バイト |
| フレーム リレー | 4 バイト |
| ATM | 5 バイト/セル |

## 基準に基づくクラスの作成

アプリケーションの特性に基づいて、どのアプリケーションが QoS を必要とするのか、およびどの分類基準を使用するのかを確認した段階で、この情報に基づいてクラスを作成する準備が整いました。

## ポリシーの作成による各クラスのマーキング

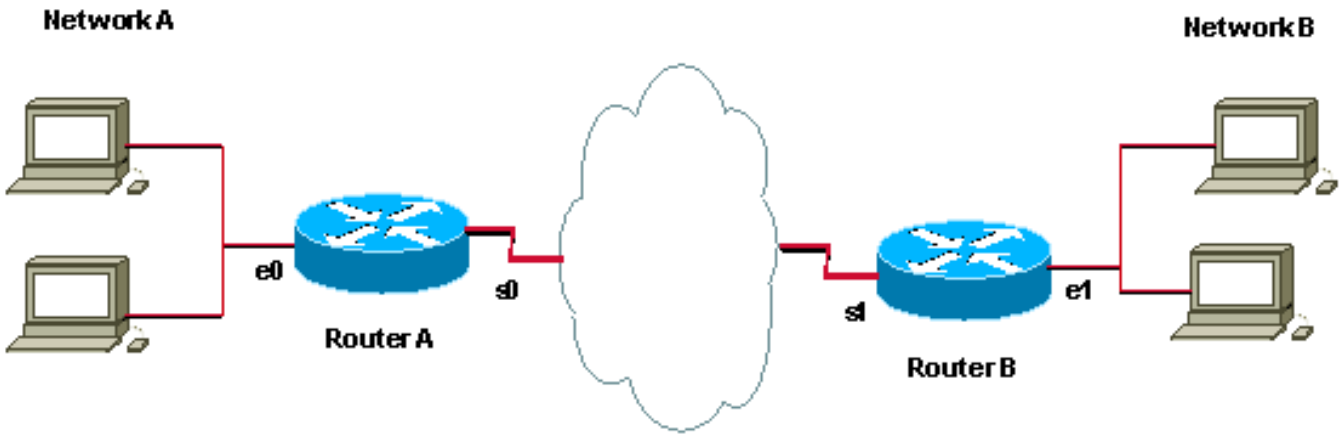
ポリシーを作成して、適切なプライオリティ値でトラフィックの各クラスをマークします（differentiated services control point（DSCP）または IP の優先順位を使用します）。 トラフィックは、ルータで受信される際に入力インターフェイスでマークされます。このマーキングは、トラフィックがルータから発信される際に出力インターフェイスで使用されます。

## エッジからコアへの作業

トラフィックに最も近いルータからコアへ向かって作業します。ルータの入力インターフェイスでマーキングを適用します。次のトポロジでは、ルータAがトラフィックをマークし、ネットワークAから送信されルータB宛てのデータにポリシーを適用する明確な場所です。トラフィックはルータAのEthernet0インターフェイスに着信するとマークされ、ルータAのSerial0インターフェイスにQoSポリシーが適用されます。同じポリシーが双方向に適用された場合（その結果、ネッ

トワーク B から受信されたトラフィックとネットワーク A へ向けられるトラフィックに同じ処理が行われます ) 、ネットワーク B から受信されたトラフィックは、ルータ B の Ethernet1 インターフェイスで受信されるときにマークされます。また、ルータから発信される際に Serial1 インターフェイスにおいて処理が行われます。

ルータの入力側インターフェイスでトラフィックがマーキングされると、再マーキングが実行されない限り、複数のホップを移動する間も同じマーキングが維持されます。 通常、トラフィックは 1 回マーキングするだけで十分です。その他のホップでは、これらのマーキングに基づいて QoS ポリシーを適用できます。再度マークする必要があるのは、トラフィックが信頼できないドメインから到着した場合に限られます。




## トラフィック処理のためのポリシー作成

これでトラフィックをマークできました。このマーキングを使用すると、ポリシーを作成して、ネットワークのその他のセグメントでトラフィックの分類を実行できます。ポリシーには 4 つを越えるクラスは使わないようにし、ポリシーを簡潔にしておくことをお勧めします。

可能であれば、ラボ環境で QoS を実装してテストを行います。ラボ環境での結果に満足できたら、実働ネットワークに QoS を実装します。

## ポリシーの適用

適切な方向にポリシーを適用します。ポリシーを単方向に適用するのか、双方向に適用するのかを判断します。このドキュメントの「各クラスにマークを付けるポリシーの作成」の項で説明されているように、トラフィックをできる限りソースに近い場所にマークして処理してください。

サイトの両側で送受信するトラフィックをフィルタリングするため、双方向で同じポリシーを提供することを推奨します。つまり、ルータ A のシリアル インターフェイスから送信する場合と、ルータ B のシリアル インターフェイスから送信する場合に、同じポリシーを適用する必要があります。

## QoS Policy Manager ( QPM ) によるポリシーの影響の監視

中央集中型のポリシー制御および自動化された高信頼性のポリシー実装のための完全なシステムとして、QPM を使用します。

# QoS に関する一般的な推奨事項

次に、QoS カテゴリ、および各カテゴリーに関連しており、よく使用される QoS 機能のいくつかを示します。

| [Category] | 関連する QoS 機能 |
|---|---|
| QoS サービス モデル | 可能であればプロビジョニングされた（Diffserv）QoS、または必要に応じてシグナリングされた（RSVP）QoS |
| 分類とマーキング | Diffservコードポイントまたはqos-group ID。 |
| 輻輳管理 | LLQまたはCBWFQ。 |
| 輻輳回避 | Diffserv準拠のWRED。 |
| リンクの効率化 | MLPPP、LFI、FRF.11、FRF.12、およびCRTP |
| シグナリング | RSVP、QPPB |
| トラフィック調整機能およびポリシング | クラスベースポリサーおよびGeneric Traffic Shaping(GTS)またはフレームリレートラフィックシェーピング(FRTS)。 |
| 設定および監視 | QPM、Modular QoS Command Line Interface（CLI; コマンドライン インターフェイス）、および QDM |

# 関連情報

- 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
- IS-IS サポート ページ
- テクニカルサポート - Cisco Systems