

Cisco SD-WANでのQoSの実装

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決方法](#)

[Cisco SD-WAN QoSの設定と実装](#)

[QoSポリシーの設定](#)

[関連情報](#)

概要

このドキュメントでは、ソフトウェア定義WAN(SD-WAN)を使用してQuality of Service(QoS)を実装するためのCisco-Viptelaアプローチについて説明します。SD-WANは、世界中の企業、ビジネス、および組織と統合するための最新のイノベーションです。SD-WANテクノロジーの新しい波により、政府や企業は追加の手間をかけずに重要なアプリケーションサポートを提供できます。クラウドによってキャパシティのプロビジョニングプロセスが大幅に簡素化されていますが、QoS管理の分野では新たな課題がいくつか存在します。新しいSD-WANは、アプリケーションとそれをホストするプラットフォームまたはインフラストラクチャによって提供されるパフォーマンス、信頼性、および可用性のレベルに一致する必要があります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SD-WANソリューション
- 従来のQoSおよびポリシー構造

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco vEdgeハードウェアデバイス
- Cisco vEdgeソフトウェア(VM)

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

問題

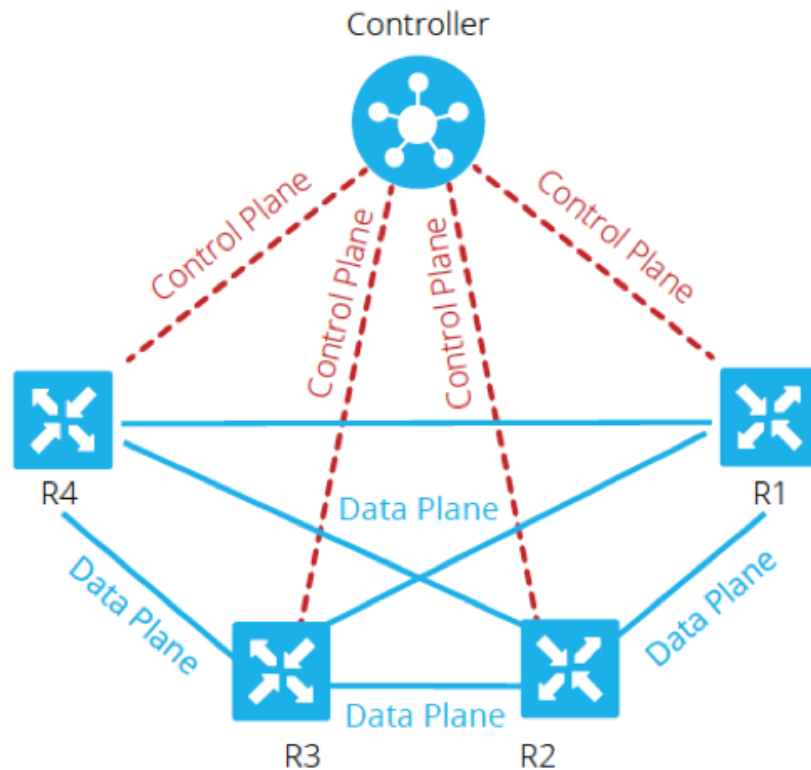
最近まで、ネットワークは基盤となる伝送ネットワークの仕組みに基づいて厳密に構築されてきました。マルチプロトコルラベルスイッチング(MPLS)トラフィックエンジニアリングなどのソリューションは、ノード間のパス選択に影響を与えましたが、2つのエンドポイント間を流れるトラフィックを許可または拒否し、完全に自律的な判断を行うために、送信元から宛先までのすべてのデバイスをプログラムする必要があります。

IP VPNやMPLSなどの従来のキャリアサービスは、組織のQoSサービスを確実に提供する唯一の方法であると多くの人々が想定しています。MPLSの最大の欠点は、帯域幅コストです。今日の消費者は、ビデオや拡張現実(AR)/仮想現実(VR)、およびMPLSが要求する高いメガビットコストなどのマルチメディアコンテンツに対する関心を高めています。最後に、MPLSネットワークは組み込みのデータ保護を提供せず、正しく実装されていない場合は、ネットワークを脆弱性に対して開放する可能性があります。

また、セキュリティの観点からは、MPLSトラフィックはデフォルトでは暗号化されません。MPLSネットワークには多くのセキュリティ機能がありますが、従来のVPNソリューションには課題はありません。事前共有キーはVPN IPsecデバイスの認証に使用されますが、複数のデバイスにまたがる多数の事前共有キーを管理するために使用されるキーは拡張されず、安全性が低くなります。

解決方法

一方、SD-WANアプローチでは、集中型のWANコントローラを使用して、ネットワーク内のノードとの隣接関係をすべてホストおよび管理します。ポリシーの作成と適用に柔軟性をもたらしめます。各デバイスは、接続およびコントロールプレーンポリシーのコントローラとだけピア関係を持ち、サービスノード間でデータトラフィックを渡すため、ネットワーク状態の全体的な可視性に基づいて動的に調整できます。次に示すように、各ルータはローカル情報をコントローラにアドバタイズします。これにより、すべてのローカルルータで適用されるポリシーを使用して、データフローをセントラルコントローラで簡単に操作できます。



この例では、R1とR4にはデータプレーンパスだけのペアワイズ隣接関係がありません。したがって、セントラルコントローラはトラフィックフローを簡単に制御および変更できます。たとえば、R3を介してR4にアドバタイズされるR1からのすべてのプレフィクス、またはR3を介してR4にアドバタイズされるプレフィクス、およびR3がR1から直接アドバタイズされるプレフィクスを制御できます。このアプローチでは、従来のネットワーキングトポロジを使用して、各ルータで実装する必要があるデータプレーンポリシーの量を大幅に削減します。SD-WANは、管理者が重要なトラフィックを特定し、ネットワーク全体で特別な処理を行うのに役立つオーバーレイネットワークです。

Cisco SD-WAN QoSの設定と実装

SD-WANオーバーレイネットワークでは、QoSはネットワークのエッジに入るパケットを検査するときに機能します。SD-WANオーバーレイネットワークとコントロールプレーン接続が起動し、実行中になると、データトラフィックはvEdgeルータ間のIPsec接続を介して自動的に流れます。集中データポリシーまたはローカライズされたデータポリシーが作成され、適用されます。

一元化されたデータポリシーは、ネットワーク経路でルーティングされるトラフィックパスを管理する制御を提供し、パケットのIPヘッダーのアドレス、ポート、およびDifferentiated Services Code Point(DSCP)フィールドに基づいてトラフィックを制御（許可またはブロック）できます。

ローカライズされたデータポリシーは、vEdgeルータのインターフェイスに出入りするデータトラフィックのフローを制御し、QoSなどの機能を有効にします。アクセスリストをアウトバウンド方向またはインバウンド方向で適用すると、ポリシーをアクティブにできます。

各インターフェイスには、ハードウェアvEdgeルータ上の8つのキューがあり、0から7の番号が付

けられています。キュー0は予約されており、制御トラフィックと低遅延キューイング(LLQ)トラフィックの両方に使用されます。LLQでは、キュー0にマップされているすべてのクラスもLLQを使用するように設定する必要があります。すべての制御トラフィックが送信されます。キュー1～7はデータトラフィックに使用できます。

図2.に示すように、QoSポリシーは、あるブランチから別のブランチに送信されるデータパケットに適用されます。

1.入力の分類：着信トラフィックは、各パケットを転送クラスに関連付けることによって分類できます。転送クラスは、データパケットをグループ化し、転送クラスに基づいてパケットを出力キューに割り当てて、宛先に送信します。

2.入力ACLとポリサーの定義：インターフェイス上の送受信データの最大トラフィックレートは、ポリサーを設定し、ネットワークを複数のプライオリティレベルに分割することで制御できます。着信インターフェイストラフィックに適用されるポリサーを使用すると、ネットワーク経由でルーティングする必要のないトラフィックをドロップして、リソースを節約できます。

3.ルートルックアップ：vEdgeルータは、パケットが宛先に到達するために使用するインターフェイスを決定するためにローカルルートテーブルをチェックします。

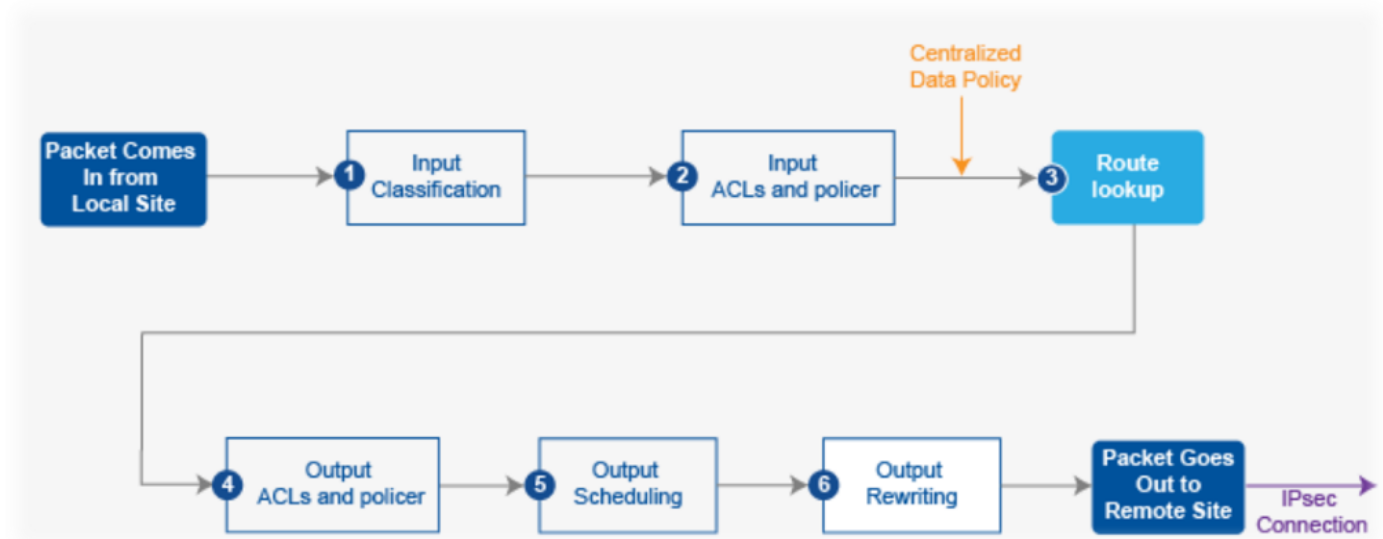
4.出力ACLおよびポリサー：ポリサーレートに準拠したトラフィックが送信され、ポリサーレートを超えるトラフィックは優先順位が下げられて送信されるか、または廃棄されます。アウトバウンドインターフェイストラフィックに適用されるポリサーは、使用される帯域幅を制御します。

5.出力スケジューリング：出力キューの帯域幅、遅延バッファサイズ、およびパケット損失優先度(PLP)を指定するために、出力キューごとにQoSマップを設定することで、パケットの優先順位を設定できます。これは、パケットに帯域幅、バッファレベル、およびドロッププロファイルの上限または下限を割り当てることができるトラフィックの優先順位によって異なります。

6.書き換え出力：ルールを書き換えると、トラフィックがシステムから出たときにポイントをコード化するためにトラフィックをマッピングできます。外部IPヘッダーのDSCPフィールドを上書きするようにrewrite-ruleを定義します。発信(出力)インターフェイスにrewrite-ruleを適用します。

QoSポリシーの設定

次の手順では、ローカライズされたデータポリシー(QoS)設定について説明します。



ステップ1：転送クラスと出力キューへのマッピングを設定します。クラスマップを定義し、パケットを重要度に応じて適切な転送クラスに分類します。アクセスリストのクラスマップを参照してください。

```
policy
```

```
class-map
```

```
class best-effort queue 3
```

```
class bulk-data queue 2
```

```
class critical-data queue 1
```

```
class voice queue 0
```

ステップ2:QoSスケジューラ転送クラスを設定します。qosスケジューラを定義し、インターフェイスでトラフィックが送信されるレートを指定します。アクセスリストのポリサーを参照してください。

```
policy
```

```
qos-scheduler be-scheduler
```

```
class best-effort
```

```
bandwidth-percent 20
```

```
buffer-percent 20
```

```
scheduling wrr
```

```
drops red-drop
```

```
!
```

```
qos-scheduler bulk-scheduler
```

```
class bulk-data
```

```
bandwidth-percent 20
```

```

buffer-percent          20

scheduling              wrt

drops                  red-drop

!

qos-scheduler critical-scheduler

class                  critical-data

bandwidth-percent      40

buffer-percent         40

scheduling             wrt

drops                  red-drop

!

qos-scheduler voice-scheduler

class                  voice

bandwidth-percent      20

buffer-percent         20

scheduling             llq

drops                  tail-drop

```

ステップ3:QoSスケジューラをグループ化し、QoSマップを定義します。

```

policy

qos-map MyQoSMap

qos-scheduler be-scheduler

qos-scheduler bulk-scheduler

qos-scheduler critical-scheduler

qos-scheduler voice-scheduler

```

ステップ4：出カインターフェイスにQoSマップを適用します。

```

interface ge0/1

qos-map MyQoSMap

```

ステップ5：データパケットを適切な転送クラスに分類するために、アクセスリストを定義します。

```

policy

access-list MyACL

```

sequence 10

match

dscp 46

!

action accept

class voice

!

!

sequence 20

match

source-ip 10.1.1.0/24

destination-ip 192.168.10.0/24

!

action accept

class bulk-data

set

dscp 32

!

!

!

sequence 30

match

destination-ip 192.168.20.0/24

!

action accept

class critical-data

set

dscp 22

!

!

!

sequence 40

```
action accept

class best-effort

set

dscp 0

!

!

!

default-action drop
```

ステップ6：アクセスリストをインターフェイスに適用します。

```
vpn 10

interface ge0/0

access-list MyACL in

!
```

関連情報

SD-WANで保証されたQoSを実現するための理想的な要件：

Cisco SD-WAN QoSソリューションは、インターネット上で動的な方法を使用してQoSレベルを提供できるため、ソリューションとしてこれが従来のMPLS WANを脅かす理由を理解することは容易です。SD-WANを使用すると、アプリケーションは標準帯域幅の範囲内ではなく、各アプリケーションに最も適した接続が選択されます。

MPLSとSD-WANのどちらが最適なソリューションであるかに関係なく、VPNでパケット損失のない対称インターネットを使用して、MPLSなしでSD-WANのQoSを実現できることに注意してください。トラフィックが複数のISPを経由して複数のホップを通過する場合、ミッションクリティカルで遅延の影響を受けやすいサービスがどのように実行されるかは企業が保証できません。実際、SD-WAN製品では、WANの信頼性とQoSを向上させるために、アクティブ/アクティブ構成が必要です。

つまり、SD-WANは、将来のMPLSネットワークへの依存度を軽減する優れたテクノロジーです。非インタラクティブトラフィックの一部をブロードバンドインターネット接続にオフロードできます。たとえば、SD-WANは、QoSを保証する音声などの遅延の影響を受けやすいトラフィックをMPLSリンクでルーティングしたり、ブロードバンドインターネット接続で他のすべてをルーティングしたり、2つのブロードバンドリンクを組み合わせるとMPLSを概算できます。