

Cisco SD-WAN에서 QoS 구현

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제](#)

[솔루션](#)

[Cisco SD-WAN QoS 구성 및 구현](#)

[QoS 정책 구성](#)

[관련 정보](#)

소개

이 문서에서는 SD-WAN(Software Defined WAN)으로 QoS(Quality of Service)를 구현하기 위한 Cisco-Viptela 접근 방식에 대해 설명합니다. SD-WAN은 전 세계의 기업, 비즈니스, 조직과 통합하기 위한 가장 최근의 혁신입니다. SD-WAN 기술의 새로운 물결은 정부와 기업이 별도의 번거로움 없이 중요한 애플리케이션 지원을 제공할 수 있게 해줍니다. 클라우드는 용량 프로비저닝 프로세스를 대폭 간소화했지만 QoS 관리 영역에서 몇 가지 새로운 과제를 안고 있습니다. 새로운 SD-WAN은 애플리케이션과 이를 호스팅하는 플랫폼 또는 인프라에서 제공하는 성능, 안정성 및 가용성 수준을 충족해야 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SD-WAN 솔루션
- 기존 QoS 및 정책 구조

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco vEdge 하드웨어 장치
- Cisco vEdge 소프트웨어(VM)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

최근까지 네트워크는 엄격하게 기반 전송망이 어떻게 구축되는지에 따라 구축되었다.

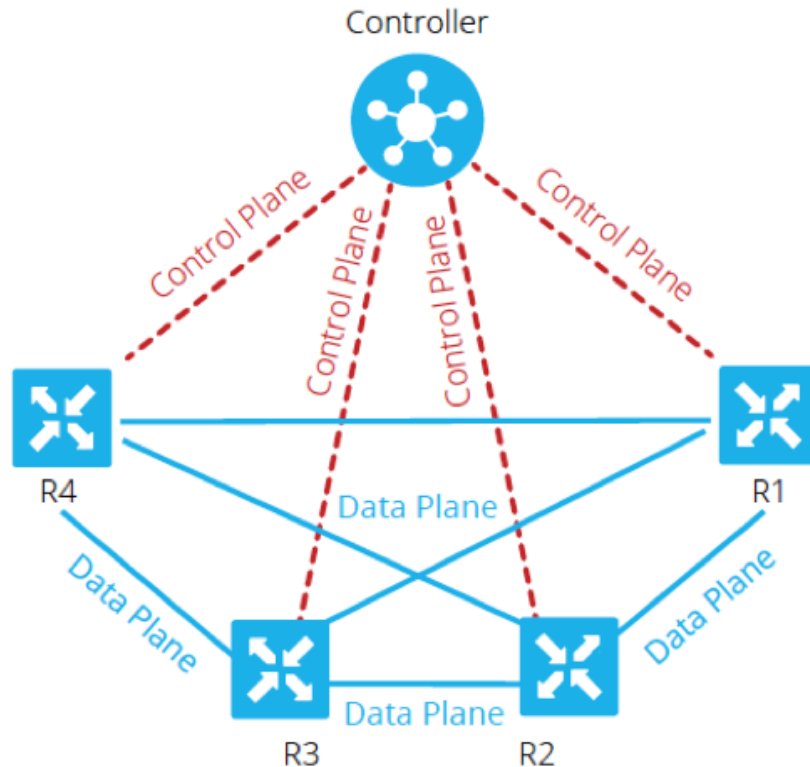
MPLS(Multiprotocol Label Switching) Traffic Engineering과 같은 일부 솔루션은 노드 간의 경로 선택에 영향을 주었지만 두 엔드포인트 간에 흐르는 트래픽을 허용하거나 거부하고 완전히 자율적인 결정을 내리기 위해서는 소스에서 대상에 이르는 모든 디바이스를 프로그래밍해야 했습니다.

IP VPN 또는 MPLS와 같은 기존 통신 사업자 서비스는 조직에 QoS 서비스를 안정적으로 제공할 수 있는 유일한 방법이라고 많은 사람들이 가정했습니다. MPLS의 가장 큰 단점은 대역폭 비용입니다. 오늘날 소비자들은 비디오, AR(Augmented Reality)/VR(Virtual Reality)과 같은 대역폭을 많이 차지하는 멀티미디어 콘텐츠와 MPLS에서 요구하는 메가바이트당 높은 비용에 점점 더 많은 관심을 보이고 있습니다. 마지막으로, MPLS 네트워크는 내장된 데이터 보호 기능을 제공하지 않으며, 잘못 구현되면 네트워크를 취약점에 개방할 수 있습니다.

또한 보안 관점에서 MPLS 트래픽은 기본적으로 암호화되지 않습니다. MPLS 네트워크는 많은 보안 기능을 제공하지만 기존 VPN 솔루션에도 문제가 없습니다. 사전 공유 키는 VPN IPSec 디바이스를 인증하는 데 사용되지만, 여러 디바이스에서 많은 수의 사전 공유 키를 관리하기 위해 확장되지 않으며 보안도 떨어집니다.

솔루션

반면, SD-WAN 접근 방식에서는 중앙 집중식 WAN 컨트롤러를 사용하여 네트워크의 노드가 있는 모든 인접성을 호스팅하고 관리합니다. 정책 생성 및 시행의 유연성을 제공합니다. 각 디바이스는 서비스 노드 간에 데이터 트래픽을 전달하기 위해 연결 및 컨트롤 플레인 정책에 대한 컨트롤러로만 피어링하므로 네트워크 상태에 대한 전반적인 가시성을 기반으로 동적으로 조정할 수 있습니다. 여기에 표시된 것처럼 각 라우터는 컨트롤러에 로컬 정보를 광고합니다. 따라서 중앙 컨트롤러에서 모든 로컬 라우터에 적용되는 정책을 사용하여 데이터 흐름을 쉽게 조작할 수 있습니다.



이 예에서 R1과 R4는 데이터 평면 경로만 쌍방향 인접성이 없습니다. 따라서 중앙 제어기가 트래픽 흐름을 쉽게 제어하고 수정할 수 있습니다. 예를 들어, R3을 통해 R4에 광고되는 R1의 모든 접두사를 제어하거나, R3을 통해 특정 접두사가 R4에 광고되는 반면, R1에서 직접 광고되는 접두사를 제어할 수 있습니다. 여기서 R3은 방화벽 정책에 대한 애플리케이션 지점일 수 있습니다. 이러한 접근 방식은 기존 네트워킹 토폴로지를 사용하여 각 라우터에 구현해야 하는 데이터 플레인 정책의 볼륨을 크게 줄입니다. SD-WAN은 오버레이 네트워크로서 관리자가 중요한 트래픽을 식별하고 네트워크 전체에서 특별한 처리를 할 수 있도록 지원합니다.

Cisco SD-WAN QoS 구성 및 구현

SD-WAN 오버레이 네트워크에서는 QoS가 네트워크 에지에서 들어오는 패킷을 검사할 때 작동합니다. 네트워크의 각 vEdge 라우터는 QoS를 프로비저닝하도록 구성해야 합니다. SD-WAN 오버레이 네트워크 및 컨트롤 플레인 연결이 작동 및 실행되면 vEdge 라우터 간의 IPsec 연결을 통해 데이터 트래픽이 자동으로 이동합니다. 중앙 집중식 데이터 정책 또는 지역화된 데이터 정책을 만들고 적용할 때 기본 데이터 패킷 전달 흐름을 수정할 수 있습니다.

중앙 집중식 데이터 정책은 네트워크를 통해 라우팅되는 트래픽 경로를 관리할 수 있는 제어 기능을 제공하며, 트래픽은 패킷의 IP 헤더에 있는 주소, 포트 및 DSCP(Differentiated Services Code Point) 필드에 따라 제어(허용 또는 차단)될 수 있습니다.

현지화된 데이터 정책은 vEdge 라우터의 인터페이스를 드나드는 데이터 트래픽의 흐름을 제어하고 QoS와 같은 기능을 활성화할 수 있습니다. 아웃바운드 방향 또는 인바운드 방향으로 액세스 목록

록을 적용할 경우 정책을 활성화할 수 있습니다.

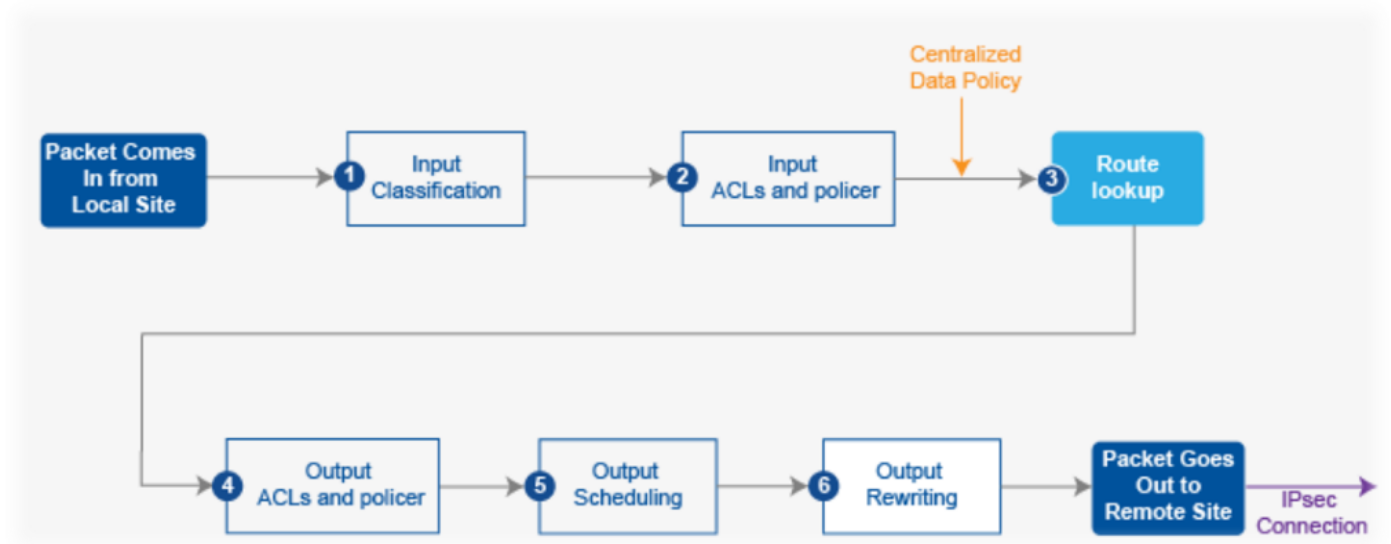
각 인터페이스에는 하드웨어 vEdge 라우터에 0~7의 번호가 지정된 8개의 대기열이 있습니다. 대기열 0은 예약되어 있으며 제어 트래픽과 LLQ(Low-Latency Queuing) 트래픽에 모두 사용됩니다. LLQ의 경우 대기열 0에 매핑된 클래스도 LLQ를 사용하도록 구성해야 합니다. 모든 제어 트래픽이 전송됩니다. 대기열 1~7은 데이터 트래픽에 사용할 수 있습니다.

이미지 2에 나와 있는 것처럼, QoS 정책은 한 브랜치에서 다른 브랜치로 전송될 때 데이터 패킷에 적용됩니다.

1. 입력 분류 - 각 패킷을 포워딩 클래스와 연결하여 수신 트래픽을 분류할 수 있습니다. 포워딩 클래스는 포워딩 클래스에 따라 데이터 패킷을 그룹화하고 목적지로 전송할 패킷을 출력 대기열에 할당합니다.
2. 입력 ACL 및 폴리서 정의 - 폴리서를 구성하여 인터페이스에서 보내거나 받은 데이터의 최대 트래픽 속도를 제어할 수 있으며 네트워크를 여러 우선 순위 레벨로 분할할 수 있습니다. 인바운드 인터페이스 트래픽에 적용되는 폴리서를 사용하면 네트워크를 통해 라우팅할 필요가 없는 트래픽을 삭제하여 리소스를 절약할 수 있습니다.
3. 경로 조회 - vEdge 라우터는 패킷이 목적지에 도달하기 위해 사용해야 할 인터페이스를 결정하기 위해 로컬 경로 테이블을 확인합니다.
4. 출력 ACL 및 폴리서 - 폴리서 속도를 준수하는 트래픽이 전송되며, 폴리서 속도를 초과하는 트래픽은 우선순위가 감소하여 전송되거나 삭제됩니다. 아웃바운드 인터페이스 트래픽에 적용되는 폴리서는 사용되는 대역폭의 양을 제어합니다.
5. 출력 스케줄링 - 출력 대기열의 대역폭, 지연 버퍼 크기 및 PLP(Packet Loss Priority)를 지정하기 위해 각 출력 대기열에 대해 QoS 맵을 구성하여 패킷의 우선 순위를 지정할 수 있습니다. 이는 더 높거나 낮은 대역폭, 버퍼 레벨 및 드롭 프로필을 할당할 수 있는 트래픽의 우선순위에 따라 달라집니다.
6. 출력 재작성 - 규칙을 재작성하면 트래픽이 시스템에서 나갈 때 코드 포인트에 트래픽을 매핑할 수 있습니다. 외부 IP 헤더의 DSCP 필드를 덮어쓰도록 rewrite-rule을 정의합니다. 아웃바운드(이그레스) 인터페이스에 재작성 규칙을 적용합니다.

QoS 정책 구성

다음 단계에서는 현지화된 데이터 정책(QoS) 컨피그레이션에 대해 설명합니다.



1단계. 출력 대기열에 대한 포워딩 클래스 및 매핑을 구성합니다. 중요도별로 패킷을 적절한 포워딩 클래스로 분류하기 위해 클래스 맵을 정의합니다. 액세스 목록의 클래스 맵을 참조하십시오.

policy

class-map

class best-effort queue 3

class bulk-data queue 2

class critical-data queue 1

class voice queue 0

2단계. QoS 스케줄러 포워딩 클래스를 구성합니다. qos 스케줄러를 정의하고 인터페이스에서 트래픽을 전송하는 속도를 지정합니다. 액세스 목록의 폴리서를 참조하십시오.

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           wrr
drops                red-drop
!

qos-scheduler critical-scheduler

class                                critical-data
bandwidth-percent    40
buffer-percent       40
scheduling           wrr
drops                red-drop
!

qos-scheduler voice-scheduler

class                                voice
bandwidth-percent    20
buffer-percent       20
scheduling           llq
drops                tail-drop

```

3단계. QoS 스케줄러를 그룹화하고 QoS 맵을 정의합니다.

```

policy

qos-map MyQoSMap

qos-scheduler be-scheduler
qos-scheduler bulk-scheduler
qos-scheduler critical-scheduler
qos-scheduler voice-scheduler

```

4단계. 이그레스 인터페이스에 QoS 맵을 적용합니다.

```
interface ge0/1

  qos-map  MyQoSMap
```

5단계. 데이터 패킷을 적절한 포워딩 클래스로 분류하기 위해 액세스 목록을 정의합니다.

```
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

```

6단계. 인터페이스에 액세스 목록을 적용합니다.

```

vpn 10

interface ge0/0

access-list MyACL in

!

```

관련 정보

SD-WAN으로 보장된 QoS를 달성하기 위한 이상적인 요건:

Cisco SD-WAN QoS 솔루션이 인터넷을 통해 동적인 방법으로 일치하는 QoS 수준을 제공할 수 있기 때문에 솔루션이 기존 MPLS WAN을 위협하는 이유를 쉽게 이해할 수 있습니다. Cisco SD-WAN은 가장 비용 효율적인 프라이빗 링크 및 공용 인터넷 연결 집합을 동적으로 선택합니다. SD-WAN에서는 애플리케이션이 표준 대역폭에 좌우되지 않지만, 대신 각 앱에 가장 적합한 연결이 선택됩니다.

MPLS 또는 SD-WAN이 최상의 솔루션인지 여부와 상관없이, VPN을 통해 패킷 손실 없이 대칭 인터넷을 사용하는 MPLS 없이 SD-WAN을 사용하는 QoS를 달성할 수 있다는 점에 유의해야 합니다. 트래픽이 여러 ISP를 통해 여러 홉을 통과하는 경우 업무상 중요하고 지연에 민감한 서비스의 수행 방식을 보장할 수 없습니다. 실제로 SD-WAN 제품은 WAN의 신뢰성과 QoS를 개선하기 위해 액티브-액티브 컨피그레이션이 필요합니다.

간단히 말해, SD-WAN은 미래의 MPLS 네트워크에 대한 의존도를 낮추는 환상적인 기술입니다. 일부 비대화형 트래픽을 광대역 인터넷 연결로 오프로드할 수 있습니다. 예를 들어, SD-WAN은 MPLS 링크를 통해 QoS를 보장하는 음성과 같은 레이턴시에 민감한 트래픽을 라우팅하거나 광대역 인터넷 연결을 통해 다른 모든 트래픽을 라우팅할 수 있습니다. 또는 두 개의 광대역 링크를 결합하여 MPLS에 근사화할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.