ASR9000에서 QOS 변경의 DSCP 값 문제 해결

목차

소개

이 문서에서는 Cisco ASR(Aggregation Services Router) 9000에서 QOS(Quality of Service) 정책 상속의 문제를 해결하는 방법에 대해 설명합니다. 이는 물리적 포트의 인그레스 정책 컨피그레이션에 DSCP(Differentiated Services Code Point) 표시가 있는 경우의 라우터 동작을 나타냅니다. 이 정책은 물리적 포트의 모든 레이어 2 및 레이어 3 하위 인터페이스에 적용됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASR9000의 레이어 2 L2VPN(Virtual Private Network) 및 이더넷 서비스 구성
  Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide

- ASR9000의 QoS 구성
  Cisco ASR 9000 Series Aggregation Services Router 모듈식 서비스 품질 컨피그레이션 가이드

사용되는 구성 요소

이 문서의 정보는 Cisco ASR9000 Series를 기반으로 합니다.

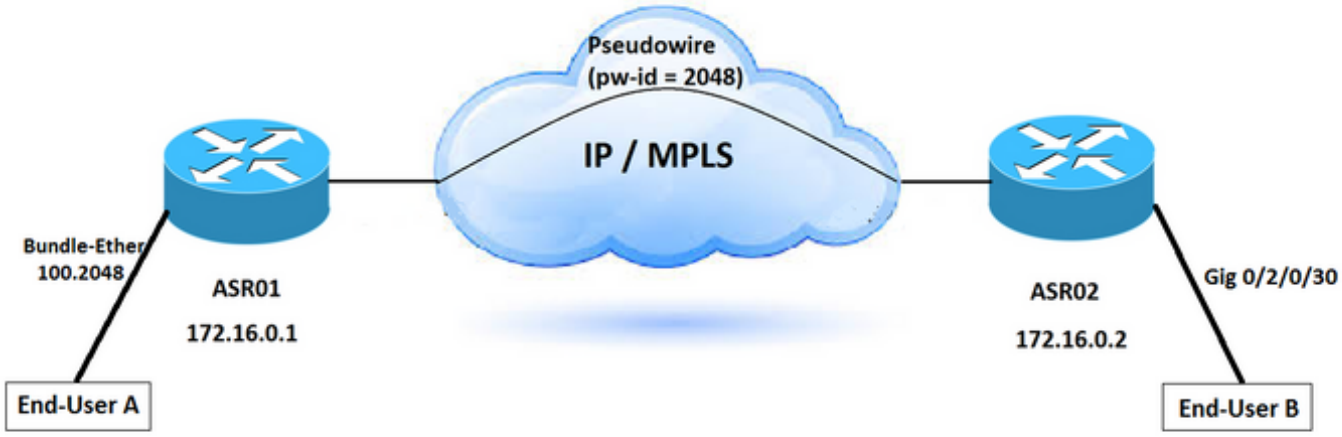
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

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

문제: QOS의 DSCP 값이 한 방향으로 변경됩니다.

패킷은 한 방향으로 표시됩니다. Cisco ASR 9000에서 L2(point-to-point Layer 2) 연결을 통과할 때 QOS에서 새로운 DSCP(Differentiated Services Code Point) 값이 표시됩니다. L2 연결은 MPLS 네트워크를 통해 구현되는 의사 와이어를 통해 구성됩니다. 이 시나리오와 관련된 모든 관련 하위 인터페이스에 대한 DSCP 값을 변경할 특정 컨피그레이션은 없습니다. 원래 패킷은 DSCP 값인 CS4로 표시된 사용자 A에서 전송됩니다. 그러나 user-B가 수신한 패킷에는 AF41로 설정된 DSCP 값이 표시됩니다. 이 문제는 A에서 B로의 한 방향으로만 나타납니다.

토폴로지



문제 해결

트래픽이 L2VPN 연결을 통해 이동한다는 사실을 고려하면 네트워크에서 DSCP 설명이 발생하는 위치를 식별해야 합니다.

패킷 캡처는 DSCP 값이 변경된 위치와 방향을 확인하는 방법 중 하나입니다. 이 시나리오에서는 트래픽이 양방향에서 캡처됩니다. ASR01에서 ASR02로의 한 방향에서 발생하는 문제를 확인할 수 있습니다. DSCP 값은 ASR02에 도달하는 즉시 변경됩니다. 패킷 캡처는 DSCP 값이 ASR01 라우터를 떠난 후에 변경되었음을 확인합니다.

Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide에 따라, ACL(Access Control Lists), 프로토콜 일치, IP 우선 순위, DSCP, IP 패킷의 MPLS(Multiprotocol Label Switching) EXP(experimental bits) 필드 또는 CoS(Class of Service) 등 단일 라우터 내에서 트래픽 흐름을 식별하기 위한 여러 방법이 수행됩니다.

트래픽을 표시하려면 IP Type of Service (ToS) 바이트에서 IP Precedence 또는 DSCP 비트를 설정합니다.

컨피그레이션 확인

근본 원인을 찾기 위해 컨피그레이션을 확인할 수 있습니다.

1단계. L2VPN 구성을 확인합니다.

```
ASR01- Config:
==============
l2vpn
router-id 172.16.0.1
pw-class TEST
encapsulation mpls
protocol ldp
!
bridge group DSCP-TEST
bridge-domain DSCP-TEST
mtu 9216
interface Bundle-Ether100.2048
!
vfi DSCP-TEST
neighbor 172.16.0.2 pw-id 2048
pw-class TEST
!

ASR02- Config:
============
l2vpn
router-id 172.16.0.2

pw-class TEST
encapsulation mpls
protocol ldp
!
bridge group DSCP-TEST
bridge-domain DSCP-TEST
mtu 9216
interface GigabitEthernet0/2/0/30.2048
!
vfi DSCP-TEST
neighbor 172.16.0.1 pw-id 2048
pw-class TEST
```

2단계. 인터페이스 컨피그레이션을 확인합니다.

번들 인터페이스(100)에 구성된 인그레스(ingress) 서비스 정책이 있는데, 이는 최종 사용자들과 연결되고 상이한 L2VPN 서비스들에 대한 다수의 트래픽을 운반한다. 트래픽을 구분하려면 하위 인터페이스를 구성하고 각 트래픽 유형에 대해 고유한 VLAN을 사용합니다.

```
ASR01- Interface Configuration:
================================
RP/0/RSP0/CPU0:ASR1# show running-config interface gigabitEthernet 0/1/0/4
Thu Jun 1 13:17:37.642 AEST
interface GigabitEthernet0/1/0/4
description "TO User-A-TEST"
bundle id 100 mode active
mtu 9192
!
RP/0/RSP0/CPU0:ASR1# show running-config interface Bundle-Ether100.2048
Thu Jun 1 13:17:43.438 AEST
interface Bundle-Ether100.2048 l2transport
encapsulation dot1q 2048 second-dot1q any
```

```
mtu 9216
!
RP/0/RSP0/CPU0:ASR1# show running-config interface gigabitEthernet 0/1/0/4.2048
Thu Jun 1 13:17:43.438 AEST
interface GigabitEthernet0/1/0/4.2048 l2transport
encapsulation dot1q 2048 second-dot1q any
mtu 9216
!
RP/0/RSP0/CPU0:ASR1# show running-config interface Bundle-Ether100
Thu Jun 1 13:20:43.438 AEST
interface Bundle-Ether100
description "To User-A"
mtu 9216
service-policy input INPUT   <<< ========================
service-policy output OUTPUT
bundle maximum-active links 1

ASR02: Interface Configuration:
============================

RP/0/RSP0/CPU0:ASR2#show running-config interface gigabitEthernet 0/2/0/30.2048
Thu Jun 1 15:25:06.742 AEST
interface GigabitEthernet0/2/0/30.2048 l2transport
encapsulation dot1q any
rewrite ingress tag push dot1q 2048 symmetric
mtu 9216
monitor-session span ethernet
!

RP/0/RSP0/CPU0:ASR2#show running-config interface gigabitEthernet 0/2/0/30
Thu Jun 1 15:25:00.516 AEST
interface GigabitEthernet0/2/0/30
description "To User-B"
mtu 9216
monitor-session span ethernet
speed 1000
transceiver permit pid all
!
```

3단계. 서비스 정책 컨피그레이션을 확인합니다.

이 컨피그레이션은 CS4로 표시된 패킷과 일치하는 비디오 트래픽에 대한 정책 맵이 있음을 나타내며 이를 AF41에 알립니다.

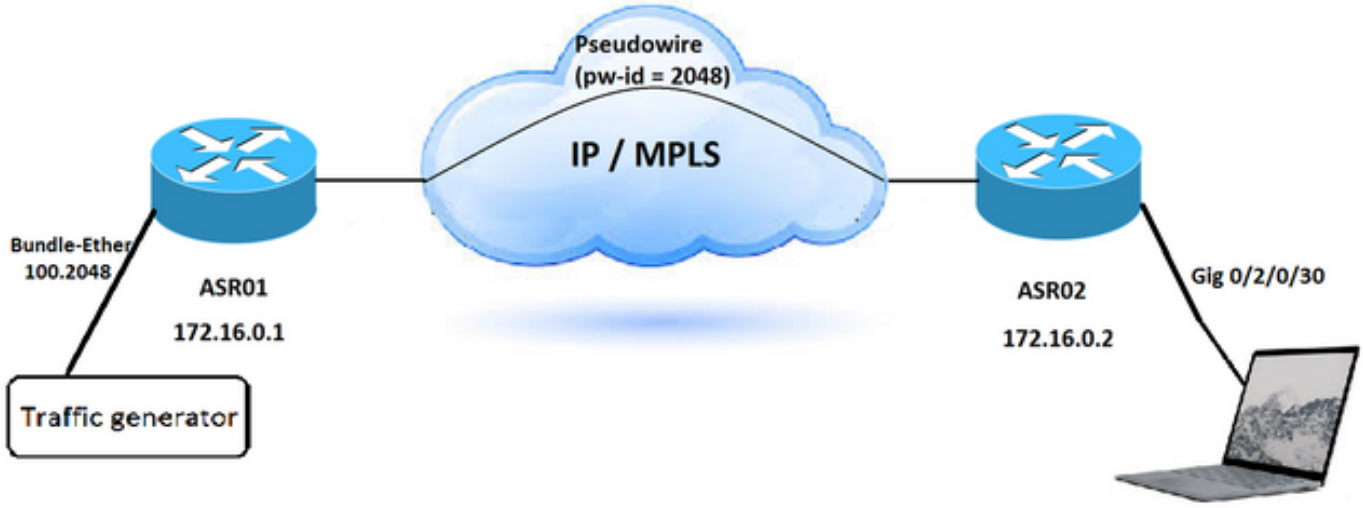
또한 이 정책은 다른 VLAN 태그가 있는 다른 L2VPN 서비스에 대해 구성됩니다. 그러나 이 조건은 이 조건을 충족하는 모든 인그레스 트래픽에 영향을 주는 기본 번들 인터페이스에 적용됩니다.

```
policy-map INPUT
class CS4
set dscp af41
!
class-map match-any CS4
description Video Traffic
match cos 4
end-class-map
!
policy-map OUTPUT
class DSCP
set cos 4
priority level 2
police rate percent 33
```

```
conform-action transmit
exceed-action drop
!
class-map match-any DSCP
description Video Traffic
match dscp af41
end-class-map
```

LAB에서 테스트 시나리오 다시 만들기

LAB에서 동일한 시나리오를 다시 생성하고 이 서비스 정책 컨피그레이션이 수신 트래픽의 DSCP 값에 미치는 영향을 확인할 수 있습니다.



1단계. 서비스 정책 없이 유사한 시나리오를 구성하고 대상에 패킷을 캡처합니다.

DSCP 값은 수신 트래픽에 대해 CS4로 설정되며 대상에서 동일하게 유지됩니다.

```
Ethernet II, Src: XeroxCor_00:0a:00 (00:00:01:00:0a:00), Dst: CiscoInc_e2:05:be
(18:ef:63:e2:05:be)
    Destination: CiscoInc_e2:05:be (18:ef:63:e2:05:be)
    Source: XeroxCor_00:0a:00 (00:00:01:00:0a:00)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2020::1, Dst: 2020::2
    0110 .... = Version: 6
    .... 1000 0000 .... .... .... .... .... = Traffic class: 0x80 (DSCP: CS4, ECN: Not-ECT) <<
============
    .... .... .... 0000 0000 0000 0000 0000 = Flow label: 0x00000
    Payload length: 20
```

2단계. 트래픽 생성기에 연결된 인터페이스의 인그레스 방향에 동일한 서비스 정책을 적용합니다.

3단계. 두 가지 유형의 트래픽을 생성합니다. DSCP 값이 CS4로 설정된 하나와 다른 DSCP 값이 있는 두 번째 하나입니다.

ASR02 이후에 캡처된 패킷은 다음을 나타냅니다.

수신 트래픽의 DSCP 값이 CS4로 설정된 경우, 대상에서 수신된 패킷은 DSCP 값을 AF41로 표시합니다. 그러나 서비스 정책 기준과 일치하지 않는 다른 DSCP 값을 설정하면 패킷이 목적지에 도착할 때 패킷의 DSCP 값이 동일하게 유지됩니다.

```
Ethernet II, Src: XeroxCor_00:0a:00 (00:00:01:00:0a:00), Dst: CiscoInc_e2:05:be
(18:ef:63:e2:05:be)

    Destination: CiscoInc_e2:05:be (18:ef:63:e2:05:be)

    Source: XeroxCor_00:0a:00 (00:00:01:00:0a:00)

    Type: IPv6 (0x86dd)

Internet Protocol Version 6, Src: 2020::1, Dst: 2020::2

    0110 .... = Version: 6

    .... 1000 1000 .... .... .... .... .... = Traffic class: 0x88 (DSCP: AF41, ECN: Not-ECT) <<
============

    .... .... .... 0000 0000 0000 0000 0000 = Flow label: 0x00000

    Payload length: 20
```

솔루션

ASR01 디바이스의 번들 인터페이스(번들 100)에서 구성된 인그레스 서비스 정책은 해당 기준과 일치하는 패킷에 대한 DSCP 값을 다시 씁니다. CS4 값을 검색하여 AF41로 표시합니다. 따라서 이 문제를 해결하려면 인그레스 서비스 정책을 제거해야 합니다.

모듈식 QoS 서비스 패킷 분류 구성 문서는 정책 상속을 설명합니다. 정책 맵이 물리적 포트에 적용되면 해당 물리적 포트 아래의 모든 레이어 2 및 레이어 3 하위 인터페이스에 대해 정책이 시행됩니다.

이는 ASR 9000의 기본 표시 동작입니다.

인그레스 또는 이그레스 인터페이스에 VLAN 태그 또는 MPLS 레이블을 추가하면 CoS 및 EXP의 기본값이 해당 태그 및 레이블로 이동합니다. 그러면 정책 맵을 기반으로 기본값을 덮어쓸 수 있습니다. CoS 및 EXP의 기본값은 시스템에 대한 인그레스 시 패킷의 신뢰할 수 있는 필드를 기반으로 합니다. 라우터는 패킷 유형 및 인그레스 인터페이스 포워딩 유형(레이어 2 또는 레이어 3)을 기반으로 특정 필드의 암시적 신뢰를 구현합니다.

기본적으로 정책 맵이 구성되지 않은 경우 라우터는 IP 우선 순위 또는 DSCP를 수정하지 않습니다.

이는 라우터의 기본 동작입니다.

- xconnect 또는 bridge-domain과 같은 인그레스 또는 이그레스 레이어 2 인터페이스에서는 인그레스 인터페이스에 추가되는 모든 필드에 대해 가장 바깥쪽 CoS 값이 사용됩니다. 레이어 2 재작성으로 인해 추가되는 VLAN 태그가 있는 경우 들어오는 가장 바깥쪽 CoS 값이 새 VLAN 태그에 사용됩니다. MPLS 레이블이 추가된 경우 CoS 값은 MPLS 태그의 EXP 비트에 사용됩니다.
- 인그레스 또는 이그레스 레이어 3 인터페이스(IPv4 또는 IPv6 패킷에 대해 라우팅된 인터페이스 또는 레이블 가중치가 지정된 인터페이스)에서 수신 패킷에서 세 DSCP 및 우선순위 비트가 식별됩니다. MPLS 패킷의 경우 EXP 비트의 가장 바깥쪽 레이블이 식별되며 이 값은 인그레스

인터페이스에서 추가되는 모든 새 필드에 사용됩니다. MPLS 라벨이 추가된 경우, 확인된 우선 순위, DSCP 또는 MPLS EXP 값이 새로 추가된 MPLS 태그의 EXP 비트에 사용됩니다.

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.