

DSCP-waarde probleemoplossing in QOS-wijzigingen in ASR 9000

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem: DSCP-waarde in QOS-wijzigingen in één richting](#)

[Topologie](#)

[Problemen oplossen](#)

[De configuratie verifiëren](#)

[Stap 1. Controleer de L2VPN-configuratie.](#)

[Stap 2. Controleer de interfaceconfiguratie.](#)

[Stap 3. Controleer de configuratie van het servicebeleid.](#)

[Het testscenario in het LAB opnieuw maken](#)

[Oplossing](#)

Inleiding

Dit document beschrijft hoe u beleidsovererving voor Quality of Service (QOS) kunt oplossen in Cisco Aggregation Services Router (ASR) 9000. Het wijst op het routergedrag wanneer er de Gedifferentieerde Markering van de Code van de Diensten (DSCP) in een configuratie van het toegangsbeleid van een fysieke haven is. Dit beleid wordt afgedwongen voor alle Layer 2- en Layer 3-subinterfaces onder die fysieke poort.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Layer 2 Virtual Private Network (L2VPN) en Ethernet-serviceconfiguratie in ASR 9000
[Configuratiehandleiding voor Cisco ASR 9000 Series aggregatieservices voor L2VPN- en Ethernet-services](#)
- Quality-of-Service configuratie in ASR 9000
[Cisco ASR 9000 Series configuratiegids voor aggregatieservices en modulaire Quality-of-Service](#)

Gebruikte componenten

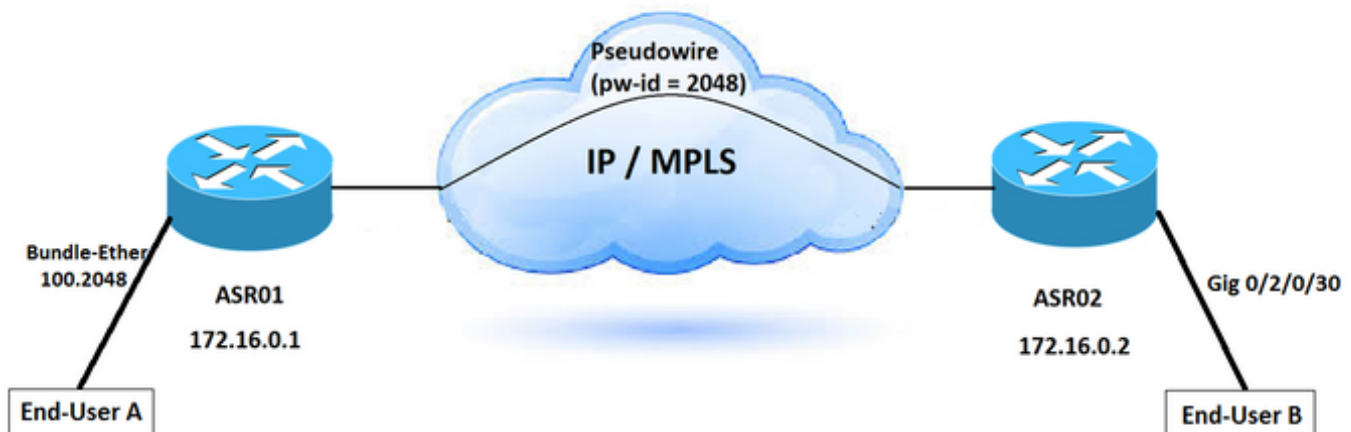
De informatie in dit document is gebaseerd op Cisco ASR 9000 Series.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Probleem: DSCP-waarde in QOS-wijzigingen in één richting

Pakketten worden in één richting gemarkeerd. Het toont een nieuwe DSCP-waarde (Differentiated Services Code Point) in QOS wanneer het door een point-to-point Layer 2 (L2)-connectiviteit op Cisco ASR 9000 gaat. De L2 connectiviteit is geconfigureerd via pseudowires, die worden geïmplementeerd via het MPLS-netwerk. Er is geen specifieke configuratie om de DSCP-waarde te wijzigen voor de gerelateerde subinterfaces die bij dit scenario betrokken zijn. De originele pakketten verzenden van Gebruiker A, die als CS4, een waarde DSCP duidelijk is. De pakketten die door gebruiker-B worden ontvangen, tonen echter de DSCP-waarde die is ingesteld als AF41. Deze kwestie wordt slechts in één richting gezien, namelijk van A naar B.

Topologie



Problemen oplossen

Overweeg het feit dat het verkeer over L2VPN verbinding stroomt, moet u identificeren waar de opmerking DSCP in het netwerk voorkomt.

Packet Capture is een van de manieren om te bevestigen waar en in welke richting de DSCP-waarde wordt gewijzigd. In dit scenario wordt het verkeer vanuit beide richtingen weergegeven. U kunt het probleem zien dat in één richting optreedt, van ASR01 tot ASR02. De DSCP-waarden veranderen zodra de waarde in ASR02 is bereikt. De pakketopname bevestigt dat de DSCP-waarden worden gewijzigd nadat de ASR01-router is verlaten.

In overeenstemming met de [modulaire Quality of Service Configuration Guide van Cisco ASR 9000 Series voor aggregatieservices](#), worden verschillende methoden uitgevoerd voor de

identificatie van de verkeersstroom binnen één router, zoals toegangscontrolelijsten (ACL's), protocolmatching, IP-voorrang, DSCP, Multiprotocol Label Switching (MPLS), experimentele bits (EXP) in IP-pakketten of serviceklasse (CoS).

Stel de IP-voorrang of DSCP-bits in de byte IP Type of Service (ToS) in om het verkeer te markeren.

De configuratie verifiëren

Om de worteloorzaak te vinden, kunt u de configuratie verifiëren.

Stap 1. Controleer de L2VPN-configuratie.

```
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
```

Stap 2. Controleer de interfaceconfiguratie.

In de bundelinterface 100 is een beleid voor toegangsdiensten geconfigureerd, dat is verbonden met de eindgebruikers en meerdere verkeer draagt voor verschillende L2VPN-services. Om het verkeer te onderscheiden, subinterfaces te configureren en uniek VLAN te gebruiken voor elk type verkeer.

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
```

```
!
```

Stap 3. Controleer de configuratie van het servicebeleid.

De configuratie geeft aan dat er een beleidskaart voor videoverkeer is die overeenkomt met het pakket dat als CS4 is gemarkeerd en dit opmerkt in AF41.

Bovendien is dit beleid geconfigureerd voor een andere L2VPN-service met verschillende VLAN-tag. Het is echter wel van toepassing op de belangrijkste bundelinterface die van invloed is op al het toegangsverkeer dat aan deze voorwaarde voldoet.

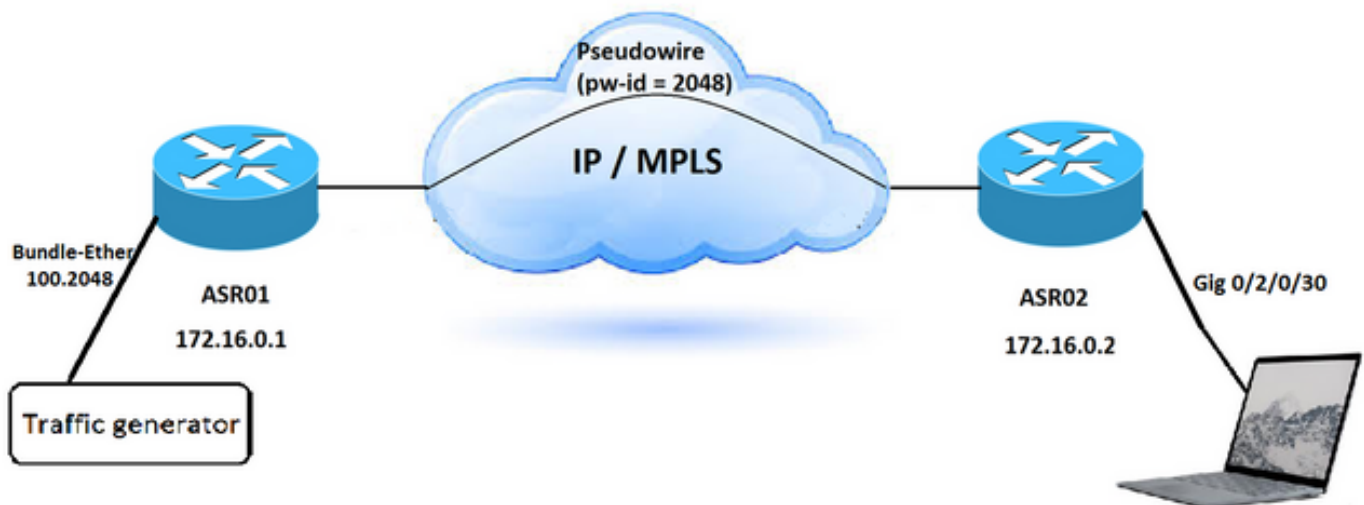
```

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

```

Het testscenario in het LAB opnieuw maken

U kunt hetzelfde scenario opnieuw genereren in het LAB en controleren hoe deze serviceconfiguratie DSCP-waarden van het inkomende verkeer beïnvloedt.



Stap 1. Configureer het vergelijkbare scenario zonder servicebeleid en neem het pakket op in de bestemming.

DSCP-waarde wordt ingesteld op CS4 voor inkomend verkeer en blijft op de bestemming hetzelfde.

```

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

Stap 2. Pas het zelfde de dienstbeleid bij toegangsrichting van de interface toe die met de verkeersgenerator wordt verbonden.

Stap 3. Genereert twee typen verkeer. Een met DSCP-waarde ingesteld op CS4 en de tweede met een andere DSCP-waarde.

Het pakket dat na ASR02 wordt opgenomen, geeft aan:

Wanneer de DSCP-waarde van het inkomende verkeer is ingesteld op CS4, wordt de DSCP-waarde in het op de bestemming ontvangen pakket weergegeven als AF41. Als u echter een andere DSCP-waarde instelt, die niet aan de criteria voor het servicebeleid voldoet, blijft de DSCP-waarde van het pakket hetzelfde wanneer deze op de bestemming aankomt.

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

Oplossing

Het toegangsbeleid dat bij de bundelinterface (bundel 100) in het ASR01-apparaat is geconfigureerd, herschrijft de DSCP-waarden voor de pakketten die aan de criteria voldoen. Het zoekt naar CS4-waarde en merkt deze op met AF41. Daarom moet u het beleid van de toegangsdienst verwijderen om deze kwestie op te lossen.

[Het configureren van het](#) document met de [modulaire QoS-pakketclassificatie voor](#) services beschrijft de beleidsovererving. Wanneer een beleidskaart wordt toegepast op een fysieke poort, wordt het beleid afgedwongen voor alle Layer 2- en Layer 3-subinterfaces onder die fysieke poort.

Dit is het standaardmarkeringsgedrag in ASR 9000:

Wanneer de VLAN-tags of MPLS-labels worden toegevoegd in een inloop- of uitloopinterface, wordt de standaardwaarde voor CoS en EXP naar die tags en labels verplaatst. De standaardwaarde kan vervolgens worden overschreven op basis van de beleidskaart. De standaardwaarde voor CoS en EXP is gebaseerd op een betrouwbaar veld in het pakket bij

toegang tot het systeem. De router implementeert een impliciet vertrouwen van bepaalde velden op basis van het pakkettype en het type voor doorsturen van toegangsinterface (Layer 2 of Layer 3).

Door gebrek, wijzigt de router niet de IP voorrang of DSCP zonder een beleid-kaart die worden gevormd.

Dit is het standaardgedrag van de router:

- Op een inkomende of uitgaande Layer 2-interface, zoals xconnect of bridge-domein, wordt de buitenste CoS-waarde gebruikt voor elk veld dat wordt toegevoegd in de indringingsinterface. Als er een VLAN-tag wordt toegevoegd vanwege een herschrijven van Layer 2, wordt de inkomende buitenste CoS-waarde gebruikt voor de nieuwe VLAN-tag. Als er een MPLS-label wordt toegevoegd, wordt de CoS-waarde gebruikt voor de EXP-bits in de MPLS-tag.
- Op een ingang of uitgang Layer 3-interface (gerouteerd of geëtiketteerd voor IPv4- of IPv6-pakketten) worden de drie DSCP- en prioriteitsbits geïdentificeerd in het inkomende pakket. Voor MPLS-pakketten wordt het buitenste label van EXP-bit geïdentificeerd en deze waarde wordt gebruikt voor elk nieuw veld dat wordt toegevoegd aan de ingangsinterface. Als een MPLS-label wordt toegevoegd, wordt de geïdentificeerde voorrang, DSCP of MPLS EXP-waarde gebruikt voor de EXP-bits in de nieuw toegevoegde MPLS-tag.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.