

Fehlerbehebung: DSCP-Wert bei QoS-Änderungen in ASR9000

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem: DSCP-Wert in QoS ändert sich in eine Richtung](#)

[Topologie](#)

[Fehlerbehebung](#)

[Konfiguration überprüfen](#)

[Schritt 1: Überprüfen der L2VPN-Konfiguration](#)

[Schritt 2: Überprüfen der Schnittstellenkonfiguration](#)

[Schritt 3: Überprüfen der Konfiguration der Servicerichtlinie](#)

[Erstellen des Testszenarios in der Übung](#)

[Lösung](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei der Richtlinienvererbung für Quality of Service (QoS) in Cisco Aggregation Services Router (ASR) 9000 beschrieben. Sie zeigt das Verhalten des Routers an, wenn eine Eingangsrichtlinienkonfiguration eines physischen Ports eine DSCP-Markierung (Differentiated Services Code Point) enthält. Diese Richtlinie wird für alle Layer 2- und Layer 3-Subschnittstellen unter diesem physischen Port durchgesetzt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Layer 2 Virtual Private Network (L2VPN) und Ethernet-Servicekonfiguration in ASR9000

[Konfigurationshandbuch für Cisco Aggregation Services Router der Serie ASR 9000 - L2VPN- und Ethernet-Services](#)

- Quality of Service-Konfiguration beim ASR9000

[Modularer Cisco Aggregation Services Router der Serie ASR 9000 - QoS-Konfigurationsleitfaden](#)

Verwendete Komponenten

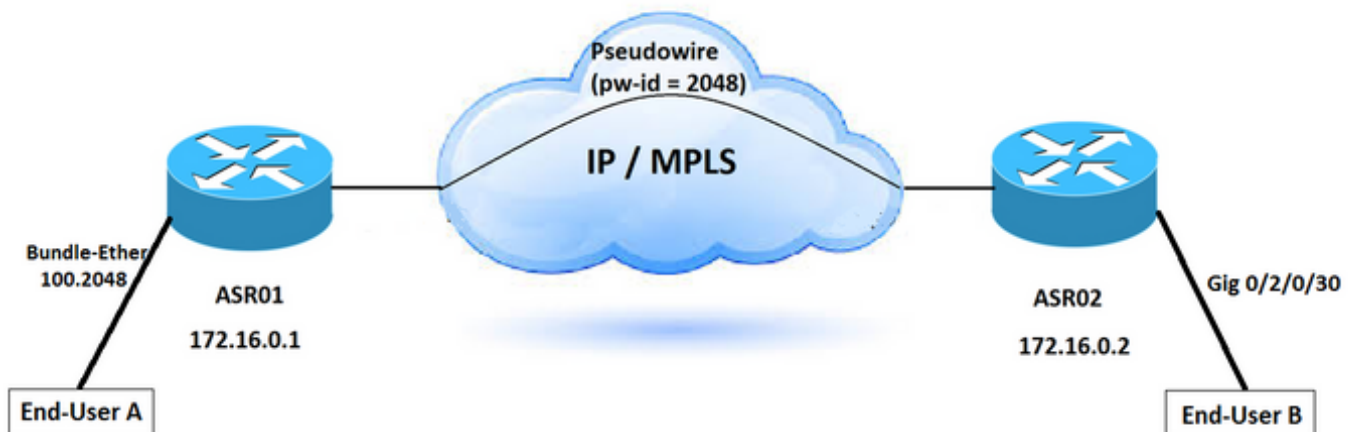
Die in diesem Dokument enthaltenen Informationen basieren auf der Cisco Serie ASR9000.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Problem: DSCP-Wert in QoS ändert sich in eine Richtung

Pakete werden in eine Richtung gekennzeichnet. Er zeigt den neuen Differentiated Services Code Point (DSCP)-Wert in QoS an, wenn er über eine Point-to-Point Layer 2 (L2)-Verbindung auf dem Cisco ASR 9000 übertragen wird. Die Konfiguration der L2-Verbindungen erfolgt über Pseudowire-Emulation, die über das MPLS-Netzwerk implementiert wird. Es gibt keine spezielle Konfiguration, um den DSCP-Wert für eine der in diesem Szenario involvierten Subschnittstellen zu ändern. Die ursprünglichen Pakete werden von Benutzer A gesendet, der als CS4 markiert ist, ein DSCP-Wert. Die vom Benutzer B empfangenen Pakete zeigen jedoch den DSCP-Wert AF41 an. Dieses Problem wird nur in eine Richtung gesehen, nämlich von A nach B.

Topologie



Fehlerbehebung

Wenn Sie bedenken, dass der Datenverkehr über eine L2VPN-Verbindung fließt, müssen Sie bestimmen, wo die DSCP-Anmerkung im Netzwerk auftritt.

Die Paketerfassung ist eine der Möglichkeiten, um zu bestätigen, wo und in welche Richtung der DSCP-Wert geändert wird. In diesem Szenario wird der Datenverkehr aus beiden Richtungen erfasst. Das Problem tritt in eine Richtung von ASR01 zu ASR02 auf. Die DSCP-Werte ändern sich, sobald sie ASR02 erreichen. Die Paketerfassung bestätigt, dass die DSCP-Werte geändert werden, nachdem der ASR01 Router verlassen wurde.

Gemäß dem [Cisco Aggregation Services Router der Serie ASR 9000 Modular Quality of Service Configuration Guide](#) werden verschiedene Methoden zur Identifizierung des Datenverkehrsflusses

innerhalb eines Routers durchgeführt, wie Zugriffskontrolllisten (ACLs), Protokollübereinstimmung, IP-Rangfolge, DSCP, Multiprotocol Label Switching (MPLS)-Feld für experimentelle Bits (EXP) in IP-Paketen oder Class of Service (Class CoS).

Um den Datenverkehr zu markieren, legen Sie die IP-Rangfolge oder die DSCP-Bits im IP Type of Service (ToS)-Byte fest.

Konfiguration überprüfen

Um die Ursache zu ermitteln, können Sie die Konfiguration überprüfen.

Schritt 1: Überprüfen der L2VPN-Konfiguration

```
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
```

Schritt 2: Überprüfen der Schnittstellenkonfiguration

In der Paketschnittstelle 100 ist eine Richtlinie für den eingehenden Service konfiguriert, die mit den Endbenutzern verbunden ist und mehrere Datenströme für verschiedene L2VPN-Services überträgt. Zur Unterscheidung des Datenverkehrs müssen Subschnittstellen konfiguriert und für jede Art von Datenverkehr ein eindeutiges VLAN verwendet werden.

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
```

!

Schritt 3: Überprüfen der Konfiguration der Servicerichtlinie

Die Konfiguration gibt an, dass eine Richtlinienzuordnung für Videodatenverkehr vorhanden ist, die mit dem als CS4 markierten Paket übereinstimmt und dies auf AF41 verweist.

Darüber hinaus wird diese Richtlinie für einen anderen L2VPN-Service mit unterschiedlichen VLAN-Tags konfiguriert. Sie gilt jedoch für die Schnittstelle des Hauptpakets. Dies wirkt sich auf den gesamten eingehenden Datenverkehr aus, der diese Bedingung erfüllt.

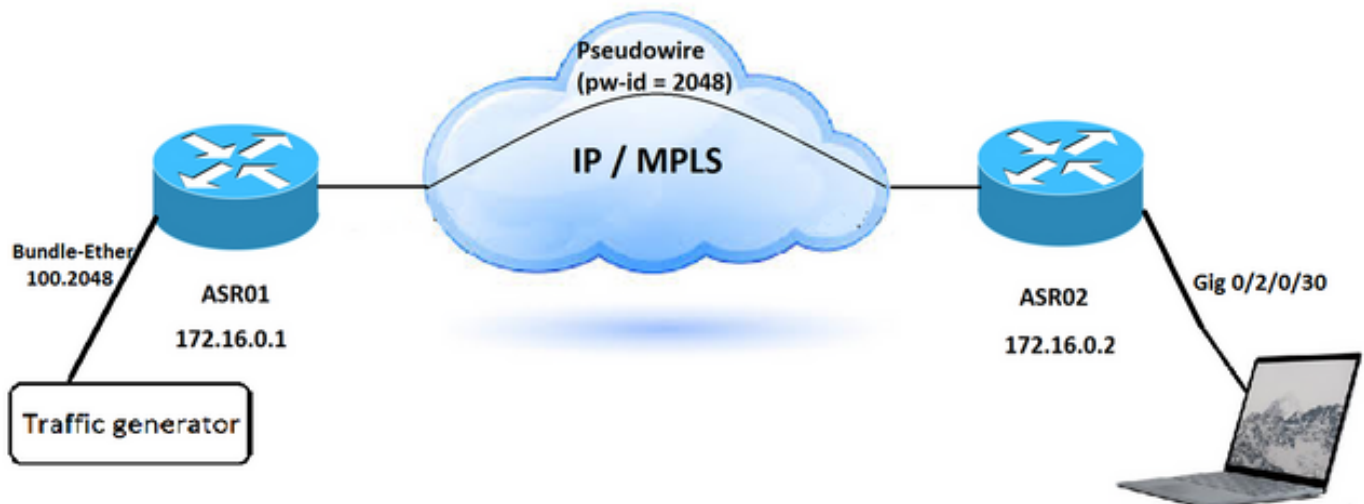
```

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

```

Erstellen des Testszenarios in der Übung

Sie können dasselbe Szenario in der LAB wiederherstellen und überprüfen, wie sich diese Konfiguration der Service-Richtlinie auf die DSCP-Werte des eingehenden Datenverkehrs auswirkt.



Schritt 1: Konfigurieren Sie ein ähnliches Szenario ohne Servicerichtlinie, und erfassen Sie das Paket am Ziel.

Der DSCP-Wert wird für eingehenden Datenverkehr auf CS4 festgelegt und bleibt am Ziel gleich.

```

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

Schritt 2: Wenden Sie die gleiche Service-Richtlinie auf die Eingangsrichtung der Schnittstelle an, die mit dem Datenverkehrsgenerator verbunden ist.

Schritt 3: Generieren Sie zwei Arten von Datenverkehr. Einer mit auf CS4 eingestelltem DSCP-Wert und der zweite mit einem anderen DSCP-Wert.

Das nach ASR02 erfasste Paket weist auf Folgendes hin:

Wenn der DSCP-Wert des eingehenden Datenverkehrs auf CS4 gesetzt ist, zeigt das am Ziel empfangene Paket den DSCP-Wert als AF41 an. Wenn Sie jedoch einen anderen DSCP-Wert festlegen, der nicht den Kriterien der Dienstrichtlinie entspricht, bleibt der DSCP-Wert des Pakets beim Erreichen des Ziels gleich.

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

Lösung

Die auf der Paketschnittstelle (Paket 100) des ASR01 konfigurierte Richtlinie für den eingehenden Service schreibt die DSCP-Werte für die Pakete um, die den Kriterien entsprechen. Es sucht nach CS4-Wert und markiert ihn mit AF41. Daher müssen Sie die Richtlinie für den Eingangsservice entfernen, um dieses Problem zu beheben.

[Das Dokument Configuring Modular QoS Service Packet Classification](#) beschreibt die Richtlinienvererbung. Wenn eine Richtlinienzuordnung auf einen physischen Port angewendet wird, wird die Richtlinie für alle Layer 2- und Layer 3-Subschnittstellen unter diesem physischen Port durchgesetzt.

Dies ist das Standardverhalten für Markierungen in ASR 9000:

Wenn die VLAN-Tags oder MPLS-Labels in einer Eingangs- oder Ausgangsschnittstelle hinzugefügt werden, wird der Standardwert für CoS und EXP zu diesen Tags und Labels verschoben. Der Standardwert kann dann basierend auf der Richtlinienzuordnung überschrieben

werden. Der Standardwert für CoS und EXP basiert auf einem vertrauenswürdigen Feld im Paket beim Eintritt in das System. Der Router implementiert eine implizite Vertrauenswürdigkeit bestimmter Felder, basierend auf dem Pakettyp und dem Weiterleitungstyp der Eingangsschnittstelle (Layer 2 oder Layer 3).

Standardmäßig ändert der Router die IP-Rangfolge oder den DSCP nicht, ohne dass eine Richtlinienzuweisung konfiguriert wird.

Dies ist das Standardverhalten des Routers:

- Auf einer Eingangs- oder Ausgangs-Layer-2-Schnittstelle, z. B. xconnect oder Bridge-Domain, wird der äußerste CoS-Wert für jedes Feld verwendet, das der Eingangs-Schnittstelle hinzugefügt wird. Wenn ein VLAN-Tag aufgrund eines Layer-2-Umschreibens hinzugefügt wird, wird der CoS-Wert für das neue VLAN-Tag in der äußersten Randlage verwendet. Wenn ein MPLS-Label hinzugefügt wird, wird der CoS-Wert für die EXP-Bits im MPLS-Tag verwendet.
- An einer Eingangs- oder Ausgangs-Layer-3-Schnittstelle (geroutet oder mit Label, gewichtet für IPv4- oder IPv6-Pakete) werden die drei DSCP- und Rangfolgebits im eingehenden Paket identifiziert. Bei MPLS-Paketen wird das äußerste Label des EXP-Bits identifiziert, und dieser Wert wird für jedes neue Feld verwendet, das an der Eingangsschnittstelle hinzugefügt wird. Wenn ein MPLS-Label hinzugefügt wird, wird der angegebene Vorrang, DSCP oder MPLS EXP-Wert für die EXP-Bits im neu hinzugefügten MPLS-Tag verwendet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.