Resolución de problemas de valor DSCP en cambios de QOS en ASR9000

Contenido

Introducción

Este documento describe cómo resolver problemas de herencia de políticas de calidad de servicio (QOS) en Cisco Aggregation Services Router (ASR) 9000. Indica el comportamiento del router cuando hay marcado de punto de código de servicios diferenciados (DSCP) en una configuración de política de ingreso de un puerto físico. Esta política se aplica para todas las subinterfaces de Capa 2 y Capa 3 bajo ese puerto físico.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de red privada virtual (L2VPN) de capa 2 y servicio Ethernet en ASR9000

Guía de configuración de servicios Ethernet y L2VPN del router de servicios de agregación Cisco ASR serie 9000

- Configuración de calidad de servicio en ASR9000

Guía de configuración de calidad de servicio modular del router de servicios de agregación Cisco ASR serie 9000

Componentes Utilizados

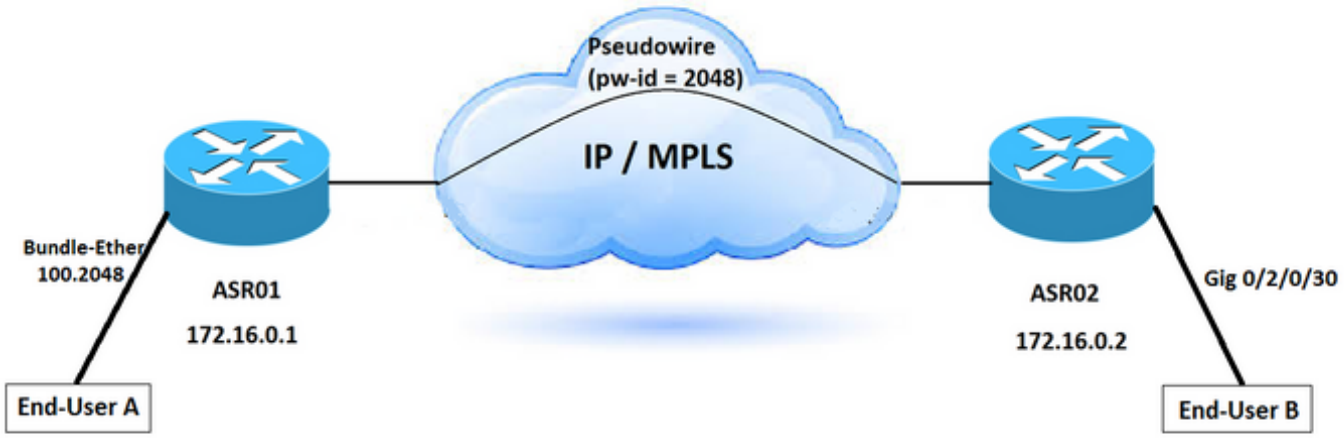
La información de este documento se basa en Cisco ASR9000 Series.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Problema: El valor DSCP en QOS cambia en una dirección

Los paquetes se remarcan en una dirección. Muestra el nuevo valor de punto de código de servicios diferenciados (DSCP) en QOS cuando pasa por una conectividad de capa 2 (L2) punto a punto en Cisco ASR 9000. La conectividad L2 se configura a través de pseudowires, que se implementan en la red MPLS. No existe una configuración específica para cambiar el valor DSCP para ninguna de las subinterfaces relacionadas involucradas en este escenario. Los paquetes originales se envían desde el usuario A, que está marcado como CS4, un valor DSCP. Sin embargo, los paquetes recibidos por el usuario B muestran el valor DSCP configurado como AF41. Este problema se ve solo en una dirección, es decir, de A a B.

Topología



Troubleshoot

Tenga en cuenta el hecho de que el tráfico fluye a través de la conexión L2VPN, debe identificar dónde se produce el comentario DSCP en la red.

La captura de paquetes es una de las formas de confirmar dónde y en qué dirección se cambia el valor DSCP. En este escenario, el tráfico se captura de ambas direcciones. Puede ver el problema que se produce en una dirección de ASR01 a ASR02. Los valores DSCP cambian tan pronto como alcanzan ASR02. La captura de paquetes confirma que los valores DSCP se cambian después de salir del router ASR01.

Según la Guía de configuración de la calidad modular de servicio del router de servicios de agregación de la serie ASR 9000 de Cisco, se realizan varios métodos para la identificación del

flujo de tráfico dentro de un único router, como listas de control de acceso (ACL), coincidencia de protocolos, precedencia de IP, DSCP, campo de bits experimentales (EXP) de conmutación de etiquetas multiprotocolo (MPLS) en paquetes IP, o clase de servicio (CoS).

Para marcar el tráfico, establezca la Precedencia IP o los bits DSCP en el byte de tipo de servicio IP (ToS).

Verificar configuración

Para encontrar la causa raíz, puede verificar la configuración.

Paso 1. Verifique la configuración L2VPN.

```
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
```

Paso 2. Verifique la configuración de la interfaz.

Existe una política de servicio de ingreso configurada en la interfaz del paquete 100, que está conectada a los usuarios finales y transporta tráfico múltiple para diferentes servicios L2VPN. Para diferenciar el tráfico, configure subinterfaces y utilice una VLAN única para cada tipo de tráfico.

```
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
!
```

Paso 3. Verifique la configuración de la política de servicio.

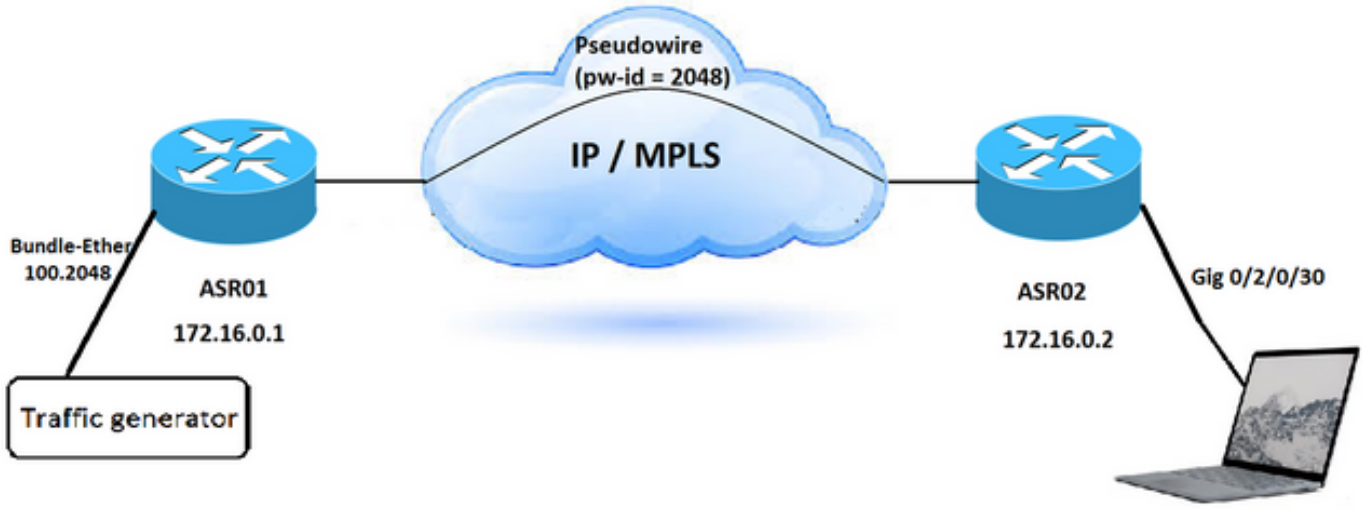
La configuración indica que existe un mapa de políticas para el tráfico de vídeo que coincide con el paquete marcado como CS4 y lo señala como AF41.

Además, esta política se configura para otro servicio L2VPN con una etiqueta VLAN diferente. Sin embargo, se aplica en la interfaz de agrupamiento principal que afecta a todo el tráfico de ingreso que cumple esta condición.

```
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
```

Recrear el escenario de prueba en el LABORATORIO

Puede recrear el mismo escenario en el LAB y verificar cómo esta configuración de política de servicio afecta los valores DSCP del tráfico entrante.



Paso 1. Configure el escenario similar sin ninguna política de servicio y capture el paquete en el destino.

El valor DSCP se establece en CS4 para el tráfico entrante y permanece igual en el destino.

```
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
```

Paso 2. Aplique la misma política de servicio en la dirección de ingreso de la interfaz conectada al generador de tráfico.

Paso 3. Genere dos tipos de tráfico. Uno con el valor DSCP establecido en CS4 y el segundo con cualquier otro valor DSCP.

El paquete capturado después de ASR02 indica:

Cuando el valor DSCP del tráfico entrante se establece en CS4, el paquete recibido en el destino muestra el valor DSCP como AF41. Sin embargo, si configura cualquier otro valor DSCP que no coincida con los criterios de la política de servicio, el valor DSCP del paquete permanece igual cuando llega al destino.

```
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
```

Solución

La política de servicio de ingreso configurada en la interfaz de agrupamiento (agrupamiento 100) en el dispositivo ASR01 vuelve a escribir los valores DSCP para los paquetes que coinciden con sus criterios. Busca el valor CS4 y lo marca con AF41. Por lo tanto, debe eliminar la política de servicio de ingreso para resolver este problema.

El documento Configuración de la clasificación de paquetes de servicio de QoS modular describe la herencia de la política. Cuando se aplica un policy map en un puerto físico, la política se aplica para todas las subinterfaces de Capa 2 y Capa 3 bajo ese puerto físico.

Este es el comportamiento de marcado predeterminado en ASR 9000:

Cuando las etiquetas VLAN o las etiquetas MPLS se agregan en una interfaz de ingreso o egreso, el valor predeterminado para CoS y EXP se traslada a esas etiquetas y etiquetas. El valor predeterminado se puede sobrescribir en función del mapa de política. El valor predeterminado para CoS y EXP se basa en un campo de confianza en el paquete al ingresar al sistema. El router implementa una confianza implícita de ciertos campos basada en el tipo de paquete y el tipo de

reenvío de interfaz de ingreso (Capa 2 o Capa 3).

De forma predeterminada, el router no modifica la precedencia IP o DSCP sin que se configure un policy-map.

Éste es el comportamiento predeterminado del router:

- En una interfaz de ingreso o egreso de Capa 2, como xconnect o bridge-domain, el valor CoS más externo se utiliza para cualquier campo que se agregue en la interfaz de ingreso. Si hay una etiqueta VLAN que se agrega debido a una reescritura de Capa 2, el valor de CoS externo entrante se utiliza para la nueva etiqueta VLAN. Si se agrega una etiqueta MPLS, el valor CoS se utiliza para los bits EXP en la etiqueta MPLS.
- En una interfaz de capa 3 de entrada o salida (enrutada o con etiqueta ponderada para paquetes IPv4 o IPv6), los tres bits de precedencia y DSCP se identifican en el paquete entrante. Para los paquetes MPLS, se identifica la etiqueta más externa del bit EXP y este valor se utiliza para cualquier campo nuevo que se agregue en la interfaz de ingreso. Si se agrega una etiqueta MPLS, se utiliza el valor de precedencia, DSCP o MPLS EXP identificado para los bits EXP en la etiqueta MPLS recién agregada.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).