Dépannage de la valeur DSCP dans les modifications QOS dans ASR9000

Table des matières

Introduction

Ce document décrit comment dépanner l'héritage de la politique de qualité de service (QOS) dans le routeur Cisco Aggregation Services Router (ASR) 9000. Il indique le comportement du routeur lorsqu'il y a un marquage DSCP (Differentiated Services Code Point) dans une configuration de stratégie d'entrée d'un port physique. Cette politique est appliquée à toutes les sous-interfaces de couche 2 et de couche 3 sous ce port physique.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de réseau privé virtuel (L2VPN) et de service Ethernet de couche 2 dans ASR9000

Guide de configuration des services L2VPN et Ethernet des routeurs à services d'agrégation de la gamme Cisco ASR 9000

- Configuration de la qualité de service dans ASR9000

Guide de configuration de la qualité de service modulaire des routeurs à services d'agrégation Cisco ASR 9000

Composants utilisés

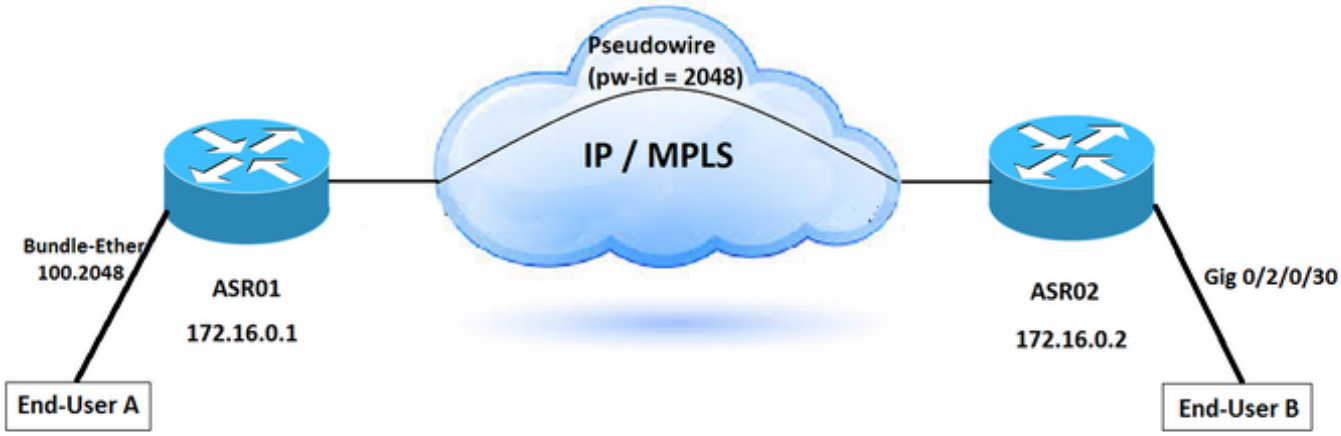
Les informations contenues dans ce document sont basées sur la gamme Cisco ASR9000.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problème : la valeur DSCP dans la QoS change dans une direction

Les paquets sont notés dans une direction. Il affiche la nouvelle valeur DSCP (Differentiated Services Code Point) dans QOS lorsqu'il passe par une connectivité point à point de couche 2 (L2) sur Cisco ASR 9000. La connectivité L2 est configurée via des pseudo-fils, qui sont implémentés sur le réseau MPLS. Aucune configuration spécifique ne permet de modifier la valeur DSCP pour les sous-interfaces associées impliquées dans ce scénario. Les paquets d'origine sont envoyés à partir de l'utilisateur A, qui est marqué comme CS4, une valeur DSCP. Cependant, les paquets reçus par l'utilisateur B affichent la valeur DSCP définie comme AF41. Cette question est vue dans une seule direction, c'est-à-dire de A à B.

Topologie



Dépannage

Considérez le fait que le trafic circule sur la connexion L2VPN, vous devez identifier où la remarque DSCP se produit dans le réseau.

La capture de paquets est l'un des moyens de confirmer où et dans quelle direction la valeur DSCP est modifiée. Dans ce scénario, le trafic est capturé des deux côtés. Vous pouvez voir le problème qui se produit dans une direction d'ASR01 à ASR02. Les valeurs DSCP changent dès qu'elles atteignent ASR02. La capture de paquets confirme que les valeurs DSCP sont modifiées après avoir quitté le routeur ASR01.

Selon le guide de configuration de la qualité de service modulaire des routeurs à services

d'agrégation de la gamme Cisco ASR 9000, plusieurs méthodes sont exécutées pour l'identification du flux de trafic au sein d'un seul routeur, telles que les listes de contrôle d'accès (ACL), la correspondance de protocole, la priorité IP, le DSCP, le champ EXP (Multiprotocol Label Switching) dans les paquets IP, ou la classe de service (CoS).

Afin de marquer le trafic, définissez la priorité IP ou les bits DSCP dans l'octet IP Type of Service (ToS).

Vérification de la configuration

Afin de trouver la cause première, vous pouvez vérifier la configuration.

Étape 1. Vérifiez la configuration de 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
```

Étape 2. Vérifiez la configuration des interfaces.

Une politique de service d'entrée est configurée dans l'interface d'ensemble 100, qui est connectée aux utilisateurs finaux et transporte plusieurs trafics pour différents services L2VPN. Afin de différencier le trafic, configurez des sous-interfaces et utilisez un VLAN unique pour chaque type de trafic.

```
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
!
```

Étape 3. Vérifiez la configuration de la stratégie de service.

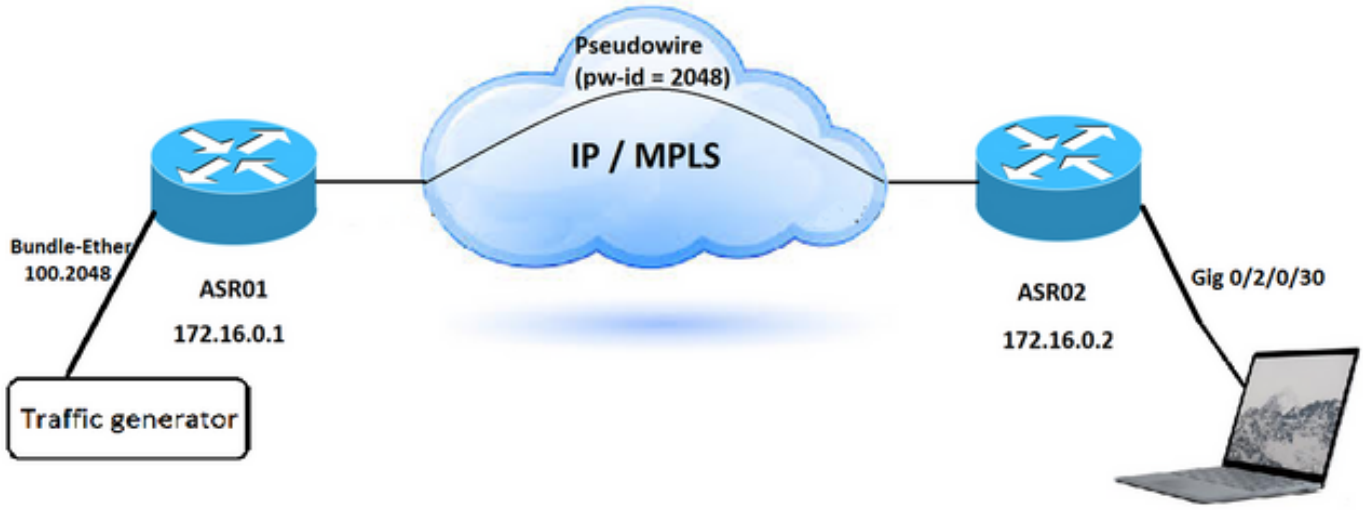
La configuration indique qu'il existe une carte de stratégie pour le trafic vidéo qui correspond au paquet marqué CS4 et le remarque à AF41.

En outre, cette stratégie est configurée pour un autre service L2VPN avec une étiquette VLAN différente. Cependant, il s'applique à l'interface du bundle principal qui affecte tout le trafic entrant remplissant cette condition.

```
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
```

Recréer le scénario de test dans les travaux pratiques

Vous pouvez recréer le même scénario dans les travaux pratiques et vérifier comment cette configuration de stratégie de service affecte les valeurs DSCP du trafic entrant.



Étape 1. Configurez le même scénario sans aucune stratégie de service et capturez le paquet dans la destination.

La valeur DSCP est définie sur CS4 pour le trafic entrant et elle reste identique à la destination.

```
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
```

Étape 2. Appliquez la même politique de service à la direction d'entrée de l'interface connectée au générateur de trafic.

Étape 3. Générez deux types de trafic. L'une avec la valeur DSCP définie sur CS4 et la seconde avec toute autre valeur DSCP.

Le paquet capturé après ASR02 indique :

Lorsque la valeur DSCP du trafic entrant est définie sur CS4, le paquet reçu à destination affiche la valeur DSCP AF41. Cependant, si vous définissez une autre valeur DSCP, qui ne correspond pas aux critères de la stratégie de service, la valeur DSCP du paquet reste la même lorsqu'il arrive à destination.

```
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
```

Solution

La stratégie de service d'entrée configurée au niveau de l'interface de l'ensemble (ensemble 100) dans le périphérique ASR01 réécrit les valeurs DSCP pour les paquets qui correspondent à ses critères. Il recherche la valeur CS4 et la remarque avec AF41. Par conséquent, vous devez supprimer la stratégie de service d'entrée pour résoudre ce problème.

Le document Configuring Modular QoS Service Packet Classification décrit l'héritage de la stratégie. Lorsqu'une carte de stratégie est appliquée à un port physique, la stratégie est appliquée à toutes les sous-interfaces de couche 2 et de couche 3 sous ce port physique.

Voici le comportement de marquage par défaut dans ASR 9000 :

Lorsque les étiquettes VLAN ou MPLS sont ajoutées dans une interface d'entrée ou de sortie, la valeur par défaut pour la CoS et l'EXP passe à ces étiquettes. La valeur par défaut peut ensuite être remplacée en fonction de la carte de stratégie. La valeur par défaut pour CoS et EXP est basée sur un champ de confiance dans le paquet lors de l'entrée dans le système. Le routeur met

en oeuvre une approbation implicite de certains champs en fonction du type de paquet et du type de transfert d’interface d’entrée (couche 2 ou couche 3).

Par défaut, le routeur ne modifie pas la priorité IP ou le DSCP sans qu'une carte de stratégie soit configurée.

Il s’agit du comportement par défaut du routeur :

- Sur une interface d'entrée ou de sortie de couche 2, telle que xconnect ou bridge-domain, la valeur de CoS la plus externe est utilisée pour tout champ ajouté dans l'interface d'entrée. Si une étiquette VLAN est ajoutée en raison d'une réécriture de couche 2, la valeur CoS la plus externe entrante est utilisée pour la nouvelle étiquette VLAN. Si une étiquette MPLS est ajoutée, la valeur CoS est utilisée pour les bits EXP dans la balise MPLS.
- Sur une interface de couche 3 d'entrée ou de sortie (routée ou étiquetée pondérée pour les paquets IPv4 ou IPv6), les trois bits DSCP et de priorité sont identifiés dans le paquet entrant. Pour les paquets MPLS, l'étiquette la plus externe du bit EXP est identifiée et cette valeur est utilisée pour tout nouveau champ qui est ajouté à l'interface d'entrée. Si une étiquette MPLS est ajoutée, la priorité identifiée, DSCP ou la valeur EXP MPLS est utilisée pour les bits EXP dans la balise MPLS nouvellement ajoutée.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.