Dépannez la valeur DSCP dans des changements QOS d'ASR9000

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Problème : La valeur DSCP dans QOS change en One Direction](#)
[Topologie](#)
[Dépannez](#)
[Vérifiez la configuration](#)
[Étape 1. Vérifiez la configuration de L2VPN.](#)
[Étape 2. Vérifiez la configuration d'interface.](#)
[Étape 3. Vérifiez la configuration de politique de service.](#)
[Recréez le scénario de test dans le LABORATOIRE](#)
[Solution](#)

Introduction

Ce document décrit comment dépanner l'héritage de stratégie de Qualité de service (QoS) dans le routeur de services d'agrégation de Cisco (ASR) 9000. Il indique le comportement de routeur quand il y a marquage de Differentiated Services Code Point (DSCP) en configuration de politique d'entrée d'un port physique. Cette stratégie est imposée pour toutes les sous-interfaces de la couche 2 et de la couche 3 sous ce port physique.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

[L'agrégation de gamme 9000 de Cisco ASR entretient le L2VPN de routeur et le guide de configuration de services Ethernet](#)

- Configuration de qualité de service dans ASR9000

[L'agrégation de gamme 9000 de Cisco ASR entretient le guide de configuration de qualité de service modulaire de routeur](#)

Composants utilisés

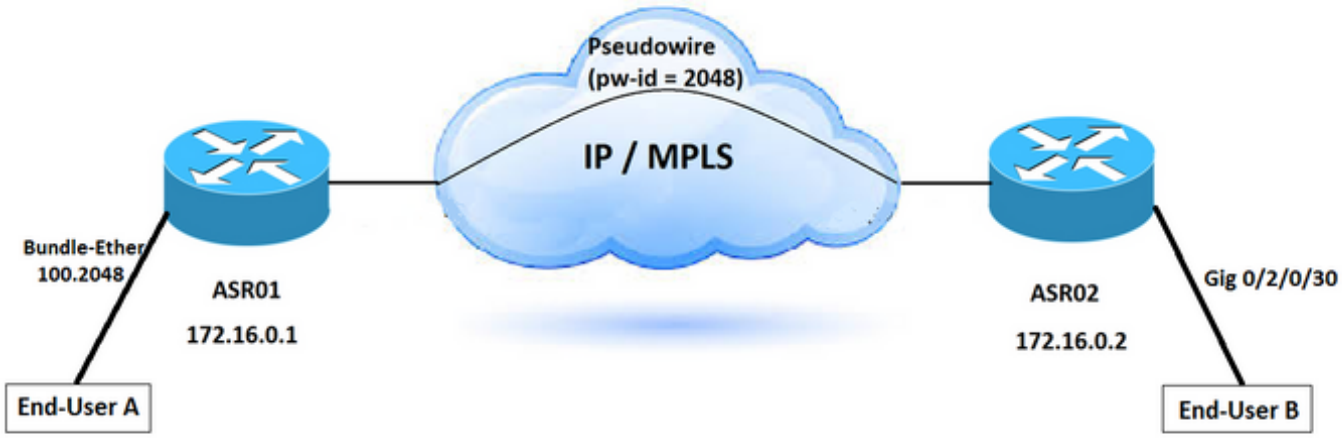
Les informations dans ce document sont basées sur la gamme Cisco ASR9000.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème : La valeur DSCP dans QOS change en One Direction

Des paquets sont remarqués dans une direction. Il affiche la nouvelle valeur de Differentiated Services Code Point (DSCP) dans QOS quand il traverse une Connectivité point par point de la couche 2 (L2) sur le Cisco ASR 9000. La Connectivité L2 est configurée par l'intermédiaire des pseudowires, qui sont mis en application au-dessus du réseau MPLS. Il n'y a aucune configuration spécifique pour changer la valeur DSCP pour des sous-interfaces relatives l'unes des impliquées dans ce scénario. Les paquets d'origine envoient de l'utilisateur A, qui est marqué comme CS4, une valeur DSCP. Cependant, les paquets reçus par l'utilisateur-b affiche la valeur DSCP réglée comme AF41. Cette question est vue dans une direction seulement, cela est d'A à B.

Topologie



Dépannez

Considérez le fait que la circulation au-dessus de la connexion de L2VPN, vous doit identifier où la remarque de DSCP se produit dans le réseau.

La capture de paquet est une de la manière de confirmer où et dans quelle direction la valeur DSCP est changé. Dans ce scénario, le trafic est capturé des deux directions. Vous pouvez voir la question qui se produit dans une direction d'ASR01 à ASR02. Les valeurs DSCP changent dès qu'il atteindra à ASR02. La capture de paquet confirme que les valeurs DSCP sont changées après qu'il congé le routeur ASR01.

Selon le guide de configuration de qualité de service modulaire de routeur de services d'agrégation de gamme 9000 de Cisco ASR, plusieurs méthodes sont exécutées pour

l'identification de la circulation chez un routeur unique, tel que le Listes de contrôle d'accès (ACL), correspondance de protocole, Priorité IP, DSCP, les bits expérimentaux de Commutation multiprotocole par étiquette (MPLS) (EXP) mettent en place dans des paquets IP, ou le Classe de service (Cos).

Afin de marquer le trafic, placez la Priorité IP ou les bits de DSCP dans l'octet de type de service IP (tos).

Vérifiez la configuration

Afin de trouver la cause principale, 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 d'interface.

Il y a une stratégie configurée de service d'entrée dans l'interface 100 de paquet, qui est connectée aux utilisateurs finaux et porte le trafic multiple pour différents services de L2VPN. Afin de différencier le trafic, configurez les sous interfaces et utilisez le seul VLAN 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 politique de service.

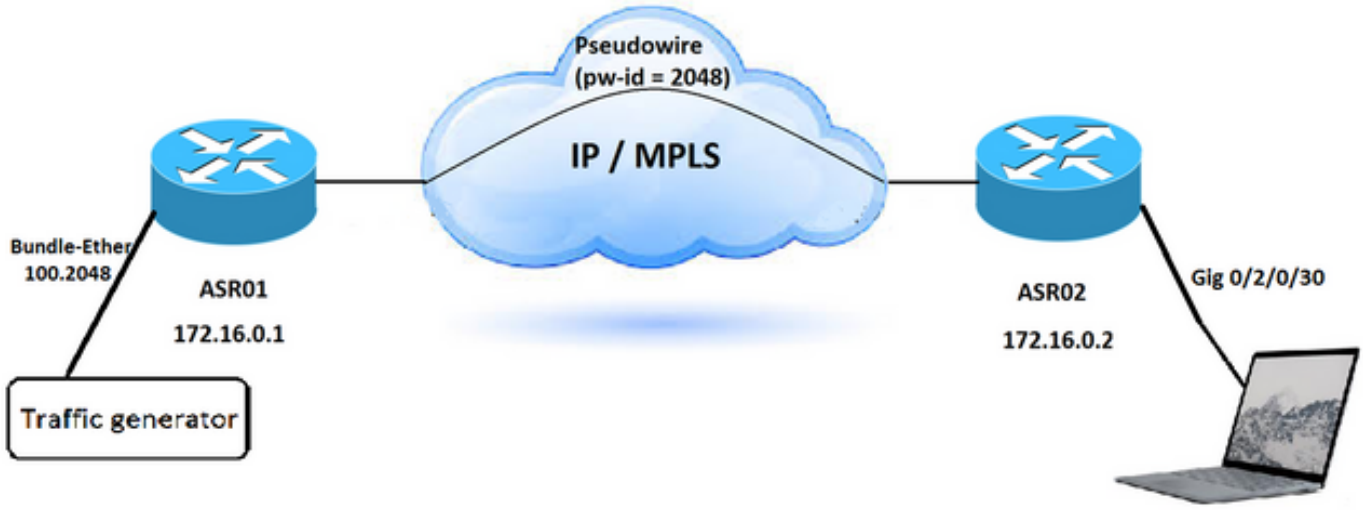
La configuration indique qu'il y a une carte de stratégie pour le trafic visuel qui apparie le paquet marqué comme CS4 et le remarque à AF41.

D'ailleurs, cette stratégie est configurée pour un autre service de L2VPN avec la balise différente VLAN. Cependant, il s'applique sur l'interface principale de paquet 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
```

Recréez le scénario de test dans le LABORATOIRE

Vous pouvez recréer le même scénario dans le LABORATOIRE et vérifier comment cette configuration de politique de service affecte des valeurs DSCP du trafic entrant.



Étape 1. Configurez le scénario semblable sans n'importe quelle stratégie de service et capturez le paquet dans la destination.

La valeur DSCP est placée à CS4 pour le trafic entrant et elle demeure même 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 stratégie de service à la direction d'entrée de l'interface connectée au générateur du trafic.

Étape 3. Générez deux types de trafic. Un avec la valeur DSCP a placé à CS4 et au second avec n'importe quelle autre valeur DSCP.

Le paquet capturé après ASR02 indique :

Quand la valeur DSCP du trafic entrant est placée à CS4, le paquet reçu à la destination affiche la valeur DSCP comme AF41. Cependant, si vous placez n'importe quelle autre valeur DSCP, qui ne fait pas mach les critères de stratégie de service, la valeur DSCP du paquet demeure la même quand elle arrive 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 1000 .... .... .... .... .... = Traffic class: 0x88 (DSCP: AF41, ECN: Not-ECT) <<
============

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

    Payload length: 20
```

Solution

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

Configurer le document modulaire de classification de paquet de service QoS décrit l'héritage de stratégie. Quand une carte de stratégie est appliquée sur un port physique, la stratégie est imposée pour toutes les sous-interfaces de la couche 2 et de la couche 3 sous ce port physique.

C'est le comportement par défaut de marquage dans ASR 9000 :

Quand les balises ou des mpls label VLAN sont ajoutés dans un d'entrée ou une interface de sortie, la valeur par défaut pour le cos et l'EXP se déplace à ceux l'étiquette et des étiquettes. La valeur par défaut peut être alors remplacée basée sur la carte de stratégie. La valeur par défaut pour le cos et l'EXP est basée sur un champ de confiance dans le paquet à l'entrée au système.

Le routeur implémente une confiance implicite de certains champs basés sur le type d'expédition de type de paquet et d'interface d'entrée (couche 2 ou couche 3).

Par défaut, le routeur ne modifie pas la Priorité IP ou le DSCP sans policy-map étant configuré.

C'est le comportement par défaut du routeur :

- Sur un d'entrée ou un interface de couche 2 de sortie, tel que le xconnect ou le bridge-domain, la valeur CoS extérieure est utilisée pour n'importe quel champ qui obtient ajouté dans l'interface d'entrée. S'il y a une balise VLAN qui obtient en raison ajouté d'une réécriture de la couche 2, la valeur CoS extérieure entrante est utilisée pour la nouvelle balise VLAN. Si des mpls label sont ajoutés, la valeur CoS est utilisée pour les bits d'EXP dans la balise MPLS.
- Sur une interface d'entrée ou de couche 3 de sortie (conduite ou étiquette pesée pour des paquets d'ipv4 ou d'IPv6), les trois DSCP et bits de priorité sont identifiés dans le paquet entrant. Pour des paquets MPLS, l'étiquette extérieure du bit d'EXP est identifiée, et cette valeur est utilisée pour n'importe quel nouveau champ qui obtient ajouté à l'interface d'entrée. Si des mpls label sont ajoutés, alors la priorité identifiée, le DSCP, ou la valeur d'EXP MPLS est utilisée pour les bits d'EXP dans la balise nouvellement ajoutée MPLS.