

Troubleshooting de Valor de DSCP em Alterações de QOS no ASR9000

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema: Valor de DSCP em Alterações de QOS em Uma Direção](#)

[Topologia](#)

[Troubleshoot](#)

[Verifique a configuração](#)

[Etapa 1. Verifique a configuração L2VPN.](#)

[Etapa 2. Verifique A Configuração Da Interface.](#)

[Etapa 3. Verifique a configuração da política de serviço.](#)

[Recrie o cenário de teste no LAB](#)

[Solução](#)

Introduction

Este documento descreve como solucionar problemas de herança de política de Qualidade de Serviço (QOS) no Cisco Aggregation Services Router (ASR) 9000. Indica o comportamento do roteador quando há marcação de Ponto de Código de Serviços Diferenciados (DSCP) em uma configuração de política de entrada de uma porta física. Essa política é aplicada para todas as subinterfaces de Camada 2 e Camada 3 sob essa porta física.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de Rede Virtual Privada (L2VPN - Virtual Private Network) de Camada 2 e Serviço Ethernet no ASR9000

[Guia de configuração dos serviços L2VPN e Ethernet do roteador de serviços de agregação Cisco ASR 9000 Series](#)

- Configuração da Qualidade de Serviço no ASR9000

[Guia de configuração da qualidade de serviço modular do roteador de serviços de agregação Cisco ASR 9000 Series](#)

Componentes Utilizados

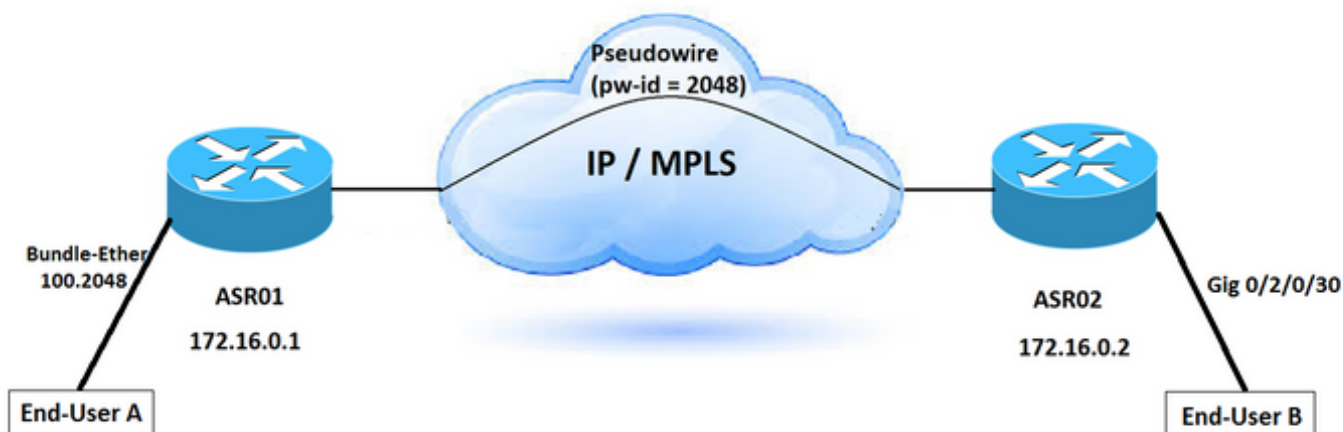
As informações neste documento são baseadas no Cisco ASR9000 Series.

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.

Problema: Valor de DSCP em Alterações de QOS em Uma Direção

Os pacotes são remarcados em uma direção. Ele mostra o novo valor do Differentiated Services Code Point (DSCP) na QOS quando passa por uma conectividade ponto a ponto da camada 2 (L2) no Cisco ASR 9000. A conectividade L2 é configurada através de pseudofios, que são implementados através da rede MPLS. Não há configuração específica para alterar o valor de DSCP para qualquer uma das subinterfaces relacionadas envolvidas neste cenário. Os pacotes originais são enviados do Usuário A, que está marcado como CS4, um valor de DSCP. No entanto, os pacotes recebidos pelo usuário B mostram o valor de DSCP definido como AF41. Esse problema é visto em uma única direção, que é de A para B.

Topologia



Troubleshoot

Considere o fato de que o tráfego flui pela conexão L2VPN, você precisa identificar onde a observação de DSCP ocorre na rede.

A captura de pacotes é uma das formas de confirmar onde e em que direção o valor de DSCP é alterado. Neste cenário, o tráfego é capturado em ambas as direções. Você pode ver o problema que ocorre em uma direção de ASR01 para ASR02. Os valores de DSCP mudam assim que atingem o ASR02. A captura de pacotes confirma que os valores de DSCP são alterados depois que ele sai do roteador ASR01.

De acordo com o [Guia de Configuração da Qualidade de Serviço Modular do Roteador de](#)

[Serviços de Agregação Cisco ASR 9000 Series](#), vários métodos são executados para a identificação do fluxo de tráfego dentro de um único roteador, como listas de controle de acesso (ACLs), correspondência de protocolo, precedência de IP, DSCP, campo de bits experimentais de Multiprotocol Label Switching (MPLS) (EXP) em pacotes IP ou Classe de Serviço (CoS).

Para marcar o tráfego, defina os bits de precedência de IP ou DSCP no byte de ToS (Tipo de serviço) de IP.

Verifique a configuração

Para encontrar a causa raiz, você pode verificar a configuração.

Etapa 1. Verifique a configuração 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
```

Etapa 2. Verifique A Configuração Da Interface.

Há uma política de serviço de entrada configurada na interface de pacote 100, que está conectada aos usuários finais e transporta vários tráfegos para diferentes serviços L2VPN. Para diferenciar o tráfego, configure subinterfaces e use VLAN exclusiva para cada tipo de tráfego.

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
```

!

Etapa 3. Verifique a configuração da política de serviço.

A configuração indica que há um mapa de política para o tráfego de vídeo que corresponde ao pacote marcado como CS4 e o comenta para AF41.

Além disso, essa política é configurada para outro serviço L2VPN com uma marca de VLAN diferente. No entanto, ele se aplica à interface do pacote principal, o que afeta todo o tráfego de entrada que atende a essa condição.

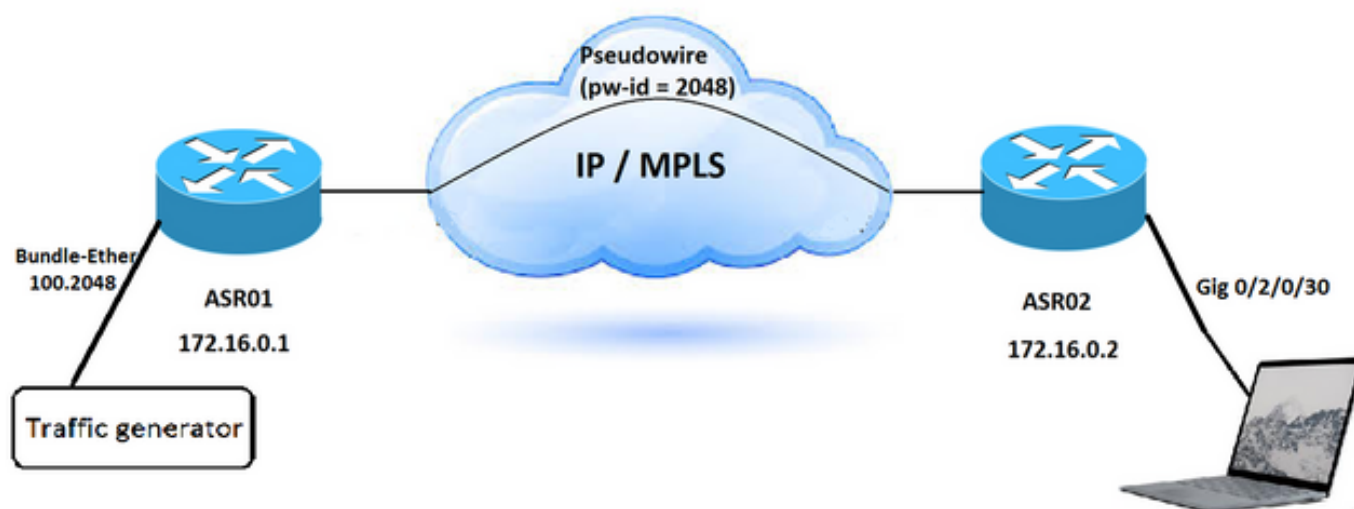
```

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

```

Recrie o cenário de teste no LAB

Você pode recriar o mesmo cenário no LAB e verificar como essa configuração de política de serviço afeta os valores de DSCP do tráfego de entrada.



Etapa 1. Configure o cenário semelhante sem qualquer política de serviço e capture o pacote no destino.

O valor de DSCP é definido como CS4 para tráfego de entrada e permanece o mesmo no 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
```

Etapa 2. Aplique a mesma política de serviço na direção de entrada da interface conectada ao gerador de tráfego.

Etapa 3. Gere dois tipos de tráfego. Um com o valor de DSCP definido como CS4 e o segundo com qualquer outro valor de DSCP.

O pacote capturado após ASR02 indica:

Quando o valor DSCP do tráfego de entrada é definido como CS4, o pacote recebido no destino mostra o valor DSCP como AF41. No entanto, se você definir qualquer outro valor de DSCP, que não corresponda aos critérios da política de serviço, o valor de DSCP do pacote permanecerá o mesmo quando chegar ao 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
```

Solução

A política de serviço de entrada configurada na interface do pacote (pacote 100) no dispositivo ASR01 regrava os valores de DSCP para os pacotes que correspondem a seus critérios. Ele procura o valor CS4 e o observa com AF41. Portanto, você deve remover a política de serviço de entrada para resolver esse problema.

O documento [Configurando a Classificação de Pacote de Serviço de QoS Modular](#) descreve a herança da política. Quando um mapa de política é aplicado em uma porta física, a política é aplicada para todas as subinterfaces de Camada 2 e Camada 3 sob essa porta física.

Este é o comportamento de marcação padrão no ASR 9000:

Quando as marcas de VLAN ou rótulos MPLS são adicionados em uma interface de entrada ou saída, o valor padrão para CoS e EXP se move para essas marcas e rótulos. O valor padrão pode ser substituído com base no mapa de políticas. O valor padrão para CoS e EXP é baseado em um campo confiável no pacote ao entrar no sistema. O roteador implementa uma confiança

implícita de determinados campos com base no tipo de pacote e no tipo de encaminhamento da interface de entrada (Camada 2 ou Camada 3).

Por padrão, o roteador não modifica a precedência do IP ou o DSCP sem que um mapa de políticas seja configurado.

Este é o comportamento padrão do roteador:

- Em uma interface de Camada 2 de entrada ou saída, como xconnect ou domínio de ponte, o valor de CoS mais externo é usado para qualquer campo que seja adicionado à interface de entrada. Se houver uma marca de VLAN que seja adicionada devido a uma regravação da Camada 2, o valor de CoS mais externo de entrada será usado para a nova marca de VLAN. Se um rótulo MPLS for adicionado, o valor de CoS será usado para os bits EXP na marca MPLS.
- Em uma interface de Camada 3 de entrada ou saída (roteada ou com rótulo ponderado para pacotes IPv4 ou IPv6), os três bits de DSCP e precedência são identificados no pacote de entrada. Para pacotes MPLS, o rótulo mais externo do bit EXP é identificado, e esse valor é usado para qualquer novo campo adicionado na interface de entrada. Se um rótulo MPLS for adicionado, o valor de precedência, DSCP ou MPLS EXP identificado será usado para os bits EXP na tag MPLS recém-adicionada.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.