排除ASR9000中QOS更改中的DSCP值故障

目录

简介

本文档介绍如何对思科聚合服务路由器(ASR)9000中的服务质量(QOS)策略继承进行故障排除。它表示在物理端口的入口策略配置中存在差分服务代码点(DSCP)标记时的路由器行为。此策略会为该物理端口下的所有第2层和第3层子接口实施。

先决条件

要求

Cisco 建议您了解以下主题：

- ASR9000中的第2层虚拟专用网络(L2VPN)和以太网服务配置
  Cisco ASR 9000系列聚合服务路由器L2VPN和以太网服务配置指南

- ASR9000中的服务质量配置
  Cisco ASR 9000系列聚合服务路由器模块化服务质量配置指南

使用的组件

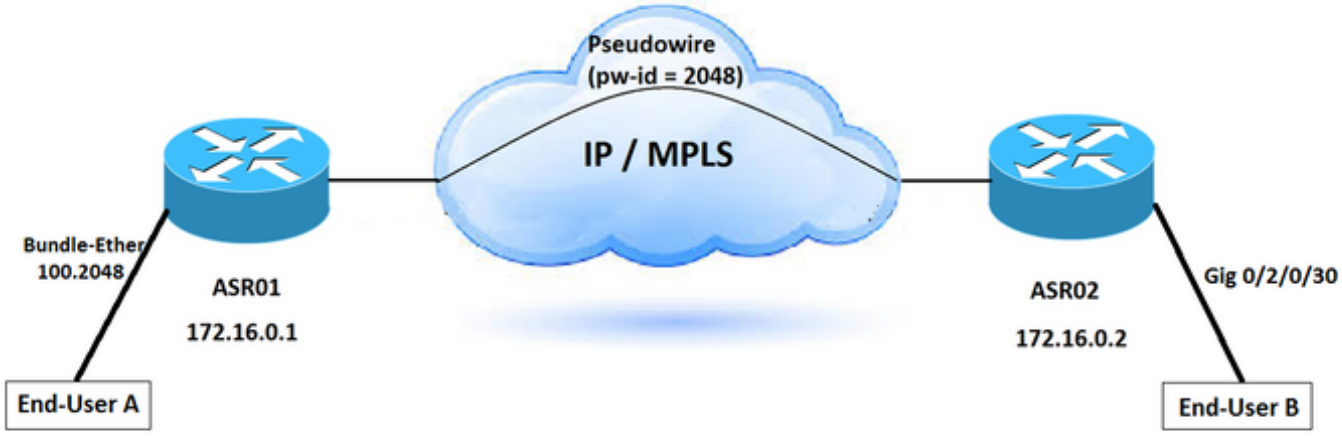
本文档中的信息基于Cisco ASR9000系列。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题：QOS中的DSCP值单向更改

数据包按一个方向重新标记。当它通过Cisco ASR 9000上的点对点第2层(L2)连接时，它显示QOS中的新差分服务代码点(DSCP)值。L2连接通过伪线进行配置，伪线通过MPLS网络实施。 没有特定配置可更改此方案中涉及的任何相关子接口的DSCP值。从用户A发送的原始数据包，标记为CS4，即DSCP值。但是，用户B接收的数据包显示设置为AF41的DSCP值。此问题仅出现在一个方向上，即从A到B。

拓扑



故障排除

考虑流量通过L2VPN连接流动的事实，您需要确定DSCP备注在网络中的位置。

数据包捕获是确认DSCP值更改的位置和方向的一种方法。在此场景中，从两个方向捕获流量。 您可以看到从ASR01到ASR02的一个方向上发生的问题。 DSCP值在到达ASR02时立即更改。数据包捕获确认DSCP值在离开ASR01路由器后已更改。

根据Cisco ASR 9000系列聚合服务路由器模块化服务质量配置指南，有几种方法可用于识别单个路由器内的流量，例如IP数据包中的访问控制列表(ACL)、协议匹配、IP优先级、DSCP、多协议标签交换(MPLS)实验位(EXP)字段或服务类别(CoS)。

要标记流量，请在IP服务类型(ToS)字节中设置IP优先级或DSCP位。

验证配置

为了找到根本原因，您可以检验配置。

步骤1:检验L2VPN配置。

```
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
```

第二步：检验接口配置。

在捆绑接口100中配置有入口服务策略，该入口服务策略连接到终端用户并传输用于不同L2VPN服务的多个流量。为了区分流量，请配置子接口并为每种流量类型使用唯一的VLAN。

```
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
!
```

第三步：验证服务策略配置。

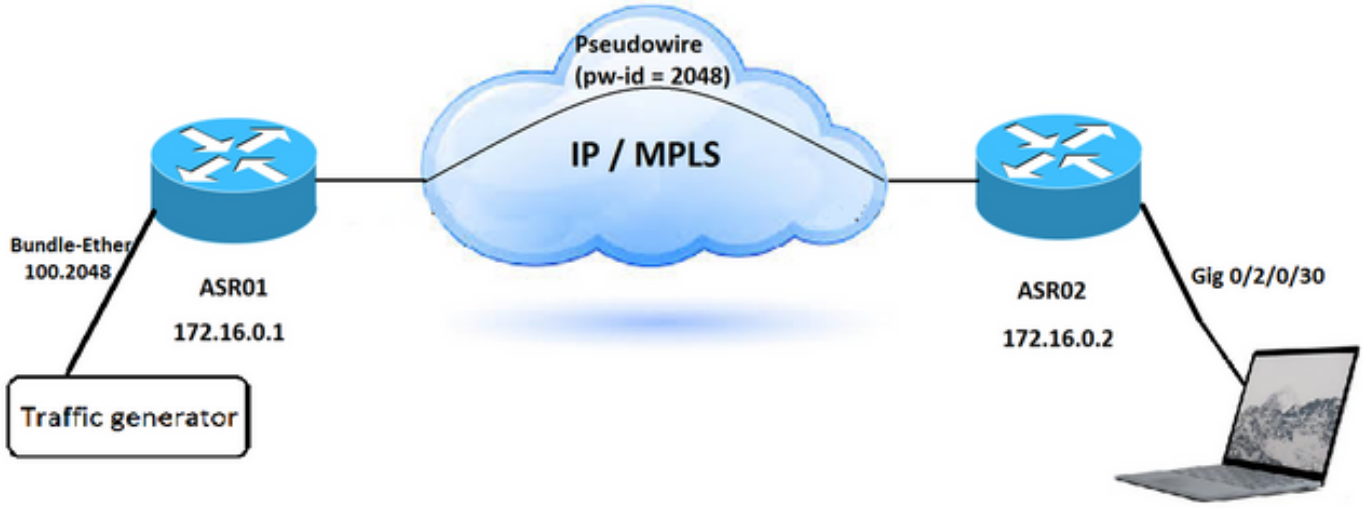
配置表明存在视频流量的策略映射，该映射与标记为CS4的数据包匹配，并将其注释为AF41。

此外，此策略是为具有不同VLAN标记的另一个L2VPN服务配置的。但是，它应用于主捆绑接口，这会影响满足此条件的所有入口流量。

```
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
```

在实验室中重新创建测试场景

您可以在实验室中重新创建相同的场景，并验证此服务策略配置如何影响传入流量的DSCP值。



步骤1:配置无任何服务策略的类似场景，并在目标位置捕获数据包。

传入流量的DSCP值设置为CS4，并且在目标处保持不变。

```
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
```

第二步：在连接到流量生成器的接口的入口方向应用相同的服务策略。

第三步： 生成两种类型的流量。一个将DSCP值设置为CS4，另一个具有任何其他DSCP值。

在ASR02之后捕获的数据包表明：

当传入流量的DSCP值设置为CS4时，在目的地接收的数据包会将DSCP值显示为AF41。但是，如果您设置了任何其他DSCP值，该值不符合服务策略条件，则数据包到达目标时的DSCP值将保持不变。

```
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
```

解决方案

在ASR01设备中的捆绑接口（捆绑包100）上配置的入口服务策略会重新写入与其条件匹配的数据包的DSCP值。它会搜索CS4值并使用AF41对其进行注释。因此，您必须删除入口服务策略才能解决此问题。

配置模块化QoS服务数据包分类文档介绍了策略继承。当策略映射应用于物理端口时，该策略会为该物理端口下的所有第2层和第3层子接口实施。

这是ASR 9000中的默认标记行为：

在入口或出口接口中添加VLAN标记或MPLS标记时，CoS和EXP的默认值将移至这些标记和标记。然后，可以根据策略映射覆盖默认值。CoS和EXP的默认值基于进入系统时数据包中的受信任字段。路由器根据数据包类型和入口接口转发类型（第2层或第3层）对某些字段实施隐式信任。

默认情况下，路由器不修改未配置策略映射的IP优先级或DSCP。

这是路由器的默认行为：

- 在入口或出口第2层接口（例如xconnect或网桥域）上，最外层的CoS值用于添加到入口接口中的任何字段。如果由于第2层重写而添加了VLAN标记，则传入的最外CoS值将用于新的VLAN标记。如果添加了MPLS标签，则CoS值用于MPLS标记中的EXP位。
- 在入口或出口第3层接口（为IPv4或IPv6数据包加权路由或标签）上，三个DSCP和优先级位在传入数据包中标识。对于MPLS数据包，识别EXP位的最外标签，该值用于入口接口处添加的任何新字段。如果添加了MPLS标签，则标识的优先级、DSCP或MPLS EXP值用于新添加的MPLS标记中的EXP位。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。