排除在QOS变化的DSCP值故障在ASR9000上

目录

简介

本文描述如何排除服务质量(QoS)在Cisco聚合服务路由器(ASR) 9000的策略继承故障。当那里差分服务代码点在一个物理端口的入口政策配置时，指示它指示路由器工作情况。此策略为在该物理端口下的所有第2层和第3层子接口被强制执行。

先决条件

要求

Cisco 建议您了解以下主题：

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

- 在ASR9000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

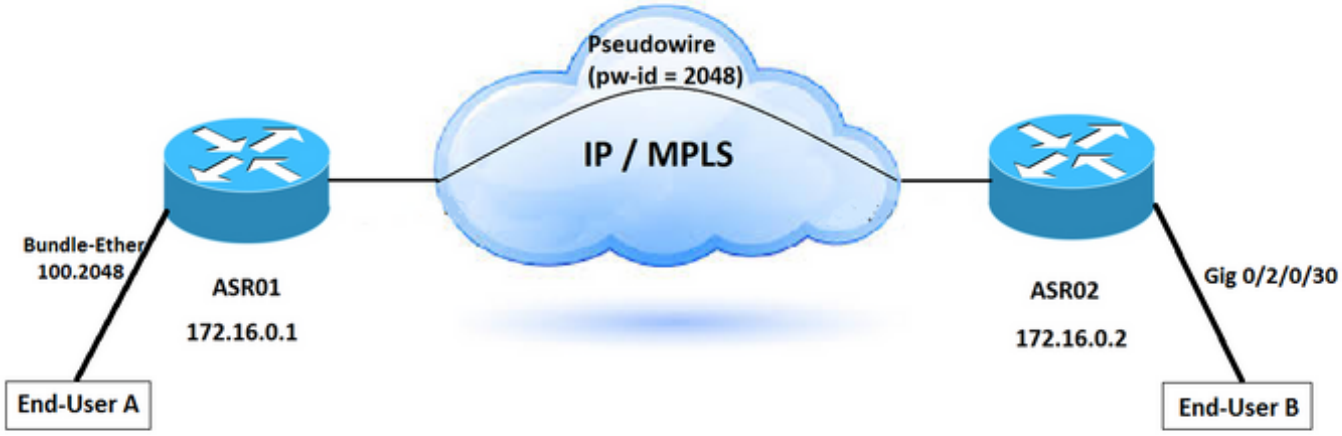
本文的信息根据Cisco ASR9000系列。

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：在QOS变化的DSCP值在一世代上

信息包在一个方向被重新标明。它在QOS显示新的差分服务代码点值，当穿过在Cisco ASR 9000的一点到点第2层(L2)时连接。L2连接通过pseudowires被配置，在MPLS网络是被实施的。 没有更改在此方案涉及的DSCP值的特定配置任何相关子接口。原始信息包从用户A发送，被标记作为CS4，DSCP值。然而，用户B收到的信息包显示作为AF41设置的DSCP值。此问题在仅一个方向被看到，那是从A到B。

拓扑



故障排除

考虑事实在L2VPN连接的通信流，您需要识别DSCP在网络的地方重新标明发生。

信息包获取哪里是一个方式确认，并且在哪个方向DSCP值更改。在此方案中，数据流从两个方向是获取的。 您能看到在一个方向发生从ASR01到ASR02的问题。 当它到达对ASR02， DSCP值更改。信息包获取确认更改DSCP值，在它事假ASR01路由器后。

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，几个方法为通信流的证明在单个路由器内的执行，例如访问控制列表(ACL)、协议匹配、IP优先级、DSCP、多协议标签交换(MPLS)实验位(EXP)字段在IP信息包或者业务类别(CoS)。

为了标记数据流、set ip precedence或者DSCP位在IP服务类型(ToS)字节。

验证配置

为了查找根本原因，您能验证配置。

步骤1.验证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
```

步骤2.验证接口配置。

有在套件接口配置的入口服务策略100，被连接到终端用户并且运载另外L2VPN服务的多个信息数据流。为了区分数据流，请配置子接口并且请使用唯一的VLAN每种流量类型。

```
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
!
```

步骤3.验证服务策略配置。

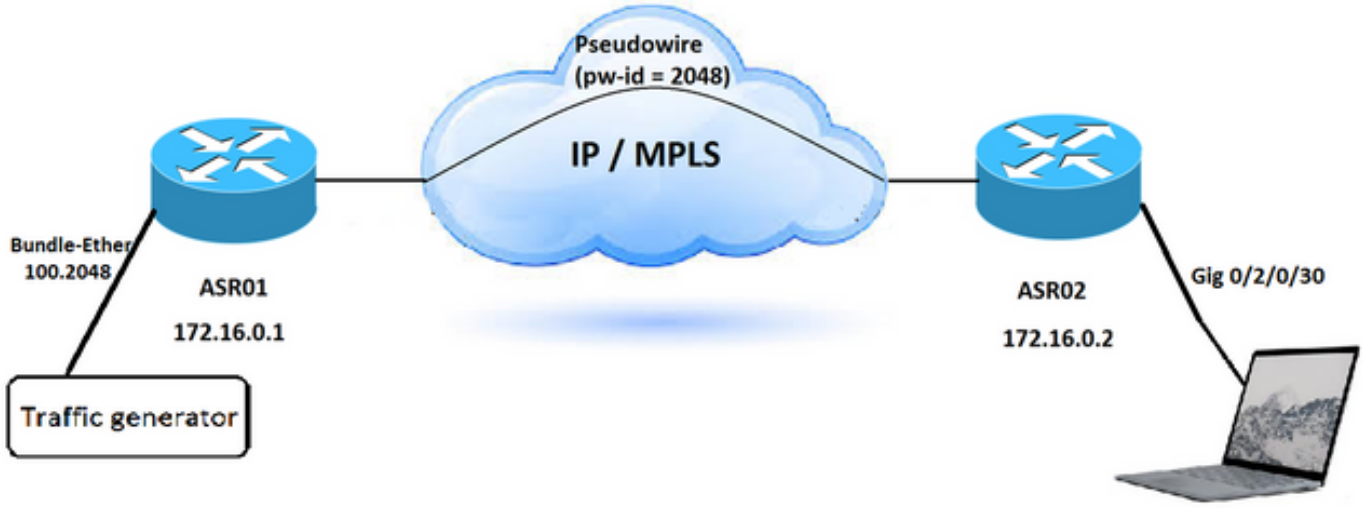
配置表明有匹配作为CS4被标记的信息包并且重新标明它对AF41的视频数据流的一个策略映射。

而且，此策略为另一项L2VPN服务被配置用另外VLAN标记。然而，它在影响符合此情况的所有入口流量的主要套件接口适用。

```
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
```

在实验室里再创测试方案

您能再创同一个方案在实验室里和验证此服务策略配置如何影响流入的数据流的DSCP值。



步骤1.配置相似的方案，不用任何服务策略并且获取在目的地的信息包。

DSCP值设置为流入的数据流的CS4，并且依然是同样在目的地。

```
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
```

步骤2.运用同一个服务策略在接口的入口方向被连接到数据流生成器。

步骤3.生成两种流量类型。一与DSCP值设置到CS4和第二个与其他DSCP值。

在ASR02指示后，信息包捕获：

当流入的数据流的DSCP值设置为CS4时，信息包收到在目的地显示DSCP值作为AF41。然而，如果设置其他DSCP值，不马赫服务策略标准，信息包的DSCP值依然是同样，当到达目的地时。

```
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

入口服务策略被配置在套件接口(请捆绑100)在ASR01设备重写匹配其标准的信息包的DSCP值。它搜索CS4值并且重新标明它与AF41。所以，您必须取消入口服务策略解决此问题。

配置模块化QoS服务信息包分类文件描述策略继承。当策略映射在一个物理端口时被应用，策略为在该物理端口下的所有第2层和第3层子接口被强制执行。

这是在ASR 9000的默认标记工作情况：

当VLAN标记时或MPLS标签在入口或输出接口被添加， DEFAULT值Cos和EXP的移动向那些标记和标签。DEFAULT值可以然后重写根据策略映射。DEFAULT值Cos和EXP的根据在信息包的一个委托的字段对系统的入口。路由器实现根据信息包类型和入口接口转发类型的某些字段含蓄信任(第2层或第3)层。

默认情况下，路由器不修改IP优先级或DSCP没有被配置的策略映射。

这是路由器的默认行为：

- 在一个入口或出口第2层接口，例如xconnect或网桥域，最外层的Cos值使用在入口接口添加的所有字段。如果有添加由于第2层重写的VLAN标记，流入最外层的Cos值使用新的VLAN标记。如果MPLS标签被添加， Cos值使用EXP位在MPLS标记。
- 在入口或出口第3层接口(路由或为IPv4或IPv6信息包衡量的标签)，三个DSCP和优先顺序位在流入信息包被识别。对于MPLS信息包， EXP位最外层的标签被识别，并且添加在入口接口的此值使用所有新字段。如果MPLS标签被添加，则被识别的优先次序、DSCP或者MPLS EXP值使用EXP位在新加的MPLS标记。