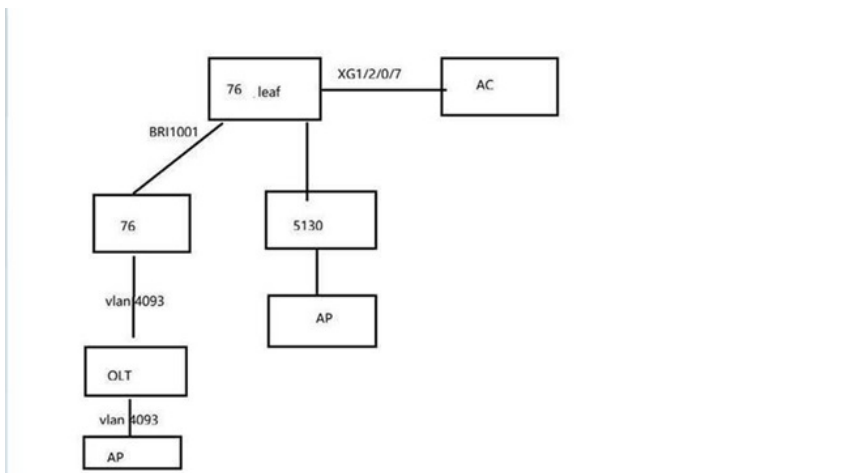


知 S7500E过设备无法传输dhcp报文典型案例分析

DHCP Snooping DHCP/DHCP Relay 李熙 2022-07-27 发表

组网及说明

leaf设备下连76做为汇聚，当前是汇聚76下行的ap无法获取的地址，在汇聚上进行流统（针对mac）统计到报文从7/0/4收到，未从2/0/34发出，设备仅做转发，ap的mac是1019-650a-8160



告警信息

不涉及

问题描述

当前是76下行的ap无法获取的地址，在汇聚上进行流统（针对mac）统计到报文从7/0/4收到，未从2/0/34发出，设备仅做转发，ap的mac是1019-650a-8160

过程分析

1、设备上对mac进行流统，从下行7/0/1收到包，未从2/0/45发出

```
ian-7606]dis qos policy interface Ten-GigabitEthernet 2/0/45
*face: Ten-GigabitEthernet2/0/45
*action: Outbound
*policy: yjc-lt
*classifier: yjc-lt
*operator: AND
*rule(s) :
  If-match source-mac 1019-650a-8160
  If-match acl 3599
  Behavior: yjc-lt
  Accounting enable:
    0 (Packets)
    0 (pps)

ian-7606]dis qos po
ian-7606]dis qos policy in
ian-7606]dis qos policy interface g
ian-7606]dis qos policy interface GigabitEthernet 7/0/1
*face: GigabitEthernet7/0/1
*action: Inbound
*policy: yjc-lt
*classifier: yjc-lt
*operator: AND
*rule(s) :
  If-match source-mac 1019-650a-8160
  If-match acl 3599
  Behavior: yjc-lt
  Accounting enable:
    26 (Packets)
    0 (pps)

ian-7606]█
```

2、2/0/45口收到很多DHCP报文并上送CPU处理丢包，并且在2/0/45口丢弃了，对应都是其他终端的discover报文，leaf设备做relay，其他的discover报文不应该广播到这台汇聚的。

%Jul 19 05:05:59:216 2022 Gexian-7606 DRVPLAT/4/SOFTCAR DROP: -Slot=2;

PktType= DHCP_SERVER , srcMAC=d468-ba06-63f7, Drop From Interface=Ten-GigabitEthernet2/0/45 at Stage=0, StageCnt=1063, TotalCnt=2991

%Jul 19 06:06:24:724 2022 Gexian-7606 DRVPLAT/4/SOFTCAR DROP: -Slot=2;

PktType= DHCP_SERVER , srcMAC=f0c2-4c28-9903, Drop From Interface=Ten-GigabitEthernet2/0/45 at Stage=63, StageCnt=6078, TotalCnt=9069

%Jul 19 06:37:33:030 2022 Gexian-7606 DRVPLAT/4/SOFTCAR DROP: -Slot=2;

PktType= DHCP_SERVER , Drop at Stage=0, StageCnt=408, TotalCnt=408, Max Rate Interface=Ten-GigabitEthernet2/0/45

%Jul 19 06:47:43:018 2022 Gexian-7606 DRVPLAT/4/SOFTCAR DROP: -Slot=2;

PktType= DHCP_SERVER , Drop at Stage=0, StageCnt=3332, TotalCnt=3740, Max Rate Interface=Ten-GigabitEthernet2/0/45

%Jul 19 06:57:52:923 2022 Gexian-7606 DRVPLAT/4/SOFTCAR DROP: -Slot=2;

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	BOOTP	64	[Malformed Packet]

<

> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface unknown, id 0

> Ethernet II, Src: Shenzhen_06:30:95 (d4:68:ba:06:30:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3016

> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

> User Datagram Protocol, Src Port: 68, Dst Port: 67

> [Malformed Packet: DHCP/BOOTP]

3、现网修改配置（删除trust以及vlan mapping配置）后恢复，g2/0/34端口本来是连AP的，不能配置dhcp snooping trust。

配置指导有如下描述:配置vlan mapping的端口应该是面向dhcp client的，同一个端口不应该同时配置trust与vlan mapping。

VLAN映射：发送给用户的报文通过查找指定VLAN对应的DHCP Snooping表项中的DHCP客户端IP地址、MAC地址和原始VLAN的信息，将报文的指定VLAN修改为原始VLAN。

但设备上g2/0/34端口既配置了trust,又配置了vlan映射。

```
interface GigabitEthernet2/0/34
port link-mode bridge
description GD-OLT1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 to 11 31 51 54 to 57 106 to 111 309 400 to 401 681 to 682 684 to 687 794
port trunk permit vlan 800 to 801 976 995 1521 2000 to 2019 2021 to 2489 2491 to 2510 2512 to 253
1 2533 to 2549 2551 to 2554
port trunk permit vlan 2556 to 2576 2578 to 2585 2587 to 2600 2602 2604 to 2609 2611 to 2618 262
0 to 2628 2631 2633 to 2634 2636 to 2639
port trunk permit vlan 2641 to 2650 2653 to 2657 2659 to 2663 2665 to 2666 2671 to 2674 2676 to 2
700 2704 to 2772 2774 to 2992 2994 3013 to 3017
```

解决方法 k permit vlan 3019 3021 3023 3201 3210 3500 to 3505 3510 to 3513 3517 3702 3704 to 370

现网修改配置（删除trust以及vlan mapping配置）后恢复，g2/0/34端口本来是连AP的，不能配置dhcp snooping trust，同时再去往dhcp服务器的端口上配置dhcp snooping trust，避免discover报文转发到不必要的设备上。

vlan mapping 4057 translated-vlan 4093

dhcp snooping trust

这导致dhcp discover在设备上软转发时，会误将报文的vlan 4093修改成 vlan 4057，引起后面dhcp discover报文不能从另一个dhcp trust端口转发出去（BR1未放通vlan 4057）。

另外，应该在设备上往dhcp服务器的端口上配置trust,避免引起dhcp discover报文转发到不必要的设备上，请检查下leaf上的配置。

