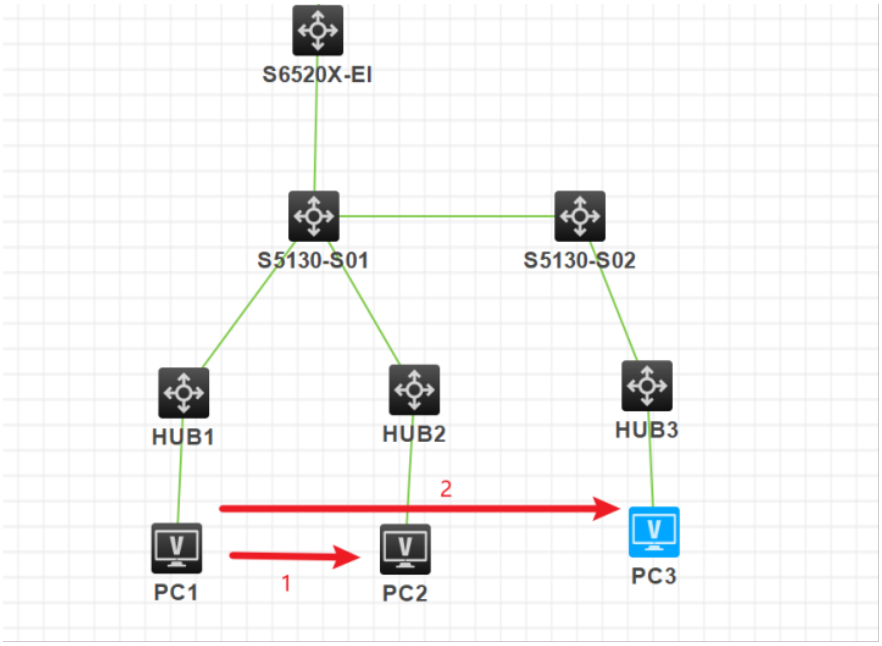
S5130S上使用dhcp snooping + arp detection后终端迁移异常

DHCP Snooping　余发宇　2022-09-06 发表

组网及说明

简易拓扑结构



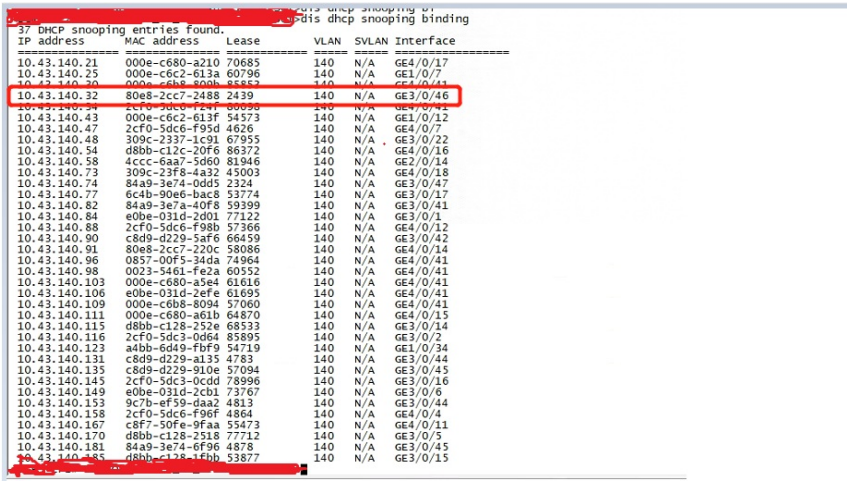
问题描述

这边现场S5130S是使用dhcp snooping + arp detection的场景；

原来终端接在10.43.252.4接入交换机下，交换机有 dhcp snooping表项和dis ip source binding 表项；

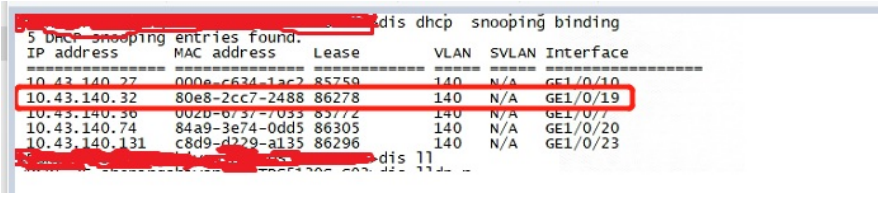
当在 10.43.252.4下串接一台新的接入交换机 10.43.252.240，终端改接到 252.240交换机上，此时 10.43.252.4和 10.43.252.240都有该终端的 dhcp snooping表项，但是此时该终端能获取到IP地址，但是无法ping通网关，只能在 10.43.252.4上reset掉关于该终端的 dhcp snooping表项后，终端才能正常通讯。

1、 现场两个设备上都可以查到dhcp snooping 表项



```
[redacted]dis dhcp snooping binding
37 DHCP snooping entries found.
IP address      MAC address    Lease         VLAN  SVLAN Interface
--------------- -------------- ------------- ----- ----- ----------------
10.43.140.21    000e-c680-a210 70685         140   N/A   GE4/0/17
10.43.140.25    000e-c6c2-613a 60796         140   N/A   GE1/0/7
10.43.140.30    000e-c6b8-809b 85852         140   N/A   GE4/0/41
10.43.140.32    80e8-2cc7-2488 2439          140   N/A   GE3/0/46
10.43.140.34    2cf0-5dc6-f24f 60098         140   N/A   GE1/0/12
10.43.140.43    000e-c6c2-613f 54573         140   N/A   GE1/0/12
10.43.140.47    2cf0-5dc6-f95d 4626          140   N/A   GE4/0/7
10.43.140.48    309c-2337-1c91 67955         140   N/A   GE3/0/22
10.43.140.54    d8bb-c12c-20f6 86372         140   N/A   GE4/0/16
10.43.140.58    4ccc-6aa7-5d60 81946         140   N/A   GE2/0/14
10.43.140.73    309c-23f8-4a32 45003         140   N/A   GE4/0/18
10.43.140.74    84a9-3e74-0dd5 2324          140   N/A   GE3/0/47
10.43.140.77    6c4b-90e6-bac8 53774         140   N/A   GE3/0/17
10.43.140.82    84a9-3e7a-40f8 59399         140   N/A   GE3/0/41
10.43.140.84    e0be-031d-2d01 77122         140   N/A   GE3/0/1
10.43.140.88    2cf0-5dc6-f98b 57366         140   N/A   GE4/0/12
10.43.140.90    c8d9-d229-5af6 66459         140   N/A   GE3/0/42
10.43.140.91    80e8-2cc7-220c 58086         140   N/A   GE4/0/14
10.43.140.96    0857-00f5-34da 74964         140   N/A   GE4/0/41
10.43.140.98    0023-5461-fe2a 60552         140   N/A   GE4/0/41
10.43.140.103   000e-c680-a5e4 61616         140   N/A   GE4/0/41
10.43.140.106   e0be-031d-2efe 61695         140   N/A   GE4/0/41
10.43.140.109   000e-c6b8-8094 57060         140   N/A   GE4/0/41
10.43.140.111   000e-c680-a61b 64870         140   N/A   GE4/0/15
10.43.140.115   d8bb-c128-252e 68533         140   N/A   GE3/0/14
10.43.140.116   2cf0-5dc3-0d64 85895         140   N/A   GE3/0/2
10.43.140.123   a4bb-6d49-fbf9 54719         140   N/A   GE1/0/34
10.43.140.131   c8d9-d229-a135 4783          140   N/A   GE3/0/44
10.43.140.135   c8d9-d229-910e 57094         140   N/A   GE3/0/45
10.43.140.145   2cf0-5dc3-0cdd 78996         140   N/A   GE3/0/16
10.43.140.149   e0be-031d-2cb1 73767         140   N/A   GE3/0/6
10.43.140.153   9c7b-ef59-daa2 4813          140   N/A   GE3/0/44
10.43.140.158   2cf0-5dc6-f96f 4864          140   N/A   GE4/0/4
10.43.140.167   c8f7-50fe-9faa 55473         140   N/A   GE4/0/11
10.43.140.170   d8bb-c128-2518 77712         140   N/A   GE3/0/5
10.43.140.181   84a9-3e74-6f96 4878          140   N/A   GE3/0/45
10.43.140.185   d8bb-c128-1fbb 53877         140   N/A   GE3/0/15
[redacted]
```

1.2、下连交换机的表项



```
[redacted]dis dhcp  snooping binding
5 DHCP snooping entries found.
IP address      MAC address    Lease         VLAN  SVLAN Interface
--------------- -------------- ------------- ----- ----- ----------------
10.43.140.27    000e-c634-1ac2 85759         140   N/A   GE1/0/10
10.43.140.32    80e8-2cc7-2488 86278         140   N/A   GE1/0/19
10.43.140.36    002b-6737-7033 85772         140   N/A   GE1/0/7
10.43.140.74    84a9-3e74-0dd5 86305         140   N/A   GE1/0/20
10.43.140.131   c8d9-d229-a135 86296         140   N/A   GE1/0/23
[redacted]dis ll
```

过程分析

1. PC迁移后能正常使用，但是每120s就需要重新认证802.1X，影响用户正常使用。

该功能需要终端PC具备自动上报用户名密码等功能，可以在重认证时不需要用户反复提交相关信息进行认证，由于现场PC不具备该能力，所以无法使用。

2．配置运行MAC迁移功能后，PC迁移后无法使用，获取不了IP地址

远程排查发现实际只在S5130-S02设备上开启了port-security mac-move permit，而S01上未开启，所以现场将PC从S01设备上的1/0/25口迁移到1/0/24口上后，查看lldp邻居在1/0/24口上，但是ip source bind表项仍显示在1/0/25口下。

```
<H3C>dis l n l
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
             # -- -- Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID                 System Name             -
GE1/0/20        2cf0-5d49-a092  2cf0-5d49-a092          -
GE1/0/24        84a9-3e75-041a  84a9-3e75-041a          -
GE1/0/24        2cf0-5dc3-0701  2cf0-5dc3-0701          -
GE1/0/24        a44c-c82d-74e0  a44c-c82d-74e0          -

<H3C>dis ip source binding | in 74e0
10.43.207.21    a44c-c82d-74e0 GE1/0/25              207  DHCP snooping
10.43.207.21    a44c-c82d-74e0 GE1/0/25              207  802.1X
```

在S01上开启MAC迁移功能后，终端在SW01上迁移后，可以重新在新端口上上线，原始端口会将该用户立即进行下线处理。此时终端可以正常发送DHCP discovery报文，并更新dhcp snooping表项。

这种方案可以允许如上图组网中在S01上配置1x认证的端口来回迁移，但是如果是从S01迁移到S02则不行，原因是设备迁移至S02后，S01原来的端口没down，感知不到这个mac迁移到了S02，当前无法解决该问题。

解决方法

针对当前现场存在跨设备迁移的情形，建议在S01和S02上增加一台汇聚设备，汇聚设备分别下联S01和S02，将1x认证只集中在汇聚上配置。或者改S01和S02为同型号设备后配置堆叠，这样两台设备虚拟成同一台设备，终端迁移后，两台设备上可以相互感知，正常迁移。