某局点S5560X下挂部分终端无法DHCP中继获取地址问题典型案例

DHCP/DHCP Relay 张文宁 2022-01-16 发表

组网及说明

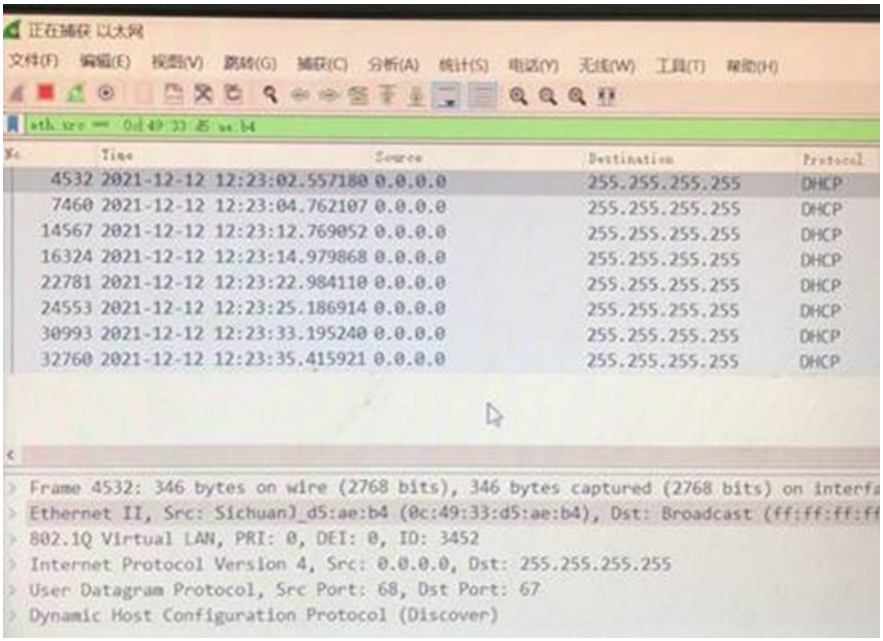
S5560X-Ei作为终端网关和DHCP中继。

问题描述

某日，客户突然发现S5560X-Ei下挂部分终端突然出现无法获取ip地址的故障现象，S5560X-Ei作为终端网关和DHCP中继。

过程分析

从故障现象出发，前方反馈设备agg 3下挂olt设备约几个个终端无法获取到ip地址，于是通过抓包确定交互报文卡在哪个过程，如下可以看到dhcp discover报文进来设备了，但是没有继续往下走流程，怀疑discover报文被设备丢弃了：



设备能学习到这个mac：

[LanHe-HJ-H3C-S5560-1]display mac-address 0c49-33d5-aeb4

MAC Address	VLAN ID	State	Port/Nickname	Aging
0c49-33d5-aeb4	3452	Learned	BAGG3	Y

底层也学习正确：

[LanHe-HJ-H3C-S5560-1-probe]debug l2 slot 1 c 0 mac/find/vid=3452/mac=0c:49:33:d5:ae:b4

find mac 0c:49:33:d5:ae:b4 in vlan 3452
*********unit 0: *********
unit 0: entry found
uiIndex 61056
validPtr 1
skipPtr 0
agedPtr 1
tgid 2,
dstInterface.hwDevNum 0,
isStatic=0 type=(0x00000000):
daCommand=0
saCommand=0
daRoute=0
mirrorToRxAnalyzerPortEn=0
sourceID=1
daQosIndex=0
saQosIndex=0
daSecurityLevel=0
saSecurityLevel=0
appSpecificCpuCode=0
spUnknown=0
saMirrorToRxAnalyzerPortEn=0
daMirrorToRxAnalyzerPortEn=0

entry detail type 0: DRV_MAC_DYNAMIC_HARDWARE_LEARNED | ;

---------- find the mac ----------

解决方法

综上，是g1/0/15口下有个74ff-4cea-6d00这个终端发送了非常大量的dhcp报文上来，触发了设备的攻击保护导致。排除攻击后问题已解决。

但是debug看不到dhcp报文上cpu，并中继出去：

<LanHe-HJ-H3C-S5560-1>debug dhcp relay packet client mac 0c49-33d5-aeb4

关于该攻击防范的底层acl，后续的R63XX和65XX增加了打印日志的功能，当某个端口触发了攻击保护，会打印日志提示。

<LanHe-HJ-H3C-S5560-1>t d

The current terminal is enabled to display debugging logs.

<LanHe-HJ-H3C-S5560-1>t m

The current terminal is enabled to display logs.

因此怀疑报文在二层丢弃了，因此查看计数，确实有丢弃：

[LanHe-HJ-H3C-S5560-1-probe]debug mrvl bridge drop_counter show s 1 chip 0

COUNT_ALL mode count :75

进一步查看底层acl，发现存在攻击命中：

[LanHe-HJ-H3C-S5560-1-probe]debug qacl show acl-resc s 1 c 0

----------Qacl VTcam UsedResc Info----------

Acl Hw Resource: Group 0, VTcamId   0, Client TTI 0

Acl Hw Resource: Group 0, VTcamId   1, Client TTI 1

Acl Hw Resource: Group 1, VTcamId   4, Client IPCL 0

 Pri 2, usedEntries   16, mode Double

 ==========

  acl type   usedEntries[16]

 ==========

  [2]MQC Port   16

 ==========

 Pri 11, usedEntries   1, mode Double

 ==========

  acl type   usedEntries[1]

 ==========

  [17]RX IPv4 High Shadow   1

 ==========

[LanHe-HJ-H3C-S5560-1-probe]debug qacl show slot 1 chip 0 verbose 0 sysidx 34

========

Acl-Type RX IPv4 Middle High, Stage IPCL 2, Global, Installed, Active

Prio Mjr/Sub 0x30b/0xf, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 4/4,

Rule Match --------

    Global range

    Dest IP: 255.255.255.255, 255.255.255.255

    IP protocol: udp

    L4 Dst Port: 67, 0xffff

    IP Fragment: 0x3

Actions --------

    Account mode packets, green and non-green

    Copy_to_cpu : Yes

    Change CPU pkt COS 3

    Red Deny

    Red_Copy_to_cpu : No

    Yel Deny

Yel_Copy_to_cpu : No
MatchedName:34, DHCP_RELAY_SERVER