某局点 S5560X 设备DHCP中继丢包问题

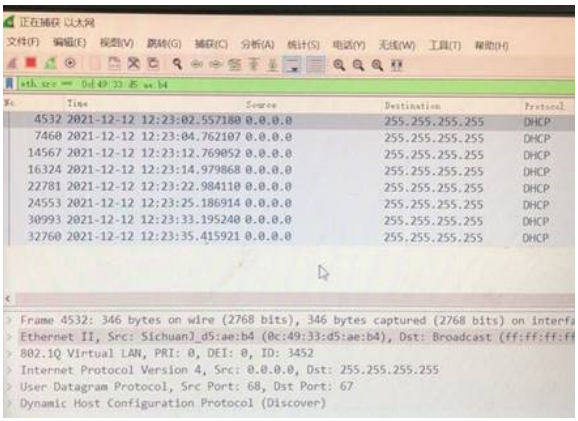
DHCP/DHCP Relay　张文宁　2021-12-14 发表

组网及说明

PC——OLT——S5560X-EI——DHCP server

问题描述

前方反馈S5560X-EI设备agg 3下挂olt设备特定几个终端无法DHCP获取到ip地址，通过抓包可以看到dhcp discover报文进来设备了



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

<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.

设备能学习到这个mac，证明不是二层不通：

[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

过程分析

进一步确认底层mac学习，是正常的：

```
[LanHe-HJ-H3C-S5560-1-probe]debug l2 slot 1 c 0 mac/find/vid=3452/mac=0c:49:33:d
5: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 ----------
```

因此确认报文进来设备了，但怀疑报文在二层环节丢弃了，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
Color Independent 1
Accounting: Hi 0, Lo 94766
========
Acl-Type RX IPv4 High Shadow, Stage IPCL 0, SinglePort, Installed, Active
Prio Mjr/Sub 0x20b/0x28, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 4/23,
Rule Match --------
Port: 14
Dest IP: 255.255.255.255, 255.255.255.255
IP protocol: udp
L4 Dst Port: 67, 0xffff
IP Fragment: 0x3
Actions --------
CAR cir 0x200, cbs 0x800, pir 0x200, pbs 0x800, mode srTCM color blind
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
Color Independent 1
Skip the following PCL lookups
Deny
Accounting: Hi 0, Lo 297
[LanHe-HJ-H3C-S5560-1-probe]

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，底层针对该物理端口下发了shadow类型的过滤acl，排除攻击后问题已解决。

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。

上述ACL代表g1/0/15口一直收到大量的DHCP_RELAY_SERVER超过阈值，为了保护cpu，因此针对该端口下发了过滤（每半分钟检测一次，如果阈值超过2/3阈值，那么就保持丢弃）

==========debug port mapping slot 1==========

[Interface] [Unit] [Port] [Combo?] [Active?] [IfIndex] [MID] [Link]
==========
===
GE1/0/1 0 2 no no 0x1 0 up
GE1/0/2 0 1 no no 0x2 0 up
GE1/0/3 0 5 no no 0x3 0 up
GE1/0/4 0 0 no no 0x4 0 up
GE1/0/5 0 4 no no 0x5 0 down
GE1/0/6 0 3 no no 0x6 0 up
GE1/0/7 0 7 no no 0x7 0 up
GE1/0/8 0 8 no no 0x8 0 up
GE1/0/9 0 6 no no 0x9 0 up
GE1/0/10 0 11 no no 0xa 0 down
GE1/0/11 0 9 no no 0xb 0 up

GE1/0/12	0	10	no	no	0xc	0	up
GE1/0/13	0	15	no	no	0xd	0	down