7609开启DHCP snooping后不更新DHCP binding table

目录

硬件平台

CISCO7609-S

```
1    24   CEF720 24 port 1000mb SFP                WS-X6724-SFP
5     2   Route Switch Processor 720  (Active)     RSP720-3C-GE
6     2   Route Switch Processor 720  (Hot)        RSP720-3C-GE
9    48   48-port 10/100/1000 RJ45  EtherModule    WS-X6148A-GE-TX
```

软件版本

IOS 12.2(33)SRE3

案例介绍

7609开启DHCP snooping和DAI，7609在收到DHCP ACK包后不建立或刷新binding表项，造成DAI告警，终端断网。

问题分析思路

1. 确定DAI告警中的IP/MAC是攻击还是合法的：
   产生DAI告警的原因是ARP报文（请求和回复）中源IP/MAC对不在DHCP binding表中，ARP报文同时被丢弃。客户反映，log中显示的这些IP/MAC对都是合法的，故问题的原因在于，没有binding表项。
2. 确定7609收到相应DHCP ACK报文时是否会更新binding表：
   客户设定的租约时间是30天，在客户的环境中很难看到DHCP binding表项刷新的现象，所以让客户建立一个测试vlan，租约时间为1min。话机连上2960时可以获取IP，同时7609上能够生成binding表项，但是表项age会一直老化到0，持续一段时间后消失，随后出现DAI告警log。过一段时间后，话机会重新获取IP，7609上表项会重新出现。
3. 将7609上DHCP snooping和DAI配置删除，在2960上开启DHCP snooping和snooping debug。在2960上每到租约时间一半，会收到DHCP ACK并更新binding表项。

7609上此时开启DHCP snooping，但不开启DAI，无DHCP binding表项。开启debug，能看到DHCP request但没有ACK，说明7609没有收到ACK或收到没有对其进行处理。
ELAM能够抓到ACK包，说明7609收到了但是没有处理。
让话机重新获取IP，在这个过程中，server回复的ACK目的IP为7609上的网关（DHCP relay ip），7609能够生成binding表项。
话机获取IP后，到达租约时间的一半，会向DHCP server单播request来更新租约，server回复单播ACK。但是7609 DHCP snooping没有处理这类ACK报文。

4. 搭lab重现：
   如下拓扑下，7609作为DHCP relay，能够更新binding表
   ```
   DHCP server  --------- 7609 ------- 2960 ------- IP phone
   ```
   如下拓扑，当7609-2收到的ACK是mpls包，便不会更新binding表。说明问题和MPLS有关。
   ```
   DHCP  server----- 7609-1 ------ MPLS ------- 7609-2 ------- 2960 ------- IP phone
   ```
5. 配置命令mls mpls recir-agg强制带有aggregation lable的包recirculate，问题解决。
   或应用包含 “default-class”的policy-map在7609-2连7609-1的接口上，这类policy-map有side effect disable VPN CAM，同样能够解决问题。

没有应用以上workaround时，netdr抓包结果表明上CPU的包仍然带有MPLS label：

------- dump of incoming inband packet -------

```
interface Gi1/1, routine  process_rx_packet_inline, timestamp 16:57:22.515
dbus info: src_vlan 0x3FD(1021),  src_indx 0x0(0), len 0x15E(350)
  bpdu 0, index_dir 0,  flood 0, dont_lrn 0, dest_indx 0x7E05(32261)     <<<<< index 0x7E05CPU
  08020401 03FD0000  00000001 5E000000 FE000554 0E000040 00000000 7E052000
destmac 00.23.04.0E.E3.40,  srcmac 00.23.04.17.F5.C0, protocol 8847        <<<<< MPLS
layer 3 data: 00065BFE 45000148  00410000 FF1153C2 0A4B3164 14F11602
               00430044 0134BEF5 02010600 C81D8791 00000000 14F11602
               14F11602 00000000 00000064 00000001 000043FD 7AC5
```

应用以上的workaround，vpn-cam空了：

```
PE1-sp#show  mls vpn-cam 0 511
TYCHO  Sindex VPN RAM: Dumping entries 0 -> 511
Key:  * => Set, - => Clear

Index  MPLS Label   VPN    COS
=====+============+======+=====

PE1#show  mls cef mpls labels 100

Codes:  + - Push label, - - Pop Label          * -  Swap Label, E - exp1
Index   Local         Label                    Out i/f
        Label         Op
2151    100 (EOS)     (-)                      recirc   <<<<<<
```

Netdr的抓包结果说明上CPU的包是pure IP了：

------- dump of incoming inband packet -------

```
interface NULL, routine  process_rx_packet_inline, timestamp 17:13:22.651
dbus info: src_vlan 0x3F9(1017),  src_indx 0x0(0), len 0x15A(346)
  bpdu 0, index_dir 0,  flood 0, dont_lrn 0, dest_indx  0x7E05(32261)         <<<<<<
  BD020C01 03F90000  00000001 5A000000 00110544 2E000043 00000000 7E052000
destmac 00.23.04.0E.E3.40,  srcmac 00.00.00.00.00.00, protocol 0800   <<<< IP packet
protocol ip: version 0x04, hlen  0x05, tos 0x00, totlen 328, identifier 94
  df 0, mf 0, fo 0, ttl  254, src 10.75.49.100, dst 20.241.22.2
    udp src 67,  dst 68 len 308 checksum 0xA6E9
```

问题总结

当forwarding engine收到aggregate label，L2 ASIC查找VPN CAM确定vrf #。随后去掉MPLS label，将IP头交L3 ASIC做三层查找。

在L3 ASIC中会进行两个并行的查找：ACL TCAM查找和FIB TCAM查找。ACL TCAM查找返回一个指向CPU的index，FIB TCAM返回的信息是下一跳和rewrite信息。由于ACL TCAM返回结果的优先级更高，所以包不会被rewrite而原封不动的转给CPU做处理，即包含MPLS包头。

Dhcp snooping code并不解mpls包，所以dhcp binding表项不会被更新。

配置mls mpls recir-agg disable VPN CAM从而强制带有aggregation label的包recirculate。或应用了包含“match-any”或“default-class”的policy-map，有一个side effect会disable VPN CAM。这样，由于VPN CAM被disable了，MPLS包会在forwarding engine中进行两次查找。第一次查找后会将MPLS label弹出，并再次进入forwarding engine做第二次查找，查找的结果是redirect to CPU。此时DHCP snooping code便能够识别这个包，成功更新DHCP database。

经验总结

找到表象的内在原因：DAI是由于没有binding表项，则去查没有binding条目的原因。
将问题简化，在7609上仅保留DHCP snooping配置，去掉DAI。

相关命令

- Show ip dhcp snooping
- Show ip dhcp snooping binding
- Debug ip dhcp snooping H.H.H