某局点 S5130S-EI 802.1X认证失败

802.1X ACL 倪民 2021-04-27 发表

组网及说明

不涉及

问题描述

三台交换机做堆叠进行1x认证，做了ead部署，在slot 3上有部分终端认证失败。

过程分析

1、设备上有如下提示信息，说明EAD重定向失败。

Mar 31 00:50:24:282 2013 B1-3F-S DOT1X/3/DOT1X_NOTENOUGH_EADMACREDIR_RES: -Slot=3; Failed to assign a rule for redirecting HTTP packets with source MAC address 2cf0-5dcd-c372 on interface GigabitEthernet3/0/38.

2、查看设备的ACL资源，发现slot3的ACL全部被包过滤使用，没有任何EAD的ACL下发。

```
Interfaces: GE3/0/1 to GE3/0/24, GE3/0/51 to GE3/0/52 (slot 3)
------------------------------------------------------------------------------
Type            Total     Reserved   Configured Remaining  Usage
------------------------------------------------------------------------------
TTI ACL         256       0          1          255        0%
PCL ACL         512       29         483        0          100%
PCL Counter     656       28         0          628        4%
IPCL Meter      768       0          0          768        0%
EPCL Meter      128       0          0          128        0%

Interfaces: GE3/0/25 to GE3/0/50 (slot 3)
------------------------------------------------------------------------------
Type            Total     Reserved   Configured Remaining  Usage
------------------------------------------------------------------------------
TTI ACL         256       0          1          255        0%
PCL ACL         512       25         487        0          100%
PCL Counter     656       25         2          629        4%
IPCL Meter      768       0          0          768        0%
EPCL Meter      128       0          0          128        0%
  ===============debug qacl show acl-resc slot 3 chip 0===============

----------------Qacl VTcam UsedResc Info----------------
Acl Hw Resource: Group  0, VTcamId   0, Client TTI 0
------------------------------------------------------
 Pri  0, usedEntries    1, mode Double
 ========================================
  acl type                 usedEntries[1]
 ========================================
  [336]Zero-Mac-Deny              1
 ====================================
------------------------------------------------------
Acl Hw Resource: Group  0, VTcamId   1, Client TTI 1
------------------------------------------------------
Acl Hw Resource: Group  0, VTcamId   1, Client IPCL 0
------------------------------------------------------
 Pri  6, usedEntries  483, mode Double
 ========================================
  acl type                 usedEntries[483]
 ========================================
  [109]PktFilter IP on PORT       483
```

3、对于EAD部署，设备需要临时下发ACL进行重定向，slot3的ACL全部被使用了导致认证失败。

4、这里需要说明的是，slot3是先配置的包过滤，slot1和slot2是先配置的802.1X，因此slot3没有资源留给802.1X，slot1和slot2其实有部分包过滤下发失败。

5、现场将slot3的部分包过滤删除，发现仍然无法认证。

6、debug dot1x all发现没有触发认证过程，display dot1x statistics发现slot3部分端口收到的EAPOL报文没有增加。

7、在slot3上抓包，能够看到设备收到了EAPOL报文。

8、将上CPU的报文打印，发现没有回显。这时可以判断EAPOL报文没有上送CPU处理，因此不触发认证，statistics计数也没有。

9、对于802.1X认证报文，设备也需要下发如下的ACL，将type为888E的协议报文上送CPU。现场部分端口该ACL没有下发成功。

```
Acl-Type RX IPv4 High, Stage IPCL 0, SinglePort, Installed, Active
Prio Mjr/Sub 0x20b/0x1c, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 1/18,
Rule Match --------
        Port: 0
```

EtherType: 0x888e, 0xffff

Actions --------

Account mode packets，green and non-green

Change CPU pkt COS 1

Permit

Red_Copy_to_cpu : No

Yel_Copy_to_cpu : No

MatchedName:36, DOT1X

Skip the following PCL lookups

Skip the Bridge

Accounting: Hi 0, Lo 7255

解决方法

1、现场最开始配置了大量包过滤，导致设备的ACL全部被占用，EAD和802.1X的保留ACL不能被成功下发。

2、删除了包过滤，仍旧无法认证，是因为802.1X 协议报文上CPU的ACL是在配置时下发的。最开始配置下发失败了，后面需要重新再配一次才能下发。

3、对于S5130这种低端设备，需要注意给设备留有部分ACL，保障基本的协议正常运行。

10、将端口的dot1x undo再配置一次后，发现能够成功认证了。