某局点S5820X下发ACL不生效问题分析案例

ACL 赵国卫 2014-10-27 发表

某局点S5820X下发ACL不生效问题分析案例

一、 **组网：**

无。

二、 问题描述：

现场两台S5820X IRF堆叠，在ACL 3001里配置177条rule，先在VLAN虚接口10上下发成功，但是在VLAN虚接口11上下发的部分ACL不生效。截取其部分配置如下：

display acl 3001

Advanced ACL 3001, named ForISPUplinkCTIn, 177 rules,

"To apply to inbound of ISP vlans for overall access control"

ACL's step is 5

rule 1 permit tcp source 114.80.133.0 0.0.0.127 destination 58.215.43.216 0.0.0.7 destination-port eq 22

rule 10 deny ip destination 58.215.173.54 0

rule 11 deny ip destination 58.215.172.212 0

rule 12 deny ip destination 58.215.177.156 0

rule 14 deny ip destination 58.215.160.176 0

rule 15 deny ip destination 58.215.173.16 0

rule 17 deny ip destination 58.215.160.156 0

rule 18 deny ip destination 58.215.187.107 0

rule 19 deny ip destination 58.215.160.170 0

rule 20 deny ip destination 58.215.172.240 0

rule 21 deny ip destination 58.215.184.49 0

rule 22 deny ip destination 58.215.173.79 0

rule 23 deny ip destination 58.215.185.34 0

rule 24 deny ip destination 58.215.170.69 0 //未生效，还是可以ping通

rule 100 deny ip source 0.0.0.0 0.255.255.255

rule 101 deny ip source 127.0.0.0 0.255.255.255

...

rule 807 permit udp destination 58.215.170.69 0 destination-port gt 1024

rule 833 permit tcp source-port range ftp-data ftp destination 58.215.170.88 0.0.0.1

rule 834 permit tcp source-port range ftp-data ftp destination 58.215.170.90 0.0.0.1

rule 835 permit tcp source-port range ftp-data ftp destination 58.215.170.92 0

rule 1104 permit tcp destination 58.215.170.72 0.0.0.7 destination-port range 10000 20000

客户反馈红色部分ACL应用在VLAN虚接口11时没有生效。

三、 过程分析：

根据客户描述，我们在实验室搭建环境对客户反馈问题进行模拟复现，当在VLAN 10里下发ACL 3001时，下发成功。

通过如下命令查看Slot 1上ACL资源使用情况如下：

[H3C-diagnose]debug qacl show acl-resc 1 0

----------Qacl Group UsedResc Info----------

Acl Hw Resource: VFP

Group 3,usedEntries 5,physlice 0,mode Single

```
  acl type                 usedEntries
-------------------------------------------------------------
  [100]Pdt VFP FirstNh2Classid       5
-------------------------------------------------------------
Acl Hw Resource: EFP
-------------------------------------------------------------
Acl Hw Resource: IFP
-------------------------------------------------------------
 Group  0,usedEntries    8,physlice 10-11,mode Double
-------------------------------------------------------------
 Group  2,usedEntries  126,physlice  9,mode Single
-------------------------------------------------------------
  acl type                 usedEntries
-------------------------------------------------------------
  [108]Policy Based Routing       126
-------------------------------------------------------------
 Group  4,usedEntries   20,physlice  6-7 ,mode Double
-------------------------------------------------------------
  acl type                 usedEntries
-------------------------------------------------------------
  [98 ]PktFilter IPV4 on VRF       20
-------------------------------------------------------------
 Group  6,usedEntries  128,physlice  4-5 ,mode Double
-------------------------------------------------------------
  acl type                 usedEntries
-------------------------------------------------------------
  [98 ]PktFilter IPV4 on VRF       128
-------------------------------------------------------------
 Group  8,usedEntries  128,physlice  2-3 ,mode Double
-------------------------------------------------------------
  acl type                 usedEntries
-------------------------------------------------------------
  [98 ]PktFilter IPV4 on VRF       128
-------------------------------------------------------------
```

可以看出acl占用的是double型的slice 6、slice 7，此时slice 6、slice 7还有128-20=108条可以使用。

接着在VLAN 11同样下发ACL 3001后会发现ACL下发失败，提示资源不足的错误（通过display logbuffer中可以看到）。这是因为ACL 3001前面一部分的rule接着下发到double型的slice 6 7，直到下满为止。剩下的rule要继续下发到single型的slice 8里，一般的rule可以下发进去，但是4层端口号范围的rule需要扩展匹配长度，现网ACL 3001里边有5条匹配4层端口号范围的rule：

rule 807 permit udp destination 58.215.170.69 0 destination-port gt 1024

rule 833 permit tcp source-port range ftp-data ftp destination 58.215.170.88 0.0.0.1

rule 834 permit tcp source-port range ftp-data ftp destination 58.215.170.90 0.0.0.1

rule 835 permit tcp source-port range ftp-data ftp destination 58.215.170.92 0

rule 1104 permit tcp destination 58.215.170.72 0.0.0.7 destination-port range 10000 20000

这5条rule需要被下发到double型的slice，出现下发失败的原因就在于这5条rule被下发到了single型的slice里，由于singe的 slice无法满足匹配4层端口号范围的要求，而设备又没有其他double型的资源可用，所以最终下发失败。

其表现现象就是部分ACL规则不生效。如下查看在VLAN 11同样下发acl 3001后的acl 资源信息：

```
[H3C-diagnose]debug qacl show acl-resc 1 0
----------Qacl Group UsedResc Info----------
Acl Hw Resource: VFP
------------------------------------------------------------
  Group  3,usedEntries    5,physlice  0,mode Single
------------------------------------------------------------
    acl type                  usedEntries
------------------------------------------------------------
    [100]Pdt VFP FirstNh2Classid        5
------------------------------------------------------------
Acl Hw Resource: EFP
------------------------------------------------------------
Acl Hw Resource: IFP
------------------------------------------------------------
  Group  0,usedEntries    8,physlice 10-11,mode Double
------------------------------------------------------------
    acl type                  usedEntries
------------------------------------------------------------
    [22 ]RX Low                     4
    [24 ]Super_RX Low               1
    [60 ]Zero-Mac-Deny              1
    [94 ]DATAPROTECT                2
------------------------------------------------------------                          Group  2,usedEntries  126,physlice  9,mod
e Single
------------------------------------------------------------
    acl type                  usedEntries
------------------------------------------------------------
    [108]Policy Based Routing        126
------------------------------------------------------------
  Group  3,usedEntries   82,physlice  8,mode Single
------------------------------------------------------------
    acl type                  usedEntries
------------------------------------------------------------
    [98 ]PktFilter IPV4 on VRF       82
------------------------------------------------------------
  Group  4,usedEntries  128,physlice  6-7 ,mode Double
------------------------------------------------------------
    acl type                  usedEntries
------------------------------------------------------------
    [98 ]PktFilter IPV4 on VRF       128
------------------------------------------------------------
  Group  6,usedEntries  128,physlice  4-5 ,mode Double
------------------------------------------------------------
    acl type                  usedEntries
------------------------------------------------------------
    [98 ]PktFilter IPV4 on VRF       128
------------------------------------------------------------
```

Group 8,usedEntries 128,physlice 2-3 ,mode Double

---

acl type usedEntries

---

[98]PktFilter IPV4 on VRF 128

四、 解决方法：

ACL问题相对比较复杂，很多问题都需要查看底层ACL的相关信息，底层ACL资源信息可以通过debug qacl show acl-resc 1 0（1为槽位号，0为芯片号）来查看。对于我们本例遇到的情况可以通过下面的方法来解决：

解决方案：基于现有配置可以把5条匹配4层端口号范围的规则排到ACL 3001的前面，然后同时在VLAN 10接口和VLAN 11接口上下发。这样double规则就可以优先在Slice 6、Slice 7上下发成功。