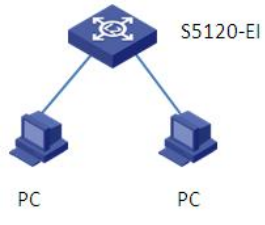
# 某局点S5120-EI设备启用dot1x认证后端口绑定失效问题分析

ACL 802.1X 赵国卫 2013-10-30 发表

## 某局点S5120-EI设备启用dot1x认证后端口绑定失效问题分析

**一、 组网：**




客户组网拓扑示意图如上，S5120-EI作为接入设备直接连接PC。客户最初采用IP+端口绑定来限制用户随意修改IP地址。后来又在接入设备部署了dot1x认证。

**二、 问题描述：**

客户反馈内网H3C交换机S5120-52C-PWR-EI在开启dot1x认证后，IP地址与端口绑定会失效，在没有开启dot1x时候，IP与端口绑定有效。 端口下开启dot1x后，此时， PC更换为非绑定IP照样能ping通外部地址和业务访问，导致IP+端口的绑定限制不起作用。

**三、 过程分析：**

针对客户反馈问题，首先查看端口配置：

#

interface GigabitEthernet1/0/14

port access vlan 517

loopback-detection enable

loopback-detection action shutdown

flow-interval 30

broadcast-suppression 1

stp edged-port enable

dot1x max-user 1

dot1x

arp rate-limit rate 20 drop

arp max-learning-num 1

user-bind ip-address 30.136.28.26

ip check source ip-address

发现端口配置并没有问题。既然端口绑定配置是正确的，这里应该会对IP地址进行检查，只允许30.136.28.26这个IP地址通过此端口访问网络，但为何会不生效呢？考虑问题出现的触发条件是开启dot1x认证，从实现原理出发，开启端口绑定会在设备底层下发ACL，而dot1x认证时往往与下发EAD ACL配合使用，进而怀疑问题产生的原因，可能是ACL动作冲突导致。经过了解，发现客户确实下发了ACL，配置如下：

#

acl number 3000

rule 1 permit ip destination 101.102.1.41 0

rule 2 permit ip destination 102.192.9.41 0

rule 3 permit ip destination 30.102.1.3 0

rule 4 permit ip destination 30.102.1.6 0

rule 5 permit ip destination 30.1.229.24 0

rule 10 deny ip

acl number 3001

rule 7 deny tcp destination-port eq 445

rule 8 deny udp destination-port eq 445

rule 9 deny tcp destination-port eq 539

rule 10 deny udp destination-port eq 539

rule 11 deny tcp destination-port eq 593

rule 12 deny udp destination-port eq 593

rule 19 permit ip

dot1x认证通过后，设备上会下发3001的安全ACL。为了证明我们的怀疑，进一步查看了底层ACL信息，查看底层ACL信息的方法：

en_diag　　//进入诊断模式

debug qacl show 1 0 verbose  0

//1为槽位号，第一个0为芯片号，后面0为序号，序号以30为步长增加，直到没有内容显示为止。

截取部分相关底层ACL信息如下：

Acl-Type PortBind Bind, Stage IFP, GroupPri 11, EntryID 301, Inactive

Health 1, PoolFree 0, PoolID 1, Prio_Mjr 516, Prio_Sub 4,Slice 11,SliceIdx 0

Rule Match --------

Ports: 0x000000001, 0x01fffffff

Source mac: 0011-254E-D869, FFFF-FFFF-FFFF

Outer Vlan: 0x0, 0x0

Source IP: 30.136.28.26, 255.255.255.255

IP Type: Any IPv4 packet

Actions --------

Permit

Red Permit

Yel Permit

==========

Acl-Type EAD AAA-Rule, Stage IFP, GroupPri 12, EntryID 173, Active

Health 1, PoolFree 0, PoolID 2, Prio_Mjr 516, Prio_Sub 11,Slice 12,SliceIdx 6

Rule Match --------

Ports: 0x000000400, 0x01fffffff

Source mac: ECA8-6BC8-2B9B, FFFF-FFFF-FFFF

Outer Vlan: 0x0, 0x0

EtherType: 0x0, 0x0

Source IP: 0.0.0.0, 0.0.0.0

Dest IP: 0.0.0.0, 0.0.0.0

IP protocol: 0x0, 0x0

DSCP-TOS: 0x0, 0x0

IP Type: Any IPv4 packet

L4 Source Port: 0, 0x0

L4 Dst Port: 0, 0x0

Actions --------

Permit

上述两条ACL信息分别代表了端口绑定的底层ACL和EAD  ACL，

端口绑定的ACL优先级低于EAD动态下发的ACL优先级(GroupPri数字越大优先级越高)

，这样导致端口绑定的规则没有生效，因此对IP绑定的限制没有生效，导致了客户的这个问题。

**四、 解决方法：**

通过我们的分析这样在EAD ACL中，由于rule 19这个permit 规则与端口绑定规则的冲突，而EAD的ACL又优先于端口绑定的规则生效从而覆盖了端口绑定的ACL规则，导致端口绑定规则没有生效。

acl number 3001

rule 7 deny tcp destination-port eq 445

rule 8 deny udp destination-port eq 445

rule 9 deny tcp destination-port eq 539

rule 10 deny udp destination-port eq 539

rule 11 deny tcp destination-port eq 593

rule 12 deny udp destination-port eq 593

rule 19 permit ip

解决方法就是删除rule 19这条规则，现场修改配置如下：

acl number 3001

rule 7 deny tcp destination-port eq 445

rule 8 deny udp destination-port eq 445

rule 9 deny tcp destination-port eq 539

rule 10 deny udp destination-port eq 539

rule 11 deny tcp destination-port eq 593

rule 12 deny udp destination-port eq 593

修改配置之后，问题得到解决。这里再补充说明一点，ACL 3001中原来的rule 19其实根本没有必要配置，因为我们设备ACL中报文是缺省允许通过的，不配置rule 19 permit ip，报文直接进行硬件转发不经过ACL模块处理，而配置了这个rule，则报文转发之前先去匹配这个ACL规则，从而导致了ACL冲突。