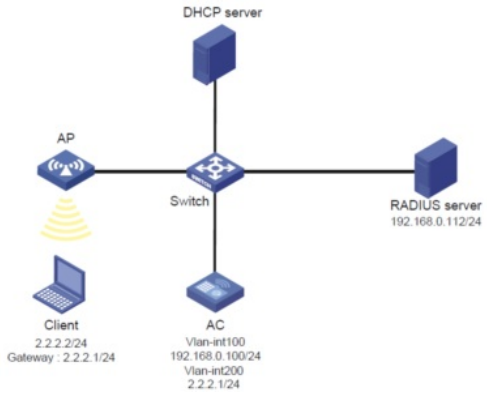
802.1X认证通过iMC下发ACL不生效问题经验案例

ACL　姚超飞　2020-04-01 发表

组网及说明



客户需求：内网特定地址可以被访问，其他地址禁止访问。

问题描述

问题现象: 终端上线后permit的地址无法正常访问。

过程分析

（1）　查看acl是否下发给终端

通过display wlan client verbose 查看acl参数，如红色部分所示，服务器已下发acl到终端。

```
[AC]dis wlan client verbose
Total number of clients: 1

 MAC address                    : [redacted]
 IPv4 address                   : [redacted]
 IPv6 address                   : N/A
 Username                       : [redacted]
 AID                            : 1
 AP ID                          : 1
 AP name                        : [redacted]
 Radio ID                       : 1
 SSID                           : [redacted]
 BSSID                          : 80e4-[redacted]
 VLAN ID                        : 131
 Sleep count                    : 248
 Wireless mode                  : 802.11a
 Supported rates                : 6, 9, 12, 18, 24, 36,
                                  48, 54 Mbps
 QoS mode                       : WMM
 Listen interval                : 250
 RSSI                           : 59
 Rx/Tx rate                     : 54/6 Mbps
 Speed                          : 0.384/3.544Kbps
 Authentication method          : Open system
 Security mode                  : WPA
 AKM mode                       : 802.1X
 Cipher suite                   : TKIP
 User authentication mode       : 802.1X
 WPA3 status                    : Disabled
 Authorization CAR              : N/A
 Authorization ACL ID           : 3003
 Authorization user profile     : N/A
 Roam status                    : N/A
 Key derivation                 : SHA1
 PMF status                     : N/A
 Forwarding policy name         : Not configured
 Online time                    : 0days 0hours 3minutes 2seconds
 FT status                      : Inactive
[AC]
```

2、display acl 3003 并复现问题，查看acl 匹配次数是否增加

```
<AC>dis acl 3003
Advanced IPv4 ACL 3003, 8 rules,
ACL's step is 5
 rule 1 permit ip destination 10.151.6.17 0 (5 times matched)
 rule 10 permit ip destination 10.151.1.230 0 (2 times matched)
 rule 20 permit ip destination 10.151.1.254 0
 rule 30 permit ip destination 10.151.75.254 0 (1 times matched)
 rule 40 permit ip destination 10.151.0.6 0
 rule 50 permit ip destination 10.151.0.21 0
 rule 60 deny ip destination 10.0.0.0 0.255.255.255 (5425 times matched)
 rule 61 permit ip (982 times matched)
```

```
<AC>dis acl 3003
Advanced IPv4 ACL 3003, 8 rules,
ACL's step is 5
 rule 1 permit ip destination 10.151.6.17 0 (6 times matched)
 rule 10 permit ip destination 10.151.1.230 0 (2 times matched)
 rule 20 permit ip destination 10.151.1.254 0
 rule 30 permit ip destination 10.151.75.254 0 (1 times matched)
 rule 40 permit ip destination 10.151.0.6 0
 rule 50 permit ip destination 10.151.0.21 0
 rule 60 deny ip destination 10.0.0.0 0.255.255.255 (5578 times matched)
 rule 61 permit ip (998 times matched)
```

从匹配次数上看，复现问题后acl被击中的次数还是在增加的，说明acl生效了。

2、查看acl配置:

```
[AC]dis acl 3003
Advanced IPv4 ACL 3003, 5 rules,
ACL's step is 5
 rule 1 permit ip destination 10.151.6.17 0 (21 times matched)
 rule 2 permit ip destination 10.151.1.230 0
 rule 5 permit ip destination 10.151.75.254 0
 rule 60 deny ip destination 10.0.0.0 0.255.255.255 (76 times matched)
 rule 61 permit ip (57 times matched)
```

ACL配置放通了目的为10.151.6.17，10.151.1.230，10.151.75.254的地址；deny了该网段的其他地址，直观看着并似乎没有啥问题。

但是，我们分析一下流量走向，ping包路径是有去有回的，acl只放通了目的为10.151.6.17的地址，但是对于计划放通的地址，只放通了该地址作为目的的规则，没有放通该地址作为源的规则，回程的报文不通。所以还需要放通源地址。

解决方法

所有计划permit的地址既要允许作为目的放通，又要允许作为源放通
Rule 10 permit ip destination x.x.x.x 0
Rule 15 permit ip source x.x.x.x 0
……