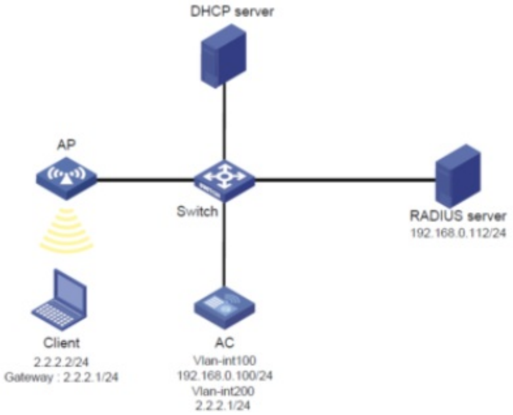
# Sending an ACL through iMC does not take effect

Wireless 孟普 2020-06-05 Published

## Network Topology



Customer requirements: some specific addresses on the Intranet can be accessed, while others are not.

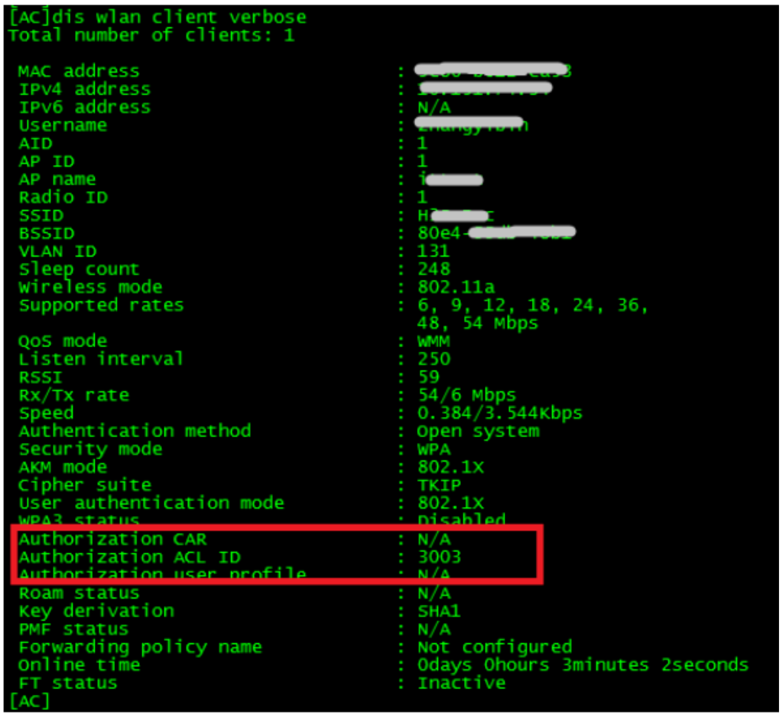
## Problem Description

Problem: Unable to access the permit address after the terminal is online

## Process Analysis

1. Check whether the ACL is issued to the terminal

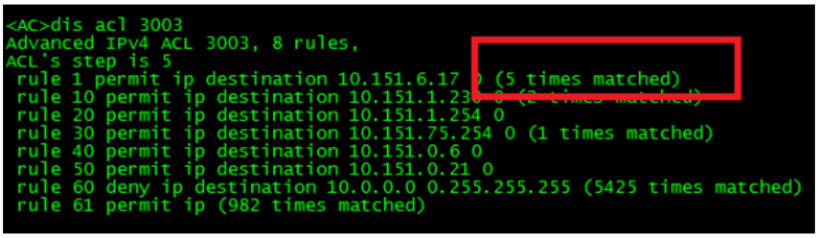
View the ACL parameter through the Display Wlan client verbose, shown in red, where the server has sent the ACL to the terminal.



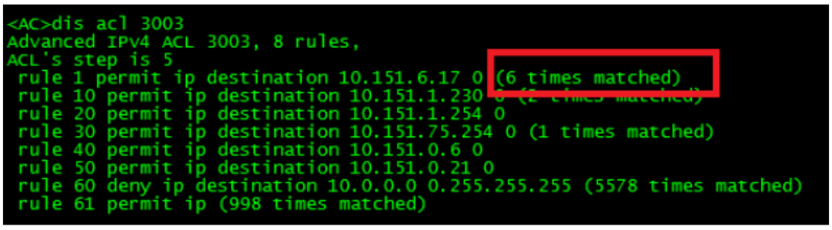
```
[AC]dis wlan client verbose
Total number of clients: 1

 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 and reproduce the problem to see if the number of ACL matches increases



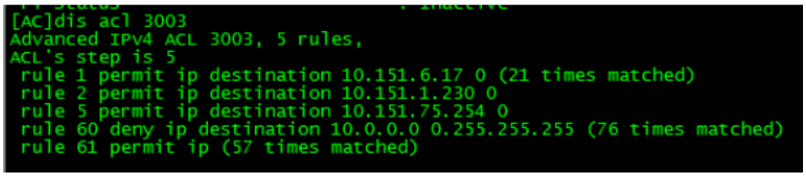
```
<AC>dis acl 3003
Advanced IPv4 ACL 3003, 8 rules,
ACL's step is 5
 rule 1 permit ip destination 10.151.6.17 0 (5 times matched)
 rule 10 permit ip destination 10.151.1.23[illegible] 0 (2 times matched)
 rule 20 permit ip destination 10.151.1.254 0
 rule 30 permit ip destination 10.151.75.254 0 (1 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)
```

Check the number of ACL matches. The number of ACL matches is still increasing after repeating the problem, indicating that the ACL is in effect.

3.View the configuration of  ACL



```
[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 configuration puts through the addresses for 10.151.6.17, 10.151.1.230, 10.151.75.254;This denies the other addresses in the segment, which doesn't seem to be a problem.

However, let's analyze the traffic direction. The ping packet path is back and forth. The ACL only puts through the address with the purpose of 10.151.6.17, but for the address planned to put through, it only puts through the rule with the address as the destination.So you also need to put through the source address.

## Solution

All plan permit addresses allow both for purpose and source release

Rule 10 permit IP Destination X.X.X.X 0

Rule 15 permit IP Source X.X.X.X 0