802.1x DACL、每用户ACL、过滤器ID和设备跟踪的行为

目录

简介

本文如何描述IP设备跟踪功能工作，包括什么触发是添加并且删除主机。并且，跟踪设备的影响在可下载的802.1x访问控制表(DACL)解释。行为更改在版本和平台之间。

本文的第二部分着重访问控制表(ACL)返回由验证、授权和统计(AAA)服务器和应用对802.1x会话。提交在DACL、每用户ACL和过滤器ID ACL之间的一个比较。并且，关于ACL重写的一些警告和默认ACL讨论。

设备跟踪的理论

设备跟踪添加一个条目，当：

- 它通过监听的DHCP了解新的条目。
- 它通过地址解析协议(ARP)请求了解新的条目(读发送方MAC地址和发送方IP地址从ARP数据包)。功能有时呼叫ARP检查，但是它不是相同的象动态ARP检查(戴)。默认情况下功能启用并且不可能禁用。它也呼叫监听的ARP，但是调试不会显示它，在“监听的debug arp”启用后。监听默认情况下的ARP启用并且不可能禁用或被控制。

设备跟踪删除条目，当没有ARP请求的时无响应(发送每台主机的探测器在跟踪表，默认情况下每30秒)的设备。

设备跟踪的配置

```
ip dhcp excluded-address 192.168.0.1 192.168.0.240
ip dhcp pool POOL
  network 192.168.0.0 255.255.255.0
!
ip dhcp snooping vlan 1
ip dhcp snooping
ip device tracking
!
interface Vlan1
ip address 192.168.0.2 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.48.66.1
!
interface FastEthernet0/1
description PC
```

跟踪测验的设备

```
BSNS-3560-1# show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                Hardware address
192.168.0.241    0100.5056.994e.a1       Mar 02 1993 02:31 AM    Automatic

BSNS-3560-1# show ip device tracking all
IP Device Tracking = Enabled
---------------------------------------------------------------
 IP Address     MAC Address       Interface          STATE
---------------------------------------------------------------
192.168.0.241   0050.5699.4ea1 FastEthernet0/1        ACTIVE
```

从版本12.2.33的调试， DHCP更新的IP设备跟踪监听

监听的DHCP填充绑定表：

```
BSNS-3560-1#  show debugging
DHCP Snooping packet debugging is on
DHCP Snooping event debugging is on
DHCP server packet debugging is on.
DHCP server event debugging is on.
track:
 IP device-tracking redundancy events debugging is on
```

```
 IP device-tracking cache entry Creation debugging is on
 IP device-tracking cache entry Destroy debugging is on
 IP device-tracking cache events debugging is on

02:30:57: DHCP_SNOOPING: checking expired snoop binding entries
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak.  Was Vl1
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Vl1 for pak.  Was Fa0/1
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak.  Was Vl1
02:31:12: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)
02:31:12: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input
interface: Fa0/1, MAC da: 001f.27e6.cfc0, MAC sa: 0050.5699.4ea1, IP da: 192.168.0.2,
IP sa: 192.168.0.241, DHCP ciaddr: 192.168.0.241, DHCP yiaddr: 0.0.0.0,
DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.5699.4ea1
02:31:12: DHCP_SNOOPING: add relay information option.
02:31:12: DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port format
02:31:12: DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format
02:31:12: DHCP_SNOOPING: binary dump of relay info option, length: 20 data&colon;
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0x1 0x1 0x3 0x2 0x8 0x0 0x6 0x0 0x1F 0x27 0xE6 0xCF 0x80
02:31:12: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: 001F.27E6.CFC0,
packet is flooded to ingress VLAN: (1)
02:31:12: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan1.
02:31:12: DHCPD: DHCPREQUEST received from client 0100.5056.994e.a1.
02:31:12: DHCPD: Sending DHCPACK to client 0100.5056.994e.a1 (192.168.0.241).
02:31:12: DHCPD: unicasting BOOTREPLY to client 0050.5699.4ea1 (192.168.0.241).
02:31:12: DHCP_SNOOPING: received new DHCP packet from input interface (Vlan1)
02:31:12: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface:
Vl1, MAC da: 0050.5699.4ea1, MAC sa: 001f.27e6.cfc0, IP da: 192.168.0.241,
IP sa: 192.168.0.2, DHCP ciaddr: 192.168.0.241, DHCP yiaddr: 192.168.0.241,
DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.5699.4ea1
02:31:12: DHCP_SNOOPING: add binding on port FastEthernet0/1.
02:31:12: DHCP_SNOOPING: added entry to table (index 189)
02:31:12: DHCP_SNOOPING: dump binding entry: Mac=00:50:56:99:4E:A1 Ip=192.168.0.241
Lease=86400     ld Type=dhcp-snooping Vlan=1 If=FastEthernet0/1
```

在DHCP绑定被添加到数据库后，触发设备跟踪的通知：

```
02:31:12: sw_host_track-ev:host_track_notification: Add event for host 0050.5699.4ea1,
192.168.0.241 on interface FastEthernet0/1
02:31:12: sw_host_track-ev:Async Add event for host 0050.5699.4ea1, 192.168.0.241
on interface FastEthernet0/1
02:31:12: sw_host_track-ev:MSG = 2
02:31:12: DHCP_SNOOPING_SW no entry found for 0050.5699.4ea1 0.0.0.1 FastEthernet0/1
02:31:12: DHCP_SNOOPING_SW host tracking not found for update add dynamic
(192.168.0.241, 0.0.0.0, 0050.5699.4ea1) vlan 1
02:31:12: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/1.
02:31:12: sw_host_track-ev:Add event: 0050.5699.4ea1, 192.168.0.241, FastEthernet0/1
02:31:12: sw_host_track-obj_create:0050.5699.4ea1(192.168.0.241) Cache entry created
02:31:12: sw_host_track-ev:Activating host 0050.5699.4ea1, 192.168.0.241 on
interface FastEthernet0/1
02:31:12: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
```

默认情况下ARP探测器被发送每30秒：

```
02:41:12: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:41:12: sw_host_track-ev:0050.5699.4ea1: Send Host probe (0)
02:41:12: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
02:41:42: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:41:42: sw_host_track-ev:0050.5699.4ea1: Send Host probe (1)
02:41:42: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
02:42:12: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:42:12: sw_host_track-ev:0050.5699.4ea1: Send Host probe (2)
02:42:12: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
02:42:42: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:42:42: sw_host_track-obj_destroy:0050.5699.4ea1(192.168.0.241): Cache entry deleted
02:42:42: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
```

```
     3 30.0110700 Cisco_e6:cf:83      Vmware_99:4e:a1     ARP      60 Who has 192.168.0.241?  Tell 0.0.0.0
     4 30.0111260 Vmware_99:4e:a1     Cisco_e6:cf:83      ARP      42 192.168.0.241 is at 00:50:56:99:4e:a1
     5 60.0235090 Cisco_e6:cf:83      Vmware_99:4e:a1     ARP      60 Who has 192.168.0.241?  Tell 0.0.0.0
     6 60.0235250 Vmware_99:4e:a1     Cisco_e6:cf:83      ARP      42 192.168.0.241 is at 00:50:56:99:4e:a1
     7 90.0230090 Cisco_e6:cf:83      Vmware_99:4e:a1     ARP      60 Who has 192.168.0.241?  Tell 0.0.0.0
     8 90.0230250 Vmware_99:4e:a1     Cisco_e6:cf:83      ARP      42 192.168.0.241 is at 00:50:56:99:4e:a1
```

在条目从跟踪表后的设备删除，对应的DHCP绑定条目仍然是那里：

```
BSNS-3560-1#show ip device tracking all
IP Device Tracking = Enabled
---------------------------------------------------------------
 IP Address     MAC Address       Interface          STATE
---------------------------------------------------------------

BSNS-3560-1#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.0.241    0100.5056.994e.a1       Mar 02 1993 03:06 AM    Automatic
```

有问题，当您有一ARP响应时，但是跟踪条目的设备无论如何删除。bug在版本12.2.55或15.x软件方面看来在版本12.2.33和没出现。

并且有一些差异，当处理用L2端口(access-port)时和L3端口(没有switchport)。

监听的探测器和的ARP

跟踪与ARP监听的功能的设备：

```
BSNS-3560-1#show debugging
ARP:
 ARP packet debugging is on
Arp Snoop:
 Arp Snooping debugging is on

03:43:36: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
03:43:36: sw_host_track-ev:0050.5699.4ea1: Send Host probe (0)
03:43:36: IP ARP: sent req src 0.0.0.0 001f.27e6.cf83,
                dst 192.168.0.241 0050.5699.4ea1 FastEthernet0/1
03:43:36: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
03:43:36: IP ARP: rcvd rep src 192.168.0.241 0050.5699.4ea1, dst 0.0.0.0 Vlan1
```

跟踪为版本12.2.55的IP设备-隐藏命令

对于版本12.2也许有需要使用隐藏命令为了激活它：

```
BSNS-3560-1#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 2
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
-----------------------------------------------------------------------
 IP Address     MAC Address   Vlan  Interface                STATE
-----------------------------------------------------------------------
192.168.0.244   0050.5699.4ea1  55   FastEthernet0/1           ACTIVE

Total number interfaces enabled: 1
Enabled interfaces:
  Fa0/1
```

```
BSNS-3560-1#ip device tracking interface fa0/48
BSNS-3560-1#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 2
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
--------------------------------------------------------------------
 IP Address     MAC Address   Vlan  Interface                STATE
--------------------------------------------------------------------
10.48.67.87     000c.2978.825d  1006 FastEthernet0/48         ACTIVE
10.48.67.31     020a.dada.dada  1006 FastEthernet0/48         ACTIVE
10.48.66.245    acf2.c5ed.8171  1006 FastEthernet0/48         ACTIVE
192.168.0.244   0050.5699.4ea1  55   FastEthernet0/1          ACTIVE
10.48.66.193    000c.2997.4ca1  1006 FastEthernet0/48         ACTIVE
10.48.66.186    0050.5699.3431  1006 FastEthernet0/48         ACTIVE

Total number interfaces enabled: 2
Enabled interfaces:
  Fa0/1, Fa0/48
```

跟踪为版本12.2.55的IP设备-静态IP示例

在本例中， PC配置与静态IP地址。调试显示，在您得到ARP响应(MSG=2)后，跟踪条目的设备更新。

```
01:03:16: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
01:03:16: sw_host_track-ev:0050.5699.4ea1: Send Host probe (0)
01:03:16: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
01:03:16: sw_host_track-ev:host_track_notification: Add event for host 0050.5699.4ea1,
192.168.0.241 on interface FastEthernet0/1, vlan 1
01:03:16: sw_host_track-ev:Async Add event for host 0050.5699.4ea1, 192.168.0.241
on interface FastEthernet0/1
01:03:16: sw_host_track-ev:MSG = 2
01:03:16: sw_host_track-ev:Add event: 0050.5699.4ea1, 192.168.0.241, FastEthernet0/1
01:03:16: sw_host_track-ev:0050.5699.4ea1: Cache entry refreshed
01:03:16: sw_host_track-ev:Activating host 0050.5699.4ea1, 192.168.0.241 on
interface FastEthernet0/1
01:03:16: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
```

那么从PC的每个ARP请求更新跟踪表的设备(发送方MAC地址和发送方IP地址从ARP数据包)。

跟踪为版本15.x的IP设备

请记住例如802.1x的DACL LAN轻版本不支持某些功能(请当心- Cisco Feature Navigator总是不显示正确信息)。

从版本12.2的隐藏命令可以被执行，但是不会有效果。在软件版本15.x中，跟踪的IP设备(IPDT)默认情况下为有启用的802.1x的接口只启用：

```
bsns-3750-5#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
--------------------------------------------------------------------
 IP Address     MAC Address   Vlan  Interface                STATE
--------------------------------------------------------------------
192.168.10.12   0007.5032.6941  100  GigabitEthernet1/0/1     ACTIVE
192.168.2.200   000c.29d7.0617  1    GigabitEthernet1/0/1     ACTIVE
```

```
Total number interfaces enabled: 2
Enabled interfaces:
 Gi1/0/1, Gi1/0/2

bsns-3750-5#show run int g1/0/3
Building configuration...

Current configuration : 38 bytes
!
interface GigabitEthernet1/0/3

bsns-3750-5(config)#int g1/0/3
bsns-3750-5(config-if)#switchport mode access
bsns-3750-5(config-if)#authentication port-control auto
bsns-3750-5(config-if)#do show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
------------------------------------------------------------------------
 IP Address     MAC Address   Vlan  Interface                STATE
------------------------------------------------------------------------
192.168.10.12   0007.5032.6941  100  GigabitEthernet1/0/1     ACTIVE
192.168.2.200   000c.29d7.0617  1    GigabitEthernet1/0/1     ACTIVE

Total number interfaces enabled: 3
Enabled interfaces:
 Gi1/0/1, Gi1/0/2, Gi1/0/3
```

在802.1x配置以后删除从端口， IPDT从该端口也将删除。端口状态也许是“DOWN”，因此有“switchport mode access”和“authenticaion波尔特控制自动”为了有在该端口激活的IP设备跟踪是必要的。最大接口设备限制定到10 ：

```
bsns-3750-5(config-if)#ip device tracking maximum ?
 <1-10>  Maximum devices
```

跟踪为Cisco IOS XE ®的IP设备

再次，在Cisco IOS XE 3.3的行为更改，当与Cisco IOS版本15.x比较。从版本12.2的隐藏命令过时，但是此错误当前将返回：

```
3850-1#  no ip device tracking int g1/0/48
% Command accepted but obsolete, unreleased or unsupported; see documentation.
```

在Cisco IOS XE，设备跟踪为所有接口(没有配置的802.1x)的那些激活：

```
3850-1#show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
---------------------------------------------------------------------------------------
 IP Address    MAC Address   Vlan  Interface           Probe-Timeout
  State    Source
---------------------------------------------------------------------------------------
10.48.39.29     000c.29bd.3cfa 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.28     0016.9dca.e4a7 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.76.117    0021.a0ff.5540 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
```

```
10.48.39.21     00c0.9f87.7471 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.16     0050.5699.1093 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.76.191.247   0024.9769.58cf 20   GigabitEthernet1/0/48  30
  ACTIVE   ARP
192.168.99.4    d48c.b52f.4a1e 99   GigabitEthernet1/0/12  30
  INACTIVE ARP
10.48.39.13     000c.296e.8dbc 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.15     0050.5699.128d 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.9      0012.da20.8c00 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.8      6c20.560e.1b64 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.11     000c.29e9.db25 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.5      0014.f15f.f7ca 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.4      000c.2972.57bc 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.7      5475.d029.74cf 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.76.108    001c.58de.9340 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.1      0006.f62a.c4a3 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.3      0050.5699.1bee 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.76.84     0015.58c5.e8b7 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.56     0015.fa13.9a40 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.59     0050.5699.1bf4 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP
10.48.39.58     000c.2957.c7ad 1    GigabitEthernet1/0/48  30
  ACTIVE   ARP


Total number interfaces enabled: 57
Enabled interfaces:
 Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7,
 Gi1/0/8, Gi1/0/9, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14,
 Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/20, Gi1/0/21,
 Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28,
 Gi1/0/29, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35,
 Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/40, Gi1/0/41, Gi1/0/42,
 Gi1/0/43, Gi1/0/44, Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/48, Gi1/1/1,
 Gi1/1/2, Gi1/1/3, Gi1/1/4, Te1/1/1, Te1/1/2, Te1/1/3, Te1/1/4
3850-1#$

3850-1#sh run int g1/0/48
Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet1/0/48
end

3850-1(config-if)#ip device tracking maximum ?
 <0-65535>  Maximum devices (0 means disabled)
```

并且，没有最大条目的限额每个端口(0含义已禁用)。

跟踪与802.1x和DACL的IP设备版本12.2.55的

如果802.1x配置与DACL，跟踪条目的设备用于为了填装设备的IP地址。此示例显示设备跟踪的静态工作配置的IP的：

```
BSNS-3560-1#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 2
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
---------------------------------------------------------------------
 IP Address     MAC Address   Vlan  Interface                STATE
---------------------------------------------------------------------
192.168.0.244   0050.5699.4ea1  2    FastEthernet0/1          ACTIVE

Total number interfaces enabled: 1
Enabled interfaces:
 Fa0/1
```

这是用“permit icmp建立的802.1x会话所有任何” DACL ：

```
BSNS-3560-1# sh authentication sessions  interface fa0/1
           Interface:  FastEthernet0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.0.244
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  2
              ACS ACL:  xACSACLx-IP-DACL-516c2694
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A3042A900000008008900C5
     Acct Session ID:  0x0000000D
              Handle:  0x19000008

Runnable methods list:
      Method   State
      dot1x    Authc Success BSNS-3560-1#show epm session summary
EPM Session Information
-----------------------
Total sessions seen so far : 1
Total active sessions      : 1

Interface               IP Address        MAC Address     Audit Session Id:
---------------------------------------------------------------------------
FastEthernet0/1         192.168.0.244     0050.5699.4ea1   0A3042A900000008008900C5
```

这显示已应用ACL ：

```
 BSNS-3560-1#show ip access-lists
Extended IP access list Auth-Default-ACL
   10 permit udp any range bootps 65347 any range bootpc 65348
   20 permit udp any any range bootps 65347
   30 deny ip any any (8 matches)
Extended IP access list xACSACLx-IP-DACL-516c2694 (per-user)
   10 permit icmp any any (6 matches)
```

并且，在fa0/1接口的ACL是相同的：

```
BSNS-3560-1#show ip access-lists interface fa0/1
    permit icmp any any
```

即使默认是dot1x ACL ：

```
BSNS-3560-1#show ip interface fa0/1
FastEthernet0/1 is up, line protocol is up
 Inbound  access list is Auth-Default-ACL
```

也许预计为了ACL能使用“其中任一”作为**192.168.0.244**。象这样的工作验证代理的，然而802.1x DACL src的“其中任一”没有更改对PC的检测的IP。

对于验证代理，缓存从ACS的一个原始ACL，并且显示与**show ip access-list命令**和特定(每用户与特定IP) ACL在接口应用用**显示IP访问控制列表接口fa0/1**命令。然而，验证代理不使用设备IP跟踪。

IP地址若没有正确地检测？在设备跟踪以后禁用：

```
BSNS-3560-1#show authentication sessions interface fa0/1
           Interface:  FastEthernet0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  Unknown
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  2
             ACS ACL:  xACSACLx-IP-DACL-516c2694
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A3042A9000000000000C775
     Acct Session ID:  0x00000001
              Handle:  0xB0000000

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

那么IP地址然后没有附加，但是DACL仍然应用：

```
BSNS-3560-1#show ip access-lists
Extended IP access list Auth-Default-ACL
   10 permit udp any range bootps 65347 any range bootpc 65348
   20 permit udp any any range bootps 65347
   30 deny ip any any (4 matches)
Extended IP access list xACSACLx-IP-DACL-516c2694 (per-user)
   10 permit icmp any any
```

在此方案中，跟踪为802.1x的设备没有要求。唯一的差异是那认识客户端的IP地址可以在前面用于RADIUS访问请求。在属性8以后附加：

```
radius-server attribute 8 include-in-access-req
```

它在Access-Request将存在，并且在ACS创建更加粒状的授权规则将是可能的：

```
00:17:44: RADIUS(00000001): Send Access-Request to 10.48.66.185:1645 id 1645/27, len 257
00:17:44: RADIUS:  authenticator F8 17 06 CE C1 85 E8 E8 - CB 5B 57 96 6C 07 CE CA
00:17:44: RADIUS:  User-Name           [1]   7   "cisco"
```

```
00:17:44: RADIUS:  Service-Type        [6]   6   Framed                   [2]
00:17:44: RADIUS:  Framed-IP-Address   [8]   6   192.168.0.244
```

记住TrustSec也需要跟踪为IP的IP设备对SGT捆绑。

跟踪与802.1x和DACL的IP设备版本15.x的

版本15.x和版本12.2.55有何区别在DACL ？在软件Version15.x方面，它为验证代理工作同一样。通用的ACL能被看到，当**show ip access-list命令**被输入(从AAA的被缓存的答复)时，但是，在**显示IP访问控制列表接口fa0/1**命令， src “其中任一”由主机的源IP地址后替换(已知通过跟踪的IP设备)。

这是电话和PC的示例在一个端口(g1/0/1)，在3750X的软件版本15.0.2SE2 ：

```
bsns-3750-5#sh authentication sessions interface g1/0/1
           Interface:  GigabitEthernet1/0/1
         MAC Address:  0007.5032.6941
          IP Address:  192.168.10.12
           User-Name:  00-07-50-32-69-41
              Status:  Authz Success
              Domain:  VOICE
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  100
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001012B680D23
     Acct Session ID:  0x0000017B
              Handle:  0x99000102

Runnable methods list:
      Method   State
      dot1x    Failed over
       mab      Authc Success

----------------------------------------
           Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
          IP Address:  192.168.2.200
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  20
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


Runnable methods list:
      Method   State
```

```
       dot1x    Authc Success
      mab      Not run
```
而PC使用dot1x，电话通过MAC验证旁路(MAB)验证。电话和PC使用同样ACL ：

```
bsns-3750-5#show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2 (per-user)
   10 permit ip any any
```
然而，当验证在接口级上来源由设备的IP地址替换了。IP设备跟踪更改的触发的和它能在任何时间发生(以后比ACL的验证会话和下载) ：

```
bsns-3750-5#show ip access-lists interface g1/0/1
    permit ip host 192.168.2.200 any (5 matches)
    permit ip host 192.168.10.12 any
```
应该标记两MAC地址作为静态：

```
bsns-3750-5#sh mac address-table interface g1/0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 20    0050.5699.4ea1    STATIC      Gi1/0/1
 100    0007.5032.6941    STATIC      Gi1/0/1
```

特定ACL条目

来源“其中任一”在DACL什么时候用主机IP地址替换？只有当有相同端口的(两名恳求者)至少两会话。

当只有一会话时，没有需要替换来源“其中任一”。问题也许出现，当有多个会话时，并且对于不是所有IP设备跟踪认识主机的IP地址。在该方案中它将是“中的任一”为一些条目。

该行为是不同的在一些平台。例如，既使当有每个端口，一验证会话在与版本15.0(2)EX的2960X ACL永远特定。然而，对于3560X和3750X版本15.0(2)SE，您需要有做至少两的会话该ACL特定。

控制方向

默认情况下，控制方向是类型两个：

```
bsns-3750-5(config)#int g1/0/1
bsns-3750-5(config-if)#authentication control-direction ?
 both  Control traffic in BOTH directions
 in    Control inbound traffic only

bsns-3750-5(config-if)#authentication control-direction both
```
那意味着，在请求方验证前，流量不可能发送到/从端口。为“在”模式，流量可能发送从端口到请求方，但是不从请求方到端口(可能是有用的为在LAN功能的苏醒)。

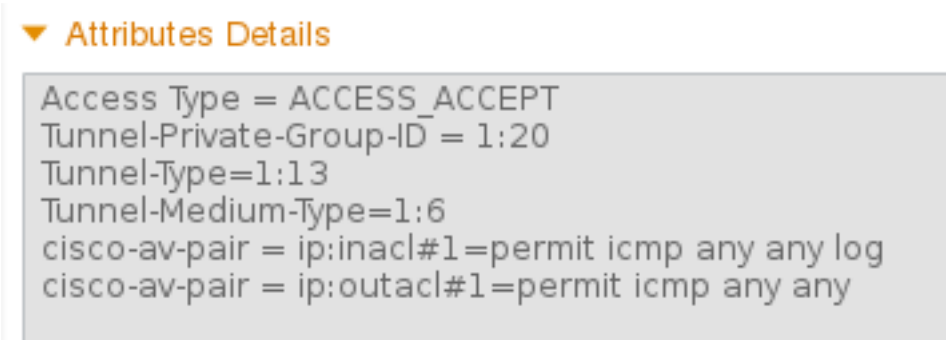
但是，交换机应用ACL在“在”方向。不重要使用哪个模式。

```
bsns-3750-5#sh ip access-lists interface g1/0/1 out
bsns-3750-5#sh ip access-lists interface g1/0/1 in
    permit ip host 192.168.2.200 any
    permit ip host 192.168.10.12 any
```
那基本意味，在验证ACL为对端口的流量应用(方向的)后，并且所有流量从端口(方向)允许。

跟踪与802.1x和每用户ACL的IP设备版本15.x的

使用每用户ACL在cisco-av-pair “ip通过的也是可能的：inacl”并且“ip ：outacl”。

此配置示例类似于先前配置，但是这次电话使用DACL和PC用途每用户ACL。PC的ISE配置文件是：



电话仍然有DACL应用：

```
bsns-3750-5#show authentication sessions interface g1/0/1
           Interface:  GigabitEthernet1/0/1
         MAC Address:  0007.5032.6941
          IP Address:  192.168.10.12
           User-Name:  00-07-50-32-69-41
              Status:  Authz Success
              Domain:  VOICE
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  100
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A800010000568431143D8
     Acct Session ID:  0x000006D2
              Handle:  0x84000569

Runnable methods list:
      Method   State
      dot1x    Failed over
      mab      Authc Success

bsns-3750-5#sh ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2 (per-user)
   10 permit ip any any
```

然而，在相同端口的PC使用每用户ACL ：

```
    Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
          IP Address:  192.168.2.200
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
```

```
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  20
        Per-User ACL:  permit icmp any any log
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000005674311400B
     Acct Session ID:  0x000006D1
              Handle:  0x9D000568
```

为了验证那如何在gig1/0/1端口合并：

```
bsns-3750-5#show ip access-lists interface g1/0/1
    permit icmp host 192.168.2.200 any log
    permit ip host 192.168.10.12 any
```

首先进入从每用户ACL被采取了(注意日志关键字)，并且第二个条目从DACL被采取。他们两个由跟踪为特定IP地址的IP设备重写。

每用户ACL能验证与**all命令调试的epm** ：

```
Apr 12 02:30:13.489: EPM_SESS_EVENT:IP Per-User ACE: permit icmp any any log received
Apr 12 02:30:13.489: EPM_SESS_EVENT:Recieved string GigabitEthernet1/0/1#IP#7844C6C
Apr 12 02:30:13.489: EPM_SESS_EVENT:Add ACE [permit icmp any any log] to ACL
[GigabitEthernet1/0/1#IP#7844C6C]
Apr 12 02:30:13.497: EPM_SESS_EVENT:Executed [ip access-list extended
GigabitEthernet1/0/1#IP#7844C6C] command through parse_cmd. Result= 0
Apr 12 02:30:13.497: EPM_SESS_EVENT:Executed [permit icmp any any log]
command through parse_cmd. Result= 0
Apr 12 02:30:13.497: EPM_SESS_EVENT:Executed [end] command through
parse_cmd. Result= 0
Apr 12 02:30:13.497: EPM_SESS_EVENT:Notifying PD regarding Policy (NAMED ACL)
application on the interface GigabitEthernet1/0/1
```

并且通过**show ip access-lists命令**：

```
bsns-3750-5#show ip access-lists
Extended IP access list GigabitEthernet1/0/1#IP#7844C6C (per-user)
   10 permit icmp any any log
```

怎么样ip ：outacl属性？它完全在版本15.x省略。属性接收，但是交换机不应用/加于的进程。

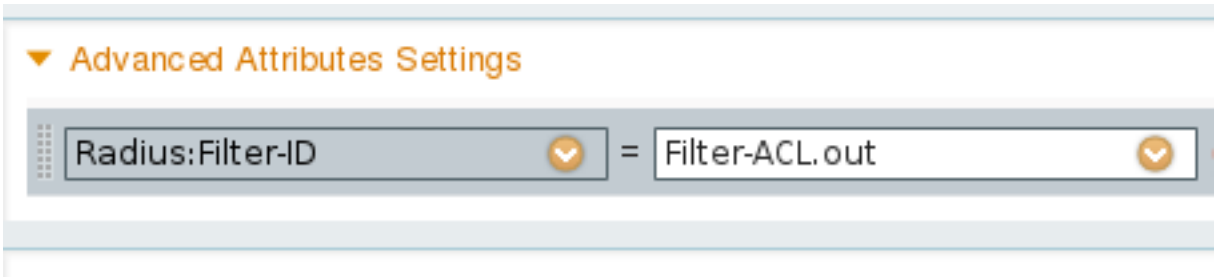
差异，当与DACL比较

在Cisco Bug ID CSCut25702中注明，每用户ACL跟DACL不同运行。与一个条目(“permit ip any any”)和一请求方的DACL连接对端口能正确地运作，无需IP设备跟踪启用。“任何”参数不会被替代，并且所有流量将允许。然而，为了每用户ACL是必须安排IP设备跟踪启用。如果它禁用并且有“permit ip any any”条目和一请求方，则所有流量将阻塞。

跟踪与802.1x和过滤器ID ACL的IP设备版本15.x的

并且，可以使用IETF属性过滤器ID [11]。AAA服务器返回ACL名称，在交换机应该定义本地。
ISE配置文件能如下所示:

注意您需要specifiy方向(在或)。对于那它手工是必要的添加属性：



然后调试显示：

```
debug epm all

Apr 12 23:41:05.170: EPM_SESS_EVENT:Filter-Id : Filter-ACL received
Apr 12 23:41:05.170: EPM_SESS_EVENT:Notifying PD regarding Policy (NAMED ACL)
application on the interface GigabitEthernet1/0/1
```

该ACL为认证的会话也将显示：

```
bsns-3750-5#show authentication sessions interface g1/0/1

           Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
          IP Address:  192.168.2.200
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  20
            Filter-Id:  Filter-ACL
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A800010000059E47B77481
     Acct Session ID:  0x00000733
              Handle:  0x5E00059F


Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

并且，作为ACL是已绑定的对接口：

```
bsns-3750-5#show ip access-lists interface g1/0/1
    permit icmp host 192.168.2.200 any log
    permit tcp host 192.168.2.200 any log
```

注意此ACL可以与ACL的其他类型在同一个接口的合并。例如，有在从ISE获得DACL的同一交换机端口另一请求方：“permit ip any any”您可能发现：

```
bsns-3750-5#show ip access-lists interface g1/0/1
    permit icmp host 192.168.2.200 any log
    permit tcp host 192.168.2.200 any log
    permit ip host 192.168.10.12 any
```

注意IP设备跟踪重写每来源的(请求方)来源IP。

怎么样“”过滤器列表？再次(作为每用户ACL)，它不会由交换机使用。

IP设备跟踪-默认和最佳实践

对于版本早于15.2(1)E，在所有功能能使用IPDT它前需要用此CLI命令全局首先启用：

```
(config)#ip device tracking
```

对于版本15.2(1)E和以后， **IP设备trace命令没有**必要。IPDT启用，只有当依靠它的功能启用它。如果功能不启用IPDT， IPDT禁用。跟踪”命令的“IP设备没有效果。特定功能有启用/禁用的控制IPDT。

当您启用IPDT时，您必须记住关于" Duplicate IP Address "问题。欲知更多信息，请参阅[排除故障“重复IP地址0.0.0.0”错误消息]。

推荐禁用在中继端口的IPDT ：

```
(config-if)# no ip device tracking
```

在最新Cisco IOS，它是不同命令：

```
(config-if)#ip device tracking maximum 0
```

推荐使在接入端口和延迟ARP探测器的IPDT为了避免" Duplicate IP Address "问题：

```
(config-if)#ip device tracking probe delay 10
```

接口版本15.x的ACL重写

对于接口ACL，它在验证前工作：

```
interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 ip access-group test1 in
 authentication order mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
end

bsns-3750-5#show ip access-lists test1
Extended IP access list test1
```

```
   10 permit tcp any any log-input
```
然而，在验证成功后它由从AAA服务器返回的ACL重写(覆盖) (不重要，如果它是DACL， ip ：inacl或者filterid)。

该ACL (test1)能阻塞在Open模式通常将允许)的流量(，但是，在验证不再后重要。既使当ACL没有从AAA服务器返回，接口ACL覆盖，并且提供完全权限。那有点误导，因为三重内容可编址存储器表明ACL仍然是在接口级上的已绑定的。这是从版本15.2.2的一示例在3750X ：

```
bsns-3750-6#show platform acl portlabels interface g1/0/2

Port based ACL: (asic 1)
----------------------------
 Input Label:  5    Op Select Index: 255
   Interface(s): Gi1/0/2
   Access Group: test1, 4 VMRs
   Ip Portal: 0 VMRs
   IP Source Guard: 0 VMRs
   LPIP: 0 VMRs
   AUTH: 0 VMRs
   C3PLACL: 0 VMRs
   MAC Access Group: (none), 0 VMRs
```
该信息是仅有效为接口级，不为会话级别。有些信息(提交被配制的ACL)可以推导从：

```
bsns-3750-6#show ip access-lists interface g1/0/2
    permit ip host 192.168.1.203 any
Extended IP access list test1
    10 permit icmp host 2.2.2.2 host 1.1.1.1
```
首先进入创建作为“permit ip any any” DACL为成功认证返回(和“其中任一”由从跟踪表)的设备的一个条目替换。第二个条目是接口ACL的结果和为所有应用新建的认证(在授权前)。

不幸地， (再从属的平台)两个ACL被连接。那在3750X的版本15.2.2发生。那意味着为已授权会话，他们两个应用。首先DACL和第二接口ACL。所以，当您添加明确“deny ip any any”， DACL不会考虑到接口ACL。通常明确拒绝在DACL接口ACL以后然后应用那。

版本15.0.2的行为在3750X是相同的，但是**interface命令嘘的IP访问控制列表不**再显示接口ACL (但是它用接口ACL在DACL将连接，除非明确拒绝存在)。

用于802.1x的默认ACL

有默认ACL的两种类型：

- 验证默认ACL开放-使用Open模式
- 用于已关闭访问-的验证默认ACL

验证默认ACL和验证默认ACL开放，当端口在未授权的状态时，使用。 默认情况下，使用关闭的访问。那意味着，在验证所有流量丢弃前，除了那个由验证默认ACL允许。此方式DHCP流量在成功的授权前允许。分配IP地址，并且下载的DACL可以正确地应用。ACL自动地创建并且不可能在配置找到。

```
bsns-3750-5#sh run | i Auth-Default

bsns-3750-5#sh ip access-lists Auth-Default-ACL
Extended IP access list Auth-Default-ACL
   10 permit udp any range bootps 65347 any range bootpc 65348 (22 matches)
   20 permit udp any any range bootps 65347 (12 matches)
   30 deny ip any any
```

它为第一验证动态地创建(在认证和授权相位之间)并且删除，在最后会话删除后。

验证默认ACL允许仅DHCP流量。在验证成功后，并且新的DACL下载，应用给该会话。当模式更改打开验证默认ACL开放出现，并且时相似地使用并且工作作为验证默认ACL ：

```
bsns-3750-5(config)#int g1/0/2
bsns-3750-5(config-if)#authentication open

bsns-3750-5#show ip access-lists
Extended IP access list Auth-Default-ACL-OPEN
   10 permit ip any any
```

两个ACL可以定制，但是他们在配置里不会被看到。

```
bsns-3750-5(config)#ip access-list extended Auth-Default-ACL
bsns-3750-5(config-ext-nacl)#permit udp any any

bsns-3750-5#sh ip access-lists
Extended IP access list Auth-Default-ACL
   10 permit udp any range bootps 65347 any range bootpc 65348 (22 matches)
   20 permit udp any any range bootps 65347 (16 matches)
   30 deny ip any any
   40 permit udp any any

bsns-3750-5#sh run | i Auth-Def
bsns-3750-5#
```

Open模式

前面部分描述默认情况下(行为包括Open模式使用的那个)的ACL的。Open模式的行为是：

- 它允许所有流量(根据验证默认ACL开放的默认)，当会话在一未授权的状态时。
- 会话在一未授权的状态在认证/授权时(有益于加密设备型号E (PXE)引导程序方案)或该进程以后发生故障(有益于方案呼叫“低影响模式”)。
- 当会话移动向多个平台的时Authorized State， ACL被连接，并且使用第一个DACL，然后接口ACL。
- 对于多验证或多域也许同时有多个会话用不同的状态(另外ACL类型然后将申请每会话)。

当接口ACL是必须

对于多个6500/4500平台，接口ACL是必须为了正确地应用DACL。

这是与4500个sup2 12.2.53SG6的一示例，没有接口ACL ：

```
brisk#show run int g2/3
!
interface GigabitEthernet2/3
 switchport mode access
 switchport voice vlan 10
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 mab
```

然后，在主机验证后， DACL下载。它不会应用，并且授权发生故障。

```
*Apr 25 04:38:05.239: RADIUS: Received from id 1645/19 10.48.66.74:1645,Access-Accept,
len 209
*Apr 25 04:38:05.239: RADIUS:  authenticator 35 8E 59 E4 D5 CF 8F 9A -
EE 1C FC 5A 9F 67 99 B2
*Apr 25 04:38:05.239: RADIUS:  User-Name           [1]   41
 "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1"
*Apr 25 04:38:05.239: RADIUS:  State               [24]  40
*Apr 25 04:38:05.239: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 61
 [ReauthSession:0a]
*Apr 25 04:38:05.239: RADIUS:   33 30 34 32 34 61 30 30 30 45 46 35 30 46 35 33
 [30424a000EF50F53]
*Apr 25 04:38:05.239: RADIUS:   35 41 36 36 39 33            [ 5A6693]
*Apr 25 04:38:05.239: RADIUS:  Class               [25]  54
*Apr 25 04:38:05.239: RADIUS:   43 41 43 53 3A 30 61 33 30 34 32 34 61 30 30 30
 [CACS:0a30424a000]
*Apr 25 04:38:05.239: RADIUS:   45 46 35 30 46 35 33 35 41 36 36 39 33 3A 69 73
 [EF50F535A6693:is]
*Apr 25 04:38:05.239: RADIUS:   65 32 2F 31 38 30 32 36 39 35 33 38 2F 31 32 38
 [e2/180269538/128]
*Apr 25 04:38:05.239: RADIUS:   36 35 35 33              [ 6553]
*Apr 25 04:38:05.239: RADIUS:  Message-Authenticato[80]  18
*Apr 25 04:38:05.239: RADIUS:   AF 47 E2 20 65 2F 59 39 72 9A 61 5C C5 8B ED F5
        [ G e/Y9ra\]
*Apr 25 04:38:05.239: RADIUS:  Vendor, Cisco       [26]  36
*Apr 25 04:38:05.239: RADIUS:   Cisco AVpair       [1]   30
 "ip:inacl#1=permit ip any any"
*Apr 25 04:38:05.239: RADIUS(00000000): Received from id 1645/19
*Apr 25 04:38:05.247: EPM_SESS_ERR:Failed to apply ACL to interface
*Apr 25 04:38:05.247: EPM_API:In function epm_send_message_to_client
*Apr 25 04:38:05.247: EPM_SESS_EVENT:Sending response message to process
AUTH POLICY Framework
*Apr 25 04:38:05.247: EPM_SESS_EVENT:Returning feature config
*Apr 25 04:38:05.247: EPM_API:In function epm_acl_feature_free
*Apr 25 04:38:05.247: EPM_API:In function epm_policy_aaa_response
*Apr 25 04:38:05.247: EPM_FSM_EVENT:Event epm_ip_wait_event state changed from
policy-apply to ip-wait
*Apr 25 04:38:05.247: EPM_API:In function epm_session_action_ip_wait
*Apr 25 04:38:05.247: EPM_API:In function epm_send_ipwait_message_to_client
*Apr 25 04:38:05.247: EPM_SESS_ERR:NULL feature list for client ctx 1B2694B0
for type DOT1X
*Apr 25 04:38:05.247: %AUTHMGR-5-FAIL: Authorization failed for client
(0007.5032.6941) on Interface Gi2/3
AuditSessionID 0A3043450000000060012C050

brisk#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE    Authz Failed   0A3043450000000060012C050
```

在接口ACL以后被添加：

```
brisk#show ip access-lists all
Extended IP access list all
   10 permit ip any any (63 matches)

brisk#sh run int g2/3
!
interface GigabitEthernet2/3
 switchport mode access
 switchport voice vlan 10
 ip access-group all in
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
```

```
 authentication priority dot1x mab
 authentication port-control auto
 mab
```

认证和授权将成功，并且DACL将正确地应用：

```
brisk#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE    Authz Success  0A30434500000008001A2CE4
```

行为不依靠“开放的验证”。为了接受DACL，您需要两的接口ACL打开/关闭模式。

在4500/6500的DACL

在4500/6500， DACL应用与acl_snoop DACLs。与4500个sup2 12.2.53SG6 (电话+ PC)的一示例显示此处。有语音(10)和数据的(100) VLAN分开的ACL ：

```
brisk#show ip access-lists
Extended IP access list acl_snoop_Gi2/3_10
   10 permit ip host 192.168.2.200 any
   20 deny ip any any
Extended IP access list acl_snoop_Gi2/3_100
   10 permit ip host 192.168.10.12 any
   20 deny ip any any
```

因为IPDT有正确条目， ACL特定：

```
brisk#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
---------------------------------------------------------------------
 IP Address     MAC Address   Vlan  Interface              STATE
---------------------------------------------------------------------
192.168.10.12   0007.5032.6941  100  GigabitEthernet2/3     ACTIVE
192.168.2.200   000c.29d7.0617  10   GigabitEthernet2/3     ACTIVE
```

认证的会话确认地址：

```
brisk#show authentication sessions int g2/3
           Interface:  GigabitEthernet2/3
         MAC Address:  000c.29d7.0617
          IP Address:  192.168.2.200
           User-Name:  00-0C-29-D7-06-17
              Status:  Authz Success
              Domain:  VOICE
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A3043450000003003258E0C
     Acct Session ID:  0x00000034
              Handle:  0x54000030

Runnable methods list:
      Method   State
      mab      Authc Success
      dot1x    Not run
```

```
----------------------------------------
           Interface:  GigabitEthernet2/3
         MAC Address:  0007.5032.6941
          IP Address:  192.168.10.12
           User-Name:  00-07-50-32-69-41
              Status:  Authz Success
              Domain:  DATA
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A3043450000002E031D1DB8
     Acct Session ID:  0x00000032
              Handle:  0x4A00002E

Runnable methods list:
      Method   State
      mab      Authc Success
      dot1x    Not run
```

在此阶段PC和电话只响应对ICMP回音，但是接口ACL存在：

```
brisk#show ip access-lists interface g2/3
    permit ip host 192.168.10.12 any
```

为什么？由于DACL仅争取电话(192.168.10.12)。对于PC，使用与Open模式的接口ACL ：

```
interface GigabitEthernet2/3
 ip access-group all in
 authentication open

brisk#show ip access-lists all
Extended IP access list all
   10 permit ip any any (73 matches)
```

总之， acl_snoop为PC和电话将创建，但是DACL为电话返回。所以该ACL被看到作为对接口的已绑定的。

802.1x的MAC地址状态

当802.1x验证开始时， MAC地址仍然被看到作为动态，但是该数据包的操作是丢弃：

```
bsns-3750-5#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/0/1    0007.5032.6941  dot1x    UNKNOWN  Running        C0A8000100000596479F4DCE

bsns-3750-5#show mac  address-table interface g1/0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 100    0007.5032.6941    DYNAMIC     Drop
Total Mac Addresses for this criterion: 1
```

在MAC地址变为的成功认证以后提供静态和端口号：

```
bsns-3750-5#show authentication sessions
```

```
Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/0/1    0007.5032.6941  mab      VOICE    Authz Success  C0A8000100000596479F4DCE

bsns-3750-5#show mac address-table interface g1/0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 100    0007.5032.6941    STATIC      Gi1/0/1
```

那真实对两个域的(语音/数据)所有mab/dot1x会话。

故障排除

切记读您的特定软件版本和平台的802.1x配置指南。

如果开TAC案例，请提供从这些命令的输出：

- show tech
- show authentication会话接口<xx>详细信息
- show mac address-table接口<xx>

收集SPAN端口数据包捕获和这些调试也是好的：

- debug radius verbose
- 调试epm全部
- debug authentication全部
- debug dot1x全部
- debug authentication功能<yy>全部
- debug aaa authentication
- debug aaa authorization

相关信息

- 802.1X验证服务配置指南， Cisco IOS XE版本3SE (Catalyst 3850交换机)
- Catalyst 3750-X和Catalyst 3560-X交换机软件配置指南， Cisco IOS版本15.2(1)E
- Catalyst 3750-X和3560-X软件配置指南，版本15.0(1)SE
- Catalyst 3560软件配置指南，版本12.2(52)SE
- 技术支持和文档 - Cisco Systems