瞭解802.1x DACL、每使用者ACL、過濾器ID和裝置跟蹤行為

目錄

簡介

本檔案將說明IP裝置追蹤功能、新增和移除主機的觸發器，以及裝置追蹤對802.1x DACL的影響。

裝置跟蹤原理

本文件說明 IP 裝置追蹤功能的運作方式，包括新增和移除主機的觸發程序。

此外，還說明了裝置跟蹤對802.1x可下載訪問控制清單(DACL)的影響。

行為在版本和平台之間更改。

本文第二部分重點介紹身份驗證、授權和記帳(AAA)伺服器返回並應用於802.1x會話的訪問控制清單(ACL)。

將比較DACL、Per-User ACL和Filter-ID ACL。

此外，還討論了ACL重寫和預設ACL的一些注意事項。

在以下情況下，裝置跟蹤會新增一個條目：

- 它通過DHCP監聽獲取新條目。
- 它通過地址解析協定(ARP)請求（從ARP資料包讀取傳送方MAC地址和傳送方IP地址）獲取新條目。

此功能有時稱為ARP檢測，但它與動態ARP檢測(DAI)不同。

該功能預設啟用，不能禁用。這也稱為ARP監聽，但是在啟用「debug arp snooping」後，調試不會顯示它。

ARP監聽預設啟用，不能禁用或控制。

當對ARP請求沒有響應時，裝置跟蹤會刪除一個條目（預設情況下每30秒為裝置跟蹤表中的每台主機傳送探測訊號）。

裝置跟蹤配置

```
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
```

裝置跟蹤測試

<#root>

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
```

從12.2.33版調試，DHCP監聽更新IP裝置跟蹤

DHCP監聽填充繫結表：

<#root>

```
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
```

將DHCP繫結新增到資料庫後，它會觸發裝置跟蹤通知：

<#root>

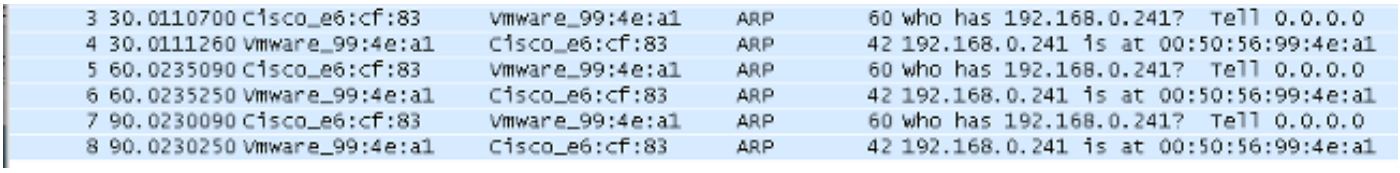
```
02:31:12:

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
```

預設情況下，每30秒傳送一次ARP探測：

<#root>

```
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

從裝置跟蹤表中刪除條目後，相應的DHCP繫結條目仍存在：

<#root>

```
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
```

當您有ARP響應時，出現問題，但裝置跟蹤條目仍然會被刪除。

該錯誤似乎存在於12.2.33版中，並未存在於12.2.55或15.x版軟體中。

在使用L2埠（接入埠）和L3埠（無交換機埠）進行處理時，也存在一些差異。

探查和ARP窺探

使用ARP窺探功能進行裝置跟蹤：

<#root>

```
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
```

12.2.55版的IP裝置追蹤 — 隱藏命令

對於此處的12.2版，請使用隱藏命令來啟用它：

```
<#root>

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
```

12.2.55版的IP裝置跟蹤 — 靜態IP示例

在本示例中，PC配置了靜態IP地址。調試程式顯示，在獲得ARP響應(MSG=2)後，裝置跟蹤條目會更新。

```
<#root>

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
```

因此PC發出的每個ARP請求都會更新裝置跟蹤表（來自ARP資料包的傳送方MAC地址和傳送方IP地址）。

適用於15.x版的IP裝置追蹤

請務必留意，LAN Lite版本不支援部分功能，例如適用於802.1x的DACL（請注意 — Cisco Feature Navigator並非始終顯示正確資訊）。

可以執行12.2版中的隱藏命令，但不起作用。在軟體版本15.x中，預設只會對已啟用802.1x的介面啟用IP裝置追蹤(IPDT):

<#root>

```
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
```

從埠刪除802.1x配置後，也會從該埠刪除IPDT。

連線埠狀態可能是「DOWN」，因此必須具有「switchport mode access」和「authentication port-control auto」，才能在該連線埠上啟用IP裝置追蹤。

最大介面裝置限制設定為10:

<#root>

```
bsns-3750-5(config-if)#
ip device tracking maximum

 ?
  <1-10>  Maximum devices
```

適用於Cisco IOS-XE®的IP裝置追蹤

同樣地，與Cisco IOS版本15.x相比，Cisco IOS-XE 3.3上的行為也發生了變化。

版本12.2中的隱藏命令已過時，但現在將返回以下錯誤：

```
<#root>

3850-1#

no ip device tracking int g1/0/48

% Command accepted but obsolete, unreleased or unsupported; see documentation.
```

在Cisco IOS-XE中，為所有介面（即使未配置802.1x的介面）啟用裝置跟蹤：

```
<#root>

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)
```

此外，每個埠的最大條目數沒有限制（0表示已禁用）。

802.1x的IP裝置跟蹤和12.2.55版的DACL

如果為802.1x配置了DACL，則使用裝置跟蹤條目來填充裝置的IP地址。

此範例顯示對靜態設定的IP執行的裝置追蹤：

<#root>

```
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
```

以下是使用「permit icmp any any」DACL建立的802.1x作業階段：

<#root>

```
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
```

<#root>

```
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
```

以下顯示已應用的ACL:

<#root>

```
 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)
```

此外，fa0/1介面的ACL也相同：

<#root>

```
BSNS-3560-1#
```

show ip access-lists interface fa0/1

```
     permit icmp any any
```

雖然預設值為dot1x ACL:

<#root>

```
BSNS-3560-1#
show ip interface fa0/1

FastEthernet0/1 is up, line protocol is up
  Inbound  access list is Auth-Default-ACL
```

ACL應使用「any」作為192.168.0.244。身份驗證代理的運作方式與此類似，但對於802.1x DACL src「any」，不會更改為檢測到的PC IP。

對於身份驗證代理，將快取來自ACS的一個原始ACL並使用show ip access-list命令顯示出來，並使用show ip access-list interface fa0/1命令在介面上應用特定（具有特定IP的每使用者）ACL。但是，身份驗證代理不使用裝置IP跟蹤。

如果未正確檢測到IP地址，該怎麼辦？禁用裝置跟蹤後：

<#root>

```
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
```

因此，此時未連線IP地址，但DACL仍然適用：

```
<#root>

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
```

在此場景中，不需要對802.1x進行裝置跟蹤。唯一的區別是，事先知道客戶端的IP地址可用於RADIUS訪問請求。附加屬性8之後：

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

它存在於存取要求中，且在ACS上，可以建立更精細的授權規則：

```
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
```

請記住，對於IP到SGT的繫結，TrustSec還需要IP裝置跟蹤。

802.1x的IP裝置跟蹤和15.x版的DACL

在DACL中，版本15.x和版本12.2.55有何區別？在軟體版本15.x中，其運作方式與驗證代理相同。

當輸入show ip access-list命令（來自AAA的快取響應）時可以看到通用ACL，但是在show ip access-list interface fa0/1命令後，src "any"會被主機的源IP地址替換（通過IP裝置跟蹤已知）。

以下是在一個連線埠(g1/0/1)上使用電話和PC的範例，3750X上的軟體版本15.0.2SE2:

<#root>

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
```

電話是透過MAC驗證略過(MAB)進行驗證的，而PC使用dot1x。電話和PC使用相同的ACL:

```
<#root>

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
```

但是，在介面級別驗證後，源地址已被裝置的IP地址替換。

IP裝置跟蹤會觸發變更，而且隨時都可能發生（遠遠晚於身份驗證會話和ACL下載）：

```
<#root>
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
```

兩個MAC地址均標籤為靜態：

```
<#root>
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條目

DACL中的源「any」何時替換為主機IP地址？僅當同一連線埠上至少有兩個作業階段（兩個請求方）時。

如果只有一個會話，則無需替換源「any」。

當存在多個會話時會出現問題，而且並不是所有會話的IP裝置跟蹤都知道主機的IP地址。在這種情況下，某些條目仍為「任意」。

某些平台上的行為有所不同。例如，在搭載15.0(2)EX版的2960X上，即使每個連線埠只有一個驗證作業階段，ACL也一律具有特定性。

但是，對於3560X和3750X版本15.0(2)SE，您需要至少有兩個作業階段才能使該ACL成為特定的。

Control-Direction

預設情況下，control-direction的型別為both:

```
<#root>

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
```

這表示在請求方通過驗證之前，流量無法傳送到連線埠或從連線埠傳送。對於「in」模式，流量可能從埠傳送到請求方，而不是從請求方傳送到埠（對於LAN喚醒功能可能很有用）。

不過，交換器會將ACL套用在「in」方向。使用哪種模式並不重要。

```
<#root>

bsns-3750-5#

sh ip access-lists interface g1/0/1 out


bsns-3750-5#

sh ip access-lists interface g1/0/1 in
```

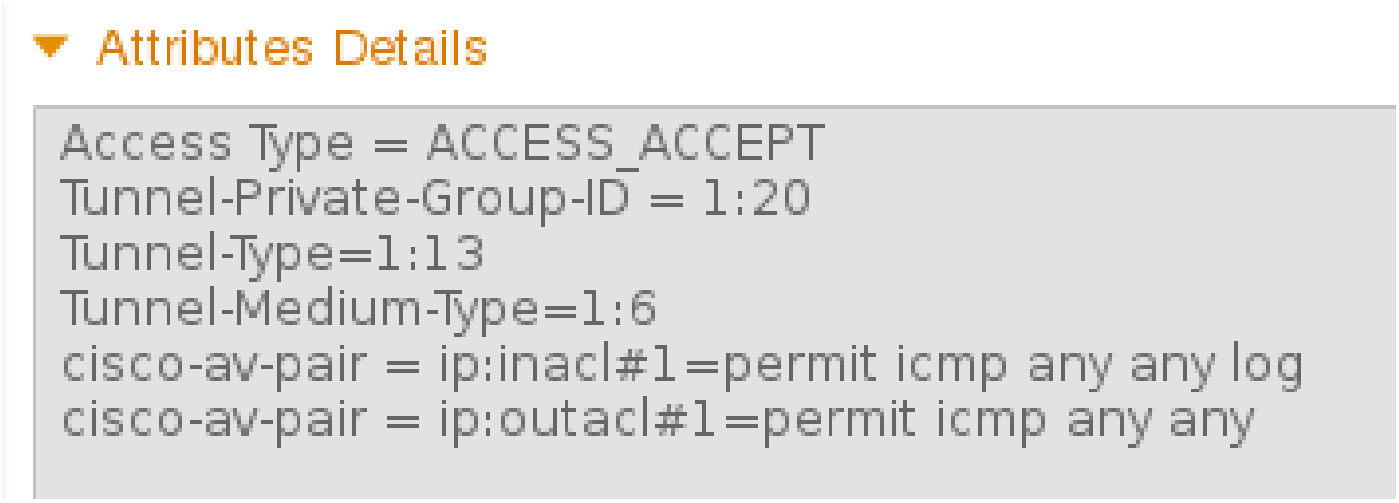
```
    permit ip host 192.168.2.200 any
    permit ip host 192.168.10.12 any
```

這基本上表示在驗證後，ACL會套用至連線埠的流量（方向），且所有流量都允許來自連線埠（輸出方向）。

802.1x的IP裝置跟蹤和版本15.x的每使用者ACL

也可以使用在cisco-av配對「ip:inacl」和「ip:outacl」中傳遞的每使用者ACL。

此示例配置與先前的配置類似，但這次電話使用DACL，而PC使用每使用者ACL。PC的ISE配置檔案為：



電話仍然應用了DACL:

<#root>

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:  C0A8000100000568431143D8
      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

但是同一連線埠上的PC會使用每使用者ACL:

<#root>

```
    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:  C0A800010000056743114008
      Acct Session ID:  0x000006D1
```

```
              Handle:  0x9D000568
```

若要驗證該連線埠如何在gig1/0/1連線埠上合併：

<#root>

```
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
```

第一個專案取自每使用者ACL（注意log關鍵字），第二個專案取自DACL。

對於特定IP地址，IP裝置跟蹤會重寫這兩種設定。

可以使用debug epm all命令驗證每使用者ACL:

<#root>

```
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

也可通過show ip access-lists命令：

<#root>

```
bsns-3750-5#
```

show ip access-lists

```
Extended IP access list GigabitEthernet1/0/1#IP#7844C6C (per-user)
    10 permit icmp any any log
```

ip:outacl屬性如何？在15.x版中完全省略。已收到該屬性，但交換機不應用/處理該屬性。

與DACL比較時的差異

如思科錯誤ID CSCut25702所述，每使用者ACL的行為與DACL不同。

只包含一個條目(「permit ip any any」)和一個連線到埠的請求方的DACL可以在未啟用IP裝置跟蹤的情況下正常工作。

「any」引數不會被替換，並且允許所有流量。但是，對於每使用者ACL，必須啟用IP裝置跟蹤。

如果系統已禁用且只有「permit ip any any」條目和一個請求方，則會阻止所有流量。

使用802.1x和Filter-ID ACL對版本15.x進行IP裝置跟蹤

此外，還可以使用IETF屬性filter-id [11]。AAA伺服器傳回ACL名稱，該名稱是在交換器上本地定義的。 ISE配置檔案可能如下所示：

請注意，您需要指定方向（輸入或輸出）。為此，必須手動新增屬性：

接著，偵錯顯示：

<#root>

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
```

對於已驗證作業階段，也會顯示該ACL:

<#root>

```
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
```

此外，由於ACL已繫結到介面：

<#root>

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
```

請注意，此ACL可與同一介面上的其他型別ACL合併。例如，在同一交換機埠上有另一個從ISE獲取DACL的請求方：「permit ip any any」您可以看到：

<#root>

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
```

請注意，IP裝置跟蹤會重寫每個源（請求方）的源IP。

「外寄」篩選清單怎麼辦？同樣地（作為每使用者ACL），交換機不會使用它。

IP裝置跟蹤 — 預設值和最佳實踐

對於低於15.2(1)E的版本，任何功能在使用IPDT之前，需要首先使用以下CLI命令全域性啟用該功能：

<#root>

(config)#

ip device tracking

對於版本15.2(1)E及更高版本，不再需要ip device tracking命令。只有在依賴它的功能啟用它時，IPDT才會啟用。

如果沒有功能啟用IPDT，則禁用IPDT。「no ip device tracking」命令無效。特定功能具有啟用/停用IPDT的控制。

啟用IPDT時，必須記住上的「重複IP地址」問題。如需詳細資訊，請參閱疑難排解「IP位址重複0.0.0.0」錯誤訊息。

建議在主干連線埠上停用IPDT:

```
<#root>

(config-if)#

no ip device tracking
```

在較新版本的Cisco IOS上，這是不同的命令：

```
<#root>

(config-if)#

 ip device tracking maximum 0
```

建議在存取連線埠上啟用IPDT並延遲ARP探測，以避免出現「重複IP位址」問題：

```
<#root>

(config-if)#

 ip device tracking probe delay 10
```

版本15.x的介面ACL重寫

對於介面ACL，它會在驗證之前運作：

```
<#root>

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
```

但是，身份驗證成功後，它將由從AAA伺服器返回的ACL重寫（覆蓋）（無論它是DACL、ip:inacl還是filterid）。

該ACL(test1)可以阻止流量（通常在開放模式下會允許該流量），但在身份驗證之後，不再重要。

即使沒有從AAA伺服器返回ACL，也會覆蓋介面ACL並提供完全訪問。

這有點誤導，因為三元內容可定址記憶體(TCAM)表示該ACL仍會在介面層級進行繫結。

以下是15.2.2版3750X的範例：

<#root>

```
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
```

該資訊僅對介面級別有效，對會話級別無效。如需瞭解更多資訊（請參閱複合ACL），請參閱：

<#root>

```
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 x.x.x.x host n.n.n.n
```

第一個條目建立為「permit ip any any」 DACL將返回以成功進行身份驗證（並且「any」將被裝置跟蹤表中的條目替換）。

第二個條目是介面ACL的結果，應用於所有新的身份驗證（在授權之前）。

遺憾的是，（同樣取決於平台）兩個ACL都是串聯的。在3750X上的15.2.2版上會發生這種情況。

這意味著，對於授權會話，兩者均適用。首先是DACL，然後是介面ACL。

因此，當您新增明確的「deny ip any any」時，DACL不會考慮介面ACL。

DACL中通常沒有明確的deny，然後在此之後應用介面ACL。

3750X上15.0.2版的行為相同，但sh ip access-list interface命令不再顯示介面ACL（但它仍然與介面ACL串聯，除非在DACL中存在明確的deny）。

用於802.1x的預設ACL

預設的ACL有兩種型別：

- auth-default-ACL-OPEN — 用於開放模式
- auth-default-ACL — 用於封閉式存取

當連線埠處於未授權狀態時，會同時使用auth-default-ACL和auth-default-ACL-OPEN。 預設情況下，使用封閉訪問。

這表示在驗證之前，除了auth-default-ACL允許的流量之外，所有流量都會遭到捨棄。

這樣，DHCP流量在成功授權之前會得到允許。

系統將分配IP地址，並且可正確應用下載的DACL。

該ACL是自動建立的，無法在配置中找到。

```
<#root>

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
```

它是為第一個身份驗證（在身份驗證和授權階段）動態建立的，並在刪除最後一個會話後刪除。

Auth-Default-ACL僅允許DHCP流量。身份驗證成功並且下載新的DACL後，會將其應用到該會話。

當模式變更為open auth-default-ACL-OPEN時，系統會顯示此模式，且其使用方式與Auth-Default-ACL的運作方式完全相同：

```
<#root>

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
```

兩個ACL均可自定義，但配置中從未顯示過。

```
<#root>

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#
```

開啟模式

前一節描述了ACL的行為（包括預設情況下用於開啟模式的ACL）。開啟模式的行為是：

- 當作業階段處於未授權狀態時，會允許所有流量（依照預設的auth-default-ACL-OPEN）。
- 在身份驗證/授權期間(適用於加密裝置型號E(PXE)引導方案)或該過程失敗之後（適用於稱為「低影響模式」的方案），會話處於未授權狀態。
- 當會話進入多個平台的授權狀態時，ACL會串聯起來，並使用第一個DACL，然後是介面ACL。
- 對於多重身份驗證或多域，可能同時有多個作業階段處於不同的狀態（然後適用於每個作業階段的不同ACL型別）。

當介面ACL為必需項時

對於多個6500/4500平台，必須提供介面ACL才能正確應用DACL。

以下是使用4500 sup2 12.2.53SG6（無介面ACL）的範例：

```
<#root>

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
```

然後，在主機通過身份驗證後，將下載DACL。未應用，授權失敗。

```
<#root>

*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 0A304345000000060012C050**

brisk#

show authentication sessions

Interface MAC Address   Method   Domain   Status   Session ID
Gi2/3   0007.5032.6941 mab   VOICE

Authz Failed

   0A304345000000060012C050

新增介面ACL後：

```
<#root>

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
```

驗證和授權成功，DACL應用正確：

```
<#root>

brisk#

show authentication sessions



Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE

 Authz Success

  0A304345000000080001A2CE4
```

該行為不依賴「身份驗證開啟」。若要接受DACL，您需要同時使用開放/關閉模式的介面ACL。

4500/6500上的DACL

在4500/6500上，DACL是以acl_snoop DACL套用。此處顯示使用4500 sup2 12.2.53SG6（電話+ PC）的範例。語音(10)和資料(100)VLAN有單獨的ACL:

<#root>

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

ACL是特定的，因為IPDT具有正確的條目：

<#root>

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

經過身份驗證的會話會確認地址：

<#root>

```
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
```

在這個階段，PC和電話都響應ICMP回應，但介面ACL僅顯示：

```
<#root>

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

192.168.10.12

 any
```

為什麼？因為只為電話(192.168.10.12)推送了DACL。對於PC，使用開放模式的介面ACL:

```
<#root>

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)
```

總而言之，會為PC和電話建立acl_snoop，但只為電話返回DACL。因此，該ACL被視為已繫結到介面。

802.1x的MAC地址狀態

當802.1x身份驗證啟動時，MAC地址仍被視為DYNAMIC，但對該資料包的操作是DROP:

```
<#root>

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
```

身份驗證成功後，MAC地址變為靜態，並且提供了埠號：

```
<#root>
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
```

對於兩個域(VOICE/DATA)的所有mab/dot1x會話都是如此。

疑難排解

請記得閱讀特定軟體版本和平台的802.1x配置指南。

如果您開啟TAC案例，請提供以下命令的輸出：

- show tech
- show authentication session interface <xx> detail
- show mac address-table interface <xx>

收集SPAN連線埠封包擷取和以下偵錯也是很好的：

- debug radius verbose
- debug epm all
- 調試全部身份驗證
- debug dot1x all
- debug authentication feature <yy> all
- 調試aaa身份驗證
- debug aaa authorization

相關資訊

- 802.1X身份驗證服務配置指南，Cisco IOS XE版本3SE（Catalyst 3850交換機）
- Catalyst 3750-X和Catalyst 3560-X交換機軟體配置指南，Cisco IOS版本15.2(1)E
- Catalyst 3750-X和3560-X軟體組態設定指南15.0(1)SE版
- Catalyst 3560軟體組態設定指南12.2(52)SE版
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。