802.1x DACL, 사용자별 ACL, 필터 ID 및 디바이스 추적 동작 이해

목차

소개

이 문서에서는 IP 디바이스 추적 기능, 호스트를 추가 및 제거하는 트리거, 802.1x DACL에 대한 디바이스 추적의 영향에 대해 설명합니다.

장치 추적 이론

이 문서에서는 IP 디바이스 추적 기능의 작동 방식에 대해 설명합니다. 여기에는 트리거가 호스트를 추가 및 제거하는 내용이 포함됩니다.

또한 디바이스 추적이 802.1x DACL(Downloadable Access Control List)에 미치는 영향에 대해서도 설명합니다.

버전 및 플랫폼 간에 동작이 변경됩니다.

이 문서의 두 번째 부분에서는 AAA(Authentication, Authorization, and Accounting) 서버에서 반환하고 802.1x 세션에 적용된 ACL(Access Control List)에 중점을 둡니다.

DACL, 사용자별 ACL 및 필터 ID ACL 간의 비교가 표시됩니다.

또한 ACL 재작성 및 기본 ACL과 관련된 몇 가지 주의 사항에 대해 설명합니다.

디바이스 추적에서는 다음과 같은 경우에 항목을 추가합니다.

- DHCP 스누핑을 통해 새 항목을 학습합니다.
- ARP(Address Resolution Protocol) 요청을 통해 새 항목을 학습합니다(ARP 패킷에서 발신자 MAC 주소 및 발신자 IP 주소 읽기).

이 기능을 ARP 검사라고도 하지만 DAI(Dynamic ARP Inspection)와 동일하지 않습니다.

이 기능은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다. ARP 스누핑이라고도 하지만 "debug arp snooping"을 활성화한 후에는 디버그에 표시되지 않습니다.

ARP 스누핑은 기본적으로 활성화되어 있으며 비활성화하거나 제어할 수 없습니다.

디바이스 추적은 ARP 요청에 대한 응답이 없을 때 항목을 제거합니다(기본적으로 디바이스 추적 테이블의 각 호스트에 대한 프로브를 30초마다 전송).

디바이스 추적 컨피그레이션

```
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
```

디바이스 추적 테스트

<#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
```

버전 12.2.33에서 디버깅, IP 장치 추적 DHCP Snooping에 의해 업데이트

DHCP 스누핑은 바인딩 테이블을 채웁니다.

<#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:
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

DHCP 바인딩이 데이터베이스에 추가되면 디바이스 추적을 위한 알림이 트리거됩니다.

<#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**

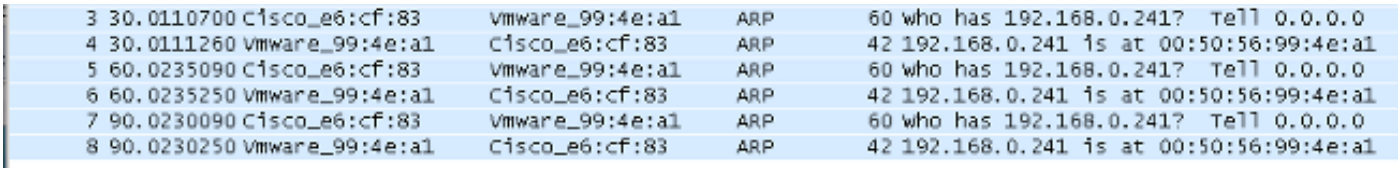
02:31:12: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/1.
02:31:12:

```
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
```

ARP 프로브는 기본적으로 30초마다 전송됩니다.

<#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
```

항목이 디바이스 추적 테이블에서 제거되어도 해당 DHCP 바인딩 항목은 그대로 유지됩니다.

<#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
```

ARP 응답이 있지만 디바이스 추적 항목이 제거되면 문제가 발생합니다.

이 버그는 버전 12.2.33에 있는 것으로 나타나며 버전 12.2.55 또는 15.x 소프트웨어에는 나타나지 않습니다.

또한 L2 포트(액세스 포트) 및 L3 포트(스위치 포트 없음)로 처리할 때 몇 가지 차이점이 있습니다.

프로브 및 ARP 스누핑

ARP 스누핑 기능을 통한 디바이스 추적:

<#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
```

버전 12.2.55에 대한 IP 디바이스 추적 - 숨겨진 명령

버전 12.2에서는 숨겨진 명령을 사용하여 활성화합니다.

<#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
```

버전 12.2.55의 IP 디바이스 추적 - 고정 IP 예

이 예에서는 PC가 고정 IP 주소로 구성되었습니다. 디버그는 ARP 응답(MSG=2)을 받은 후 디바이스 추적 항목이 업데이트됨을 보여줍니다.

<#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
```

따라서 PC의 모든 ARP 요청에서는 디바이스 추적 테이블(ARP 패킷의 발신자 MAC 주소 및 발신자 IP 주소)을 업데이트합니다.

버전 15.x에 대한 IP 디바이스 추적

802.1x용 DACL과 같은 일부 기능은 LAN Lite 버전에서 지원되지 않습니다(Cisco Feature Navigator에서 항상 올바른 정보를 표시하는 것은 아님).

버전 12.2에서 숨겨진 명령을 실행할 수 있지만 아무런 효과가 없습니다. 소프트웨어 버전 15.x에서는 기본적으로 802.1x가 활성화된 인터페이스에 대해서만 IPDT(IP 장치 추적)가 활성화됩니다.

<#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
```

포트에서 802.1x 컨피그레이션을 제거한 후 IPDT도 해당 포트에서 제거됩니다.

포트 상태가 "DOWN"일 수 있으므로 해당 포트에서 IP 장치 추적이 활성화되려면 "switchport mode access" 및 "authentication port-control auto"가 필요합니다.

최대 인터페이스 장치 제한은 10으로 설정됩니다.

<#root>

```
bsns-3750-5(config-if)#

ip device tracking maximum

 ?
  <1-10>  Maximum devices
```

Cisco IOS-XE®용 IP 장치 추적

Cisco IOS 버전 15.x와 비교했을 때 Cisco IOS-XE 3.3의 동작이 변경되었습니다.

버전 12.2의 숨겨진 명령은 더 이상 사용되지 않지만 이제 이 오류가 반환됩니다.

<#root>

```
3850-1#

no ip device tracking int g1/0/48


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

Cisco IOS-XE에서는 모든 인터페이스(802.1x가 구성되지 않은 인터페이스도)에 대해 디바이스 추적이 활성화됩니다.

<#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)
```

또한 포트당 최대 엔트리에 대한 제한이 없습니다(0은 비활성화됨을 의미함).

버전 12.2.55용 802.1x 및 DACL을 사용한 IP 디바이스 추적

802.1x가 DACL로 구성된 경우 디바이스의 IP 주소를 채우기 위해 디바이스 추적 항목이 사용됩니다.

다음 예에서는 고정으로 구성된 IP에 대해 작동하는 디바이스 추적을 보여 줍니다.

```
<#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
```

이는 "permit icmp any any" DACL로 구축된 802.1x 세션입니다.

```
<#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
```

적용된 ACL이 표시됩니다.

<#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)
```

또한 fa0/1 인터페이스의 ACL도 동일합니다.

```
<#root>

BSNS-3560-1#

show ip access-lists interface fa0/1


     permit icmp any any
```

기본값은 dot1x ACL이지만

```
<#root>

BSNS-3560-1#

show ip interface fa0/1


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

ACL에서는 "any"를 192.168.0.244로 사용해야 합니다. 이는 인증 프록시에 대해 이와 같이 작동하지만 802.1x DACL src "any"의 경우 PC의 탐지된 IP로 변경되지 않습니다.

인증 프록시의 경우 ACS의 원래 ACL 하나가 캐시되어 show ip access-list 명령으로 표시되고, 특정(특정 IP를 사용하는 사용자당) ACL이 show ip access-list interface fa0/1 명령으로 인터페이스에 적용됩니다. 그러나 auth-proxy는 디바이스 IP 추적을 사용하지 않습니다.

IP 주소가 올바르게 탐지되지 않으면 어떻게 됩니까? 디바이스 추적을 비활성화한 후:

```
<#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
```

따라서 IP 주소는 연결되지 않지만 DACL은 계속 적용됩니다.

<#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
```

이 시나리오에서는 802.1x에 대한 디바이스 추적이 필요하지 않습니다. 유일한 차이점은 클라이언트의 IP 주소를 미리 알고 RADIUS 액세스 요청에 사용할 수 있다는 것입니다. 특성 8이 연결된 후:

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

액세스 요청 및 ACS에서 보다 세분화된 권한 부여 규칙을 생성할 수 있습니다.

```
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
```

TrustSec에는 IP-SGT 바인딩에 대한 IP 디바이스 추적도 필요합니다.

버전 15.x용 802.1x 및 DACL을 사용한 IP 디바이스 추적

DACL에서 버전 15.x와 버전 12.2.55의 차이점은 무엇입니까? 소프트웨어 버전 15.x에서는 auth-proxy와 동일하게 작동합니다.

일반 ACL은 show ip access-list 명령(AAA의 캐시된 응답)을 입력하면 볼 수 있지만, show ip access-list interface fa0/1 명령 후에는 src "any"가 호스트의 소스 IP 주소로 대체됩니다(IP 디바이스 추적을 통해 알려짐).

한 포트(g1/0/1)의 전화기 및 PC, 3750X의 소프트웨어 버전 15.0.2SE2에 대한 예시입니다.

<#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:  C0A800010000001BD336EC4D6
      Acct Session ID:  0x000002F9
               Handle:  0xF80001BE


Runnable methods list:
       Method   State

  dot1x    Authc Success


       mab      Not run
```

전화기는 MAB(MAC Authentication Bypass)를 통해 인증되며 PC는 dot1x를 사용합니다. 전화기와

PC 모두 동일한 ACL을 사용합니다.

```
<#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
```

그러나 인터페이스 레벨에서 확인한 경우 소스가 디바이스의 IP 주소로 대체되었습니다.

IP 디바이스 추적은 변경을 트리거하며, 이는 언제든지 발생할 수 있습니다(ACL의 인증 세션 및 다운로드보다 훨씬 늦음).

```
<#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
```

두 MAC 주소 모두 고정으로 표시됩니다.

```
<#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
```

특정 ACL 항목

DACL의 소스 "any"가 언제 호스트 IP 주소로 대체됩니까? 동일한 포트에 적어도 두 개의 세션이 있는 경우에만(서 플리 컨 트 두 개).

세션이 하나뿐인 경우 소스 "any"를 교체할 필요가 없습니다.

여러 세션이 있는 경우 문제가 나타나며, 모든 세션이 IP 디바이스 추적에서 호스트의 IP 주소를 아는 것은 아닙니다. 이 시나리오에서는 일부 항목의 경우 여전히 "any"입니다.

이러한 동작은 일부 플랫폼에서는 다릅니다. 예를 들어, 버전 15.0(2)EX의 2960X에서는 포트당 인증 세션이 하나뿐인 경우에도 ACL이 항상 특정됩니다.

그러나 3560X 및 3750X 버전 15.0(2)SE의 경우 해당 ACL을 특정하게 하려면 최소 2개의 세션이 있어야 합니다.

제어 방향

기본적으로 control-direction은 both입니다.

```
<#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
```

즉, 신청자가 인증되기 전에 트래픽을 포트로 또는 포트에서 보낼 수 없습니다. "in" 모드의 경우 트

래픽이 포트에서 신청자로 전송되었지만 신청자에서 포트로 전송되지 않았을 수 있습니다(WAKE on LAN 기능에 유용할 수 있음).

그래도 스위치는 "수신" 방향으로만 ACL을 적용합니다. 어떤 모드를 사용하는지는 중요하지 않습니다.

<#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
```

즉, 기본적으로 인증 후 ACL은 포트에 대한 트래픽(방향)에 적용되며 모든 트래픽은 포트에서 허용됩니다(방향 외).

버전 15.x의 802.1x 및 사용자별 ACL을 통한 IP 디바이스 추적

또한 cisco av 쌍 "ip:inacl" 및 "ip:outacl"에서 전달되는 사용자별 ACL을 사용할 수 있습니다.

이 예제 컨피그레이션은 이전 컨피그레이션과 유사하지만, 이번에는 전화기에서 DACL을 사용하고 PC에서 사용자별 ACL을 사용합니다. PC의 ISE 프로파일은 다음과 같습니다.

▼ Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:20
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
cisco-av-pair = ip:inacl#1=permit icmp any any log
cisco-av-pair = ip:outacl#1=permit icmp any any
```

전화기에 DACL이 아직 적용되어 있습니다.

<#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
```

그러나 동일한 포트의 PC는 사용자별 ACL을 사용합니다.

<#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
```

gig1/0/1 포트에서 병합되는 방식을 확인하려면 다음을 수행합니다.

<#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
```

첫 번째 항목은 사용자별 ACL에서 가져온 것이며(log 키워드 참조) 두 번째 항목은 DACL에서 가져온 것입니다.

둘 다 특정 IP 주소에 대한 IP 디바이스 추적에 의해 재작성됩니다.

사용자별 ACL은 debug epm all 명령으로 확인할 수 있습니다.

<#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

또한 show ip access-lists 명령을 통해

<#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 특성은 어떻습니까? 버전 15.x에서는 완전히 생략되었습니다. 특성이 수신되었지만 스위치에서 해당 특성을 적용/처리하지 않습니다.

DACL과 비교할 때의 차이

Cisco 버그 ID CSCut25702에 설명된 것처럼 사용자별 ACL은 DACL과 다르게 작동합니다.

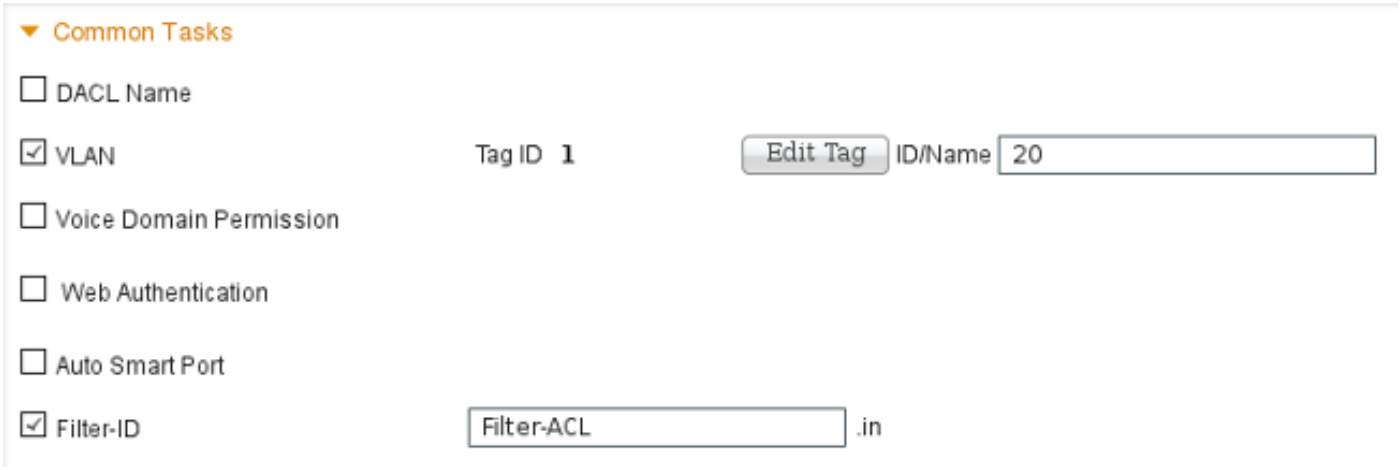
한 개의 항목("permit ip any any")과 한 개의 신청자가 포트에 연결된 DACL은 IP 디바이스 추적을 활성화하지 않고도 올바르게 작동할 수 있습니다.

"any" 인수는 대체되지 않으며 모든 트래픽이 허용됩니다. 그러나 사용자 단위 ACL의 경우 IP 디바이스 추적을 활성화해야 합니다.

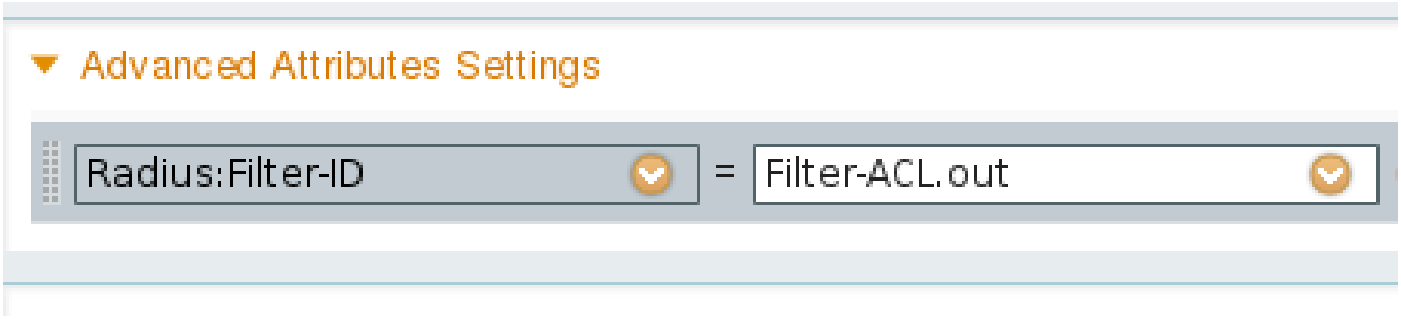
비활성화되어 있고 "permit ip any any any" 항목과 하나의 신청자만 있는 경우 모든 트래픽이 차단됩니다.

버전 15.x에 대한 802.1x 및 Filter-ID ACL을 사용한 IP 디바이스 추적

또한 IETF 특성 filter-id [11]을 사용할 수 있습니다. AAA 서버는 스위치에 로컬로 정의된 ACL 이름을 반환합니다. ISE 프로파일은 다음과 같을 수 있습니다.



방향(수신 또는 발신)을 지정해야 합니다. 이를 위해 특성을 수동으로 추가해야 합니다.



그런 다음 디버그에 다음이 표시됩니다.

<#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
```

해당 ACL은 인증된 세션에 대해서도 표시됩니다.

<#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
```

그리고 ACL이 인터페이스에 바인딩되면

```
<#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
```

이 ACL은 동일한 인터페이스에서 다른 유형의 ACL과 병합할 수 있습니다. 예를 들어, 동일한 스위치 포트에 ISE에서 DACL를 가져오는 다른 신청자 "permit ip any any" 를 가지고 있다면 다음을 볼 수 있습니다.

```
<#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
```

IP 디바이스 추적은 각 소스(신청자)에 대해 소스 IP를 재작성합니다.

"발신" 필터 목록은 어떻습니까? (사용자별 ACL로) 스위치에서 사용되지 않습니다.

IP 디바이스 추적 - 기본값 및 모범 사례

15.2(1)E 이전 릴리스의 경우 어떤 기능에서도 IPDT를 사용하려면 먼저 다음 CLI 명령을 사용하여 전역적으로 활성화해야 합니다.

```
<#root>

(config)#

ip device tracking
```

릴리스 15.2(1)E 이상에서는 ip device tracking 명령이 더 이상 필요하지 않습니다. IPDT는 이 기능에 의존하는 기능에서 활성화하는 경우에만 활성화됩니다.

IPDT를 활성화하는 기능이 없으면 IPDT가 비활성화됩니다. "no ip device tracking(ip 디바이스 추적 안 함)" 명령은 적용되지 않습니다. 특정 기능에는 IPDT를 활성화/비활성화할 수 있는 컨트롤이 있습니다.

IPDT를 활성화하면에서 "Duplicate IP Address(IP 주소 복제)" 문제를 기억해야 합니다. 자세한 내용은 "중복 IP 주소 0.0.0.0" 오류 메시지 문제 해결을 참조하십시오.

트렁크 포트에서 IPDT를 비활성화하는 것이 좋습니다.

```
<#root>

(config-if)#

no ip device tracking
```

이후 Cisco IOS에서는 다른 명령입니다.

```
<#root>

(config-if)#

 ip device tracking maximum 0
```

"Duplicate IP Address(중복 IP 주소)" 문제를 방지하려면 액세스 포트에서 IPDT를 활성화하고 ARP 프로브를 지연하는 것이 좋습니다.

```
<#root>

(config-if)#

 ip device tracking probe delay 10
```

버전 15.x에 대한 인터페이스 ACL 재작성

인터페이스 ACL의 경우 인증 전에 작동합니다.

```
<#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
```

그러나 인증이 성공하면 AAA 서버에서 반환된 ACL에 의해 다시 기록(재지정)됩니다(DACL, ip:inacl 또는 filtered인지 여부는 상관없음).

해당 ACL(test1)은 트래픽을 차단할 수 있지만(일반적으로 개방 모드에서 허용됨) 인증 후에는 더 이상 문제가 되지 않습니다.

AAA 서버에서 어떤 ACL도 반환되지 않는 경우에도 인터페이스 ACL을 덮어쓰고 전체 액세스 권한을 제공합니다.

TCAM(Ternary Content Addressable Memory)은 ACL이 인터페이스 레벨에서 여전히 바인딩되어 있음을 나타내므로 약간 오해의 소지가 있습니다.

다음은 3750X의 버전 15.2.2의 예입니다.

```
<#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
```

이 정보는 세션 수준이 아닌 인터페이스 수준에만 유효합니다. 몇 가지 추가 정보(복합 ACL 제공)는 다음에서 추론할 수 있습니다.

<#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

첫 번째 항목은 성공적인 인증을 위해 "permit ip any any" DACL이 반환되며 "any"는 디바이스 추적 테이블의 항목으로 대체됩니다.

두 번째 항목은 인터페이스 ACL의 결과이며 모든 새 인증(권한 부여 전)에 적용됩니다.

안타깝게도 두 ACL은 (플랫폼에 따라 다름) 연결되어 있습니다. 이는 3750X의 버전 15.2.2에서 발생합니다.

즉, 공인 세션의 경우 두 세션 모두 적용됩니다. 먼저 DACL을 선택하고 두 번째 인터페이스 ACL을 선택합니다.

따라서 명시적 "deny ip any any any"를 추가하면 DACL에서 인터페이스 ACL을 고려하지 않습니다.

일반적으로 DACL에는 명시적 거부가 없으며 그 이후에는 인터페이스 ACL이 적용됩니다.

3750X에서 버전 15.0.2의 동작은 동일하지만 sh ip access-list interface 명령은 더 이상 인터페이스 ACL을 표시하지 않습니다(그러나 DACL에 명시적 거부가 없는 한 인터페이스 ACL과 연결됨).

802.1x에 사용되는 기본 ACL

기본 ACL에는 두 가지 유형이 있습니다.

- auth-default-ACL-OPEN - 개방 모드에 사용됩니다.
- auth-default-ACL - 닫힌 액세스에 사용됩니다.

포트가 인증되지 않은 상태일 때 auth-default-ACL 및 auth-default-ACL-OPEN이 모두 사용됩니다. 기본적으로 닫힌 액세스가 사용됩니다.

즉, 인증 전에는 auth-default-ACL에서 허용하는 트래픽을 제외한 모든 트래픽이 삭제됩니다.

이렇게 하면 DHCP 트래픽이 권한 부여에 성공하기 전에 허용됩니다.

IP 주소가 할당되고 다운로드한 DACL을 올바르게 적용할 수 있습니다.

해당 ACL은 자동으로 생성되며 컨피그레이션에서 찾을 수 없습니다.

<#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
```

첫 번째 인증(인증 및 권한 부여 단계 사이)에 대해 동적으로 생성되며 마지막 세션이 제거된 후 제거됩니다.

Auth-Default-ACL은 DHCP 트래픽만 허용합니다. 인증이 성공하고 새 DACL이 다운로드되면 해당 세션에 적용됩니다.

모드를 open auth-default-ACL-OPEN으로 변경하면 Auth-Default-ACL-OPEN이 나타나며 이 모드가 사용되며 Auth-Default-ACL과 정확히 동일한 방식으로 작동합니다.

<#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
```

두 ACL을 모두 사용자 지정할 수 있지만 컨피그레이션에는 표시되지 않습니다.

<#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#
```

열기 모드

이전 섹션에서는 ACL(기본적으로 열기 모드에 사용되는 ACL 포함)의 동작에 대해 설명했습니다. 열기 모드의 동작은 다음과 같습니다.

- 세션이 인증되지 않은 상태일 때 (기본 auth-default-ACL-OPEN에 따라) 모든 트래픽을 허용합니다.
- 인증/권한 부여 중에(PXE(Encryption Appliance Model E) 부팅 시나리오에 적합) 또는 프로세스가 실패한 후("로우 임팩트 모드"라는 시나리오에 적합) 세션이 승인되지 않은 상태입니다.
- 세션이 여러 플랫폼에 대한 권한 부여 상태로 이동하면 ACL이 연결되고 첫 번째 DACL이 사용된 다음 인터페이스 ACL이 사용됩니다.
- 다중 인증 또는 다중 도메인의 경우 여러 세션이 동시에 여러 상태로 있을 수 있습니다(그런 다음 각 세션에 서로 다른 ACL 유형이 적용됨).

인터페이스 ACL이 필수인 경우

여러 6500/4500 플랫폼의 경우 DACL을 올바르게 적용하려면 인터페이스 ACL이 필수입니다.

다음은 인터페이스 ACL이 없는 4500 sup2 12.2.53SG6의 예입니다.

<#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
```

그런 다음 호스트가 인증된 후 DACL이 다운로드됩니다. 적용되지 않으며 권한 부여가 실패합니다.

<#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 0A3043450000000060012C050

```
brisk#
```

show authentication sessions

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

Authz Failed

```
   0A3043450000000060012C050
```

인터페이스 ACL이 추가된 후:

<#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

인증 및 권한 부여가 성공하고 DACL이 올바르게 적용됩니다.

<#root>

brisk#

show authentication sessions

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

Authz Success

  0A3043450000000800 1A2CE4

동작은 "authentication open"에 종속되지 않습니다. DACL을 수락하려면 오픈/클로즈 모드 모두에 인터페이스 ACL이 필요합니다.

4500/6500의 DACL

4500/6500에서 DACL은 acl_snoop DACL과 함께 적용됩니다. 4500 sup2 12.2.53SG6(전화 + PC)의 예가 여기에 표시됩니다. 음성(10) 및 데이터(100) VLAN에는 별도의 ACL이 있습니다.

<#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
```

IPDT에 올바른 항목이 있으므로 ACL은 고유합니다.

<#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
```

인증된 세션에서 주소를 확인합니다.

<#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
```

이 단계에서 PC와 전화기 모두 ICMP 에코에 응답하지만 인터페이스 ACL은 다음과 같은 기능만 제공합니다.

<#root>

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

192.168.10.12

 any
```

왜 그럴까요? DACL은 전화기(192.168.10.12)에 대해서만 푸시되었기 때문입니다. PC에서는 오픈 모드의 인터페이스 ACL이 사용됩니다.

<#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)
```

요약하면, acl_snoop는 PC와 전화기 모두에 대해 생성되지만 DACL은 전화기에 대해서만 반환됩니다. 따라서 해당 ACL이 인터페이스에 바인딩된 것으로 표시됩니다.

802.1x의 MAC 주소 상태

802.1x 인증이 시작되면 MAC 주소는 여전히 DYNAMIC으로 표시되지만 해당 패킷에 대한 작업은 DROP입니다.

<#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

인증에 성공하면 MAC 주소가 고정이 되고 포트 번호가 제공됩니다.

<#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**

이는 두 도메인(VOICE/DATA)의 모든 mab/dot1x 세션에 해당합니다.

문제 해결

특정 소프트웨어 버전 및 플랫폼에 대한 802.1x 컨피그레이션 가이드를 반드시 읽으십시오.

TAC 케이스를 열 경우 다음 명령의 출력을 제공합니다.

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

또한 SPAN 포트 패킷 캡처 및 다음 디버그를 수집하는 것이 좋습니다.

- 디버그 radius verbose
- epm all 디버그
- 모든 인증 디버그
- 모두 dot1x 디버그
- 인증 기능 디버그 <yy> 모두
- aaa 인증 디버그
- aaa 권한 부여 디버그

관련 정보

- 802.1X 인증 서비스 컨피그레이션 가이드, Cisco IOS XE 릴리스 3SE(Catalyst 3850 스위치)
- Catalyst 3750-X 및 Catalyst 3560-X 스위치 소프트웨어 컨피그레이션 가이드, Cisco IOS 릴리스 15.2(1)E
- Catalyst 3750-X 및 3560-X 소프트웨어 컨피그레이션 가이드, 릴리스 15.0(1)SE
- Catalyst 3560 Software 컨피그레이션 가이드, 릴리스 12.2(52)SE
- 기술 지원 및 문서 − Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.