802.1x DACL、ユーザごとのACL、フィルタID、およびデバイストラッキングの動作について

内容

はじめに

このドキュメントでは、IPデバイストラッキング機能、ホストを追加および削除するトリガー、および802.1x DACLに対するデバイストラッキングの影響について説明します。

デバイストラッキングの理論

このドキュメントでは、IP デバイス トラッキング機能の動作（ホストの追加と削除を引き起こす動作を含む）について説明します。

また、デバイストラッキングが 802.1x ダウンロード可能アクセス制御リスト（DACL）に与える影響についても説明します。

動作は、バージョンおよびプラットフォームによって異なります。

このドキュメントの後半では、認証、許可、およびアカウンティング（AAA）サーバーから返され、802.1x セッションに適用されるアクセス制御リスト（ACL）に焦点を当てています。

DACL、ユーザー単位 ACL、およびフィルタ ID ACL の比較も提供します。

また、ACL の書き換えとデフォルト ACL に関するいくつかの注意事項についても説明します。

デバイストラッキングでは、次の場合にエントリが追加されます。

- DHCP スヌーピングを介して新しいエントリを学習したとき。
- Address Resolution Protocol（ARP）要求を介して新しいエントリを学習したとき（ARP パケットから送信元 MAC アドレスと送信元 IP アドレスを読み取ったとき）。

この機能は、「ARP インスペクション」と呼ばれることもありますが、ダイナミック ARP インスペクション（DAI）とは異なります。

この機能はデフォルトで有効であり、無効にすることはできません。ARPスヌーピングとも呼ばれますが、「debug arp snooping」を有効にすると、デバッグに表示されなくなります。

ARP スヌーピングはデフォルトで有効になっており、無効にしたり制御することはできません。

デバイストラッキングでは、ARP 要求に対する応答がない場合にエントリが削除されます（デフォルトでは、30 秒ごとにデバイス トラッキング テーブルの各ホストにプローブが送信されます）。

デバイストラッキングの設定

```
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
```

デバイストラッキングのテスト

<#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
```

バージョン 12.2.33 からのデバッグ、DHCP スヌーピングによって更新される IP デバイストラッキング

DHCP スヌーピングはバインディングテーブルにデータを入力します。

<#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 バインディングがデータベースに追加されると、デバイストラッキングの通知がトリガーされます。

<#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 プローブはデフォルトで 30 秒ごとに送信されます。

<#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)

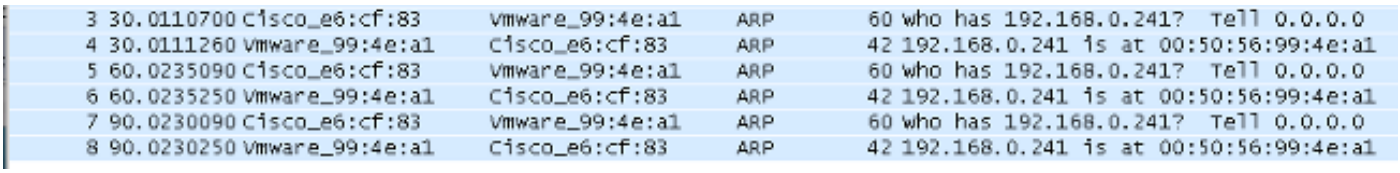
```
02:41:42: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
02:42:12: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:42:12: sw_host_track-ev:0050.5699.4ea1:
```

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
```

デバイス トラッキング テーブルからエントリが削除された後も、対応する DHCP バインディングエントリは引き続き存在します。

<#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 応答があってもデバイス トラッキング エントリが削除される問題が存在します。

このバグはバージョン 12.2.33 で見られ、バージョン 12.2.55 または 15.x ソフトウェアでは見られません。

また、L2 ポート（アクセスポート）と L3 ポート（スイッチポートなし）での処理時には、いくつかの違いが存在します。

プローブおよび ARP スヌーピング

ARP スヌーピング機能によるデバイストラッキング：

<#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
```

バージョン 12.2.55 の IP デバイストラッキング：隠しコマンド

バージョン12.2の場合は、隠しコマンドを使用してアクティブにします。

<#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
```

バージョン 12.2.55 の IP デバイストラッキング：静的 IP の例

この例では、PC に静的 IP アドレスが設定されています。デバッグでは、ARP 応答（MSG = 2）があるとデバイス トラッキング エントリが更新されることが示されます。

<#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
```

そのため、PC からのすべての ARP 要求により、デバイス トラッキング テーブル（ARP パケットからの送信元 MAC アドレスと送信元 IP アドレス）が更新されます。

バージョン 15.x の IP デバイストラッキング

802.1x の DACL などの一部の機能は LAN Lite バージョンではサポートされていないことに注意してください（なお、Cisco Feature Navigator に常に正しい情報が表示されるわけではありません）。

バージョン12.2の隠しコマンドは実行できますが、効果はありません。ソフトウェアバージョン 15.x では、IP デバイストラッキング（IPDT）は、デフォルトで、802.1x が有効になっているインターフェイスについてのみ有効になります。

<#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
```

802.1x設定をポートから削除すると、IPDTもそのポートから削除されます。

ポートのステータスは「DOWN」である可能性があるため、そのポートでIPデバイストラッキングをアクティブにするには、「switchport mode access」と「authenticaion port-control auto」が必要です。

最大インターフェイスデバイス制限は 10 に設定されます。

```
<#root>

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

Cisco IOS-XE® の IP デバイストラッキング

この場合も、Cisco IOS バージョン 15.x と比較すると、Cisco IOS-XE 3.3 の動作が変更されています。

バージョン12.2の隠しコマンドは廃止されましたが、今度は次の工ラーが返されます。

```
<#root>

3850-1#
no ip device tracking int g1/0/48

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

Cisco IOS-XE では、すべてのインターフェイス (802.1x が設定されていないインターフェイスも) についてデバイストラッキングがアクティブになります。

```
<#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)
```

また、ポートあたりの最大エントリ数に制限はありません（0 は無効を意味します）。

バージョン 12.2.55 の 802.1x と DACL による IP デバイストラッキング

802.1x が DACL で設定されている場合、デバイスの IP アドレスを入力するためにデバイス トラッキング エントリが使用されます。

次の例は、静的に設定された IP に関して機能しているデバイストラッキングを示しています。

<#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
```

次は、「permit icmp any any」DACLで構築された 802.1x セッションです。

<#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
```

次に、適用された ACL が示されています。

<#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)
```

また、fa0/1 インターフェイスの ACL も同じです。

```
<#root>

BSNS-3560-1#
show ip access-lists interface fa0/1


     permit icmp any any
```

デフォルトは dot1x ACL ですが、次のようになります。

```
<#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では192.168.0.244として「any」を使用することが想定されています。これは認証プロキシでは次のように動作しますが、802.1x DACLではsrc "any"はPCの検出されたIPに変更されません。

認証プロキシの場合は、ACS からの元の ACL が 1 つキャッシュされて、show ip access-list コマンドで表示され、show ip access-list interface fa0/1 コマンドで特定の（特定の IP を持つユーザー単位の）ACL がインターフェイスに適用されます。ただし、認証プロキシではデバイス IP トラッキングは使用されません。

IP アドレスが正しく検出されないと、どうなるでしょうか。デバイストラッキングに無効なった後は、次のようになります。

```
<#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
```

このため、IP アドレスは接続されませんが、DACL は引き続き適用されます。

```
<#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
```

このシナリオでは、802.1x のデバイストラッキングは必要ありません。唯一の違いは、クライア

ントの IP アドレスを事前に知ることで RADIUS アクセス要求に使用できることです。属性 8 が付加された後は、次のようになります。

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

これはAccess-Requestに存在し、ACSではより詳細な認可ルールを作成できます。

```
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
```

TrustSec には IP から SGT へのバインディングの IP デバイストラッキングも必要であることに注意してください。

バージョン 15.x の 802.1x と DACL による IP デバイストラッキング

DACL のバージョン 15.x とバージョン 12.2.55 の違いは何でしょうか。ソフトウェアバージョン 15.x では、認証プロキシと同じように動作します。

show ip access-list コマンドを入力すると汎用 ACL が表示されますが（AAA からのキャッシュされた応答）、show ip access-list interface fa0/1 コマンドの後に、送信元の「any」がホストの送信元 IP アドレスホスト（IP デバイストラッキングを介して認識）に置き換えられます。

次は、1 つのポート（g1/0/1）上の電話機と PC の例です（3750X 上のソフトウェアバージョン 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:  C0A800010000001012B680D23
      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
```

電話機は MAC 認証バイパス (MAB) によって認証されますが、PC は dot1x を使用します。電話機と PC の両方が同じ ACL を使用します。

```
<#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
```

ただし、インターフェイスレベルで確認すると、送信元はデバイスの IP アドレスによって置き換えられています。

IP デバイストラッキングがこの変更をトリガーし、これはいつでも (認証セッションと ACL のダウンロードからかなりの時間が経過した後でも) 発生する可能性があります。

```
<#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
```

両方のMACアドレスがスタティックとしてマークされます。

```
<#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
```

特定の ACL エントリ

DACL の送信元「any」は、どのような場合にホスト IP アドレスによって置き換えられるのでしょうか。同じポートに少なくとも 2 つのセッション（2 つのサプリカント）が存在する場合だけです。

セッションが 1 つしかない場合は、送信元「any」を置き換える必要がありません。

この問題は、複数のセッションが存在する場合に発生します。すべてのセッションについて、IPデバイストラッキングがホストのIPアドレスを認識しているわけではありません。このシナリオでは、一部のエントリに対してはまだ「any」です。

この動作は、一部のプラットフォームでは異なります。たとえば、バージョン15.0(2)EXの2960Xでは、ポートごとに認証セッションが1つだけの場合でも、ACLは常に特定です。

ただし、バージョン 15.0(2)SE を搭載する 3560X および 3750X では、その ACL を特定するために少なくとも 2 つのセッションが必要です。

制御方向

デフォルトでは、制御方向は両方向タイプです。

```
<#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
```

つまり、サプリカントが認証されるまで、ポートとの間でトラフィックを送受信できません。「入力」モードであれば、ポートからサプリカントにトラフィックを送信できますが、サプリカントからポートへは送信できません（Wake on LAN 機能には役立つ可能性があります）。

それでも、スイッチは ACL を「入力」方向にのみ適用します。使用されるモードは関係ありません。

```
<#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
```

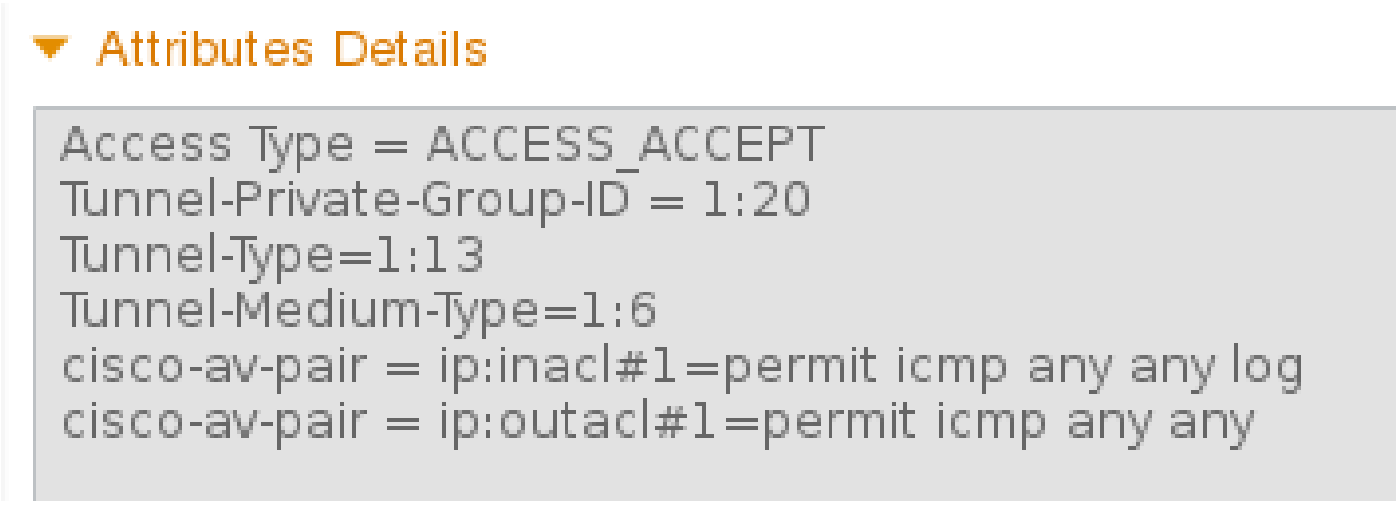
つまり、基本的には、認証後に、ポートへのトラフィック（入力方向）に ACL が適用され、ポートからのトラフィック（出力方向）はすべて許可されます。

バージョン 15.x の 802.1x とユーザー単位 ACL による IP デバイストラッキング

cisco-av-pair の「ip:inacl」と「ip:outacl」で渡されるユーザー単位 ACL を使用することもできます。

この設定例は前の設定に似ていますが、今回は、電話機が DACL を使用し、PC はユーザー単位

ACL を使用します。PC の ISE プロファイルは、次のとおりです。



電話機には引き続き DACL が適用されています。

<#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:  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

ただし、同じポートの PC はユーザー単位 ACL を使用します。

<#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:  C0A8000100000056743114008
      Acct Session ID:  0x000006D1
               Handle:  0x9D000568
```

これが gig1/0/1 ポートでどのようにマージされるのかを確認するには、次のようにします。

<#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
```

最初のエントリはユーザー単位 ACL から取得されており（log キーワードに注意）、2 番目のエントリは DACL から取得されます。

どちらも、特定 IP アドレスの IP デバイストラッキングによって書き換えられます。

ユーザー単位 ACL は、debug epm all コマンドで確認できます。

```
<#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
```

また、show ip access-lists コマンドでも確認できます。

```
<#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 属性については、どうでしょうか。バージョン 15.x では完全に省略されています。属性は受信されていますが、スイッチはその属性を適用/処理しません。

DACL と比較した場合の違い

Cisco Bug ID CSCut25702 に記載されているように、ユーザー単位 ACL の動作は DACL とは異なります。

ただ 1 つのエントリ（「 permit ip any any 」）と 1 つのサプリカントがポートに接続されている DACL は、IP デバイストラッキングを有効にしなくても正しく動作します。

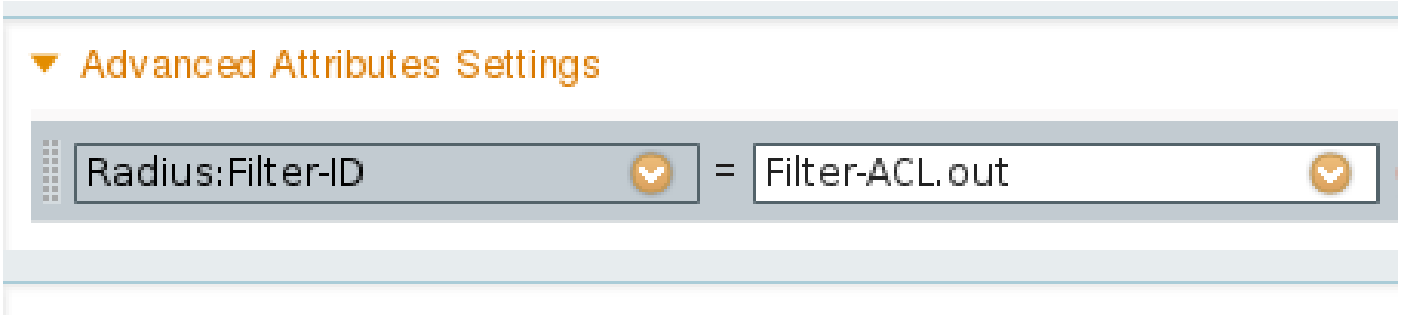
「any」引数は置き換えられず、すべてのトラフィックが許可されます。しかし、ユーザー単位 ACL の場合は、IP デバイストラッキングを有効にする必要があります。

これが無効で、「permit ip any any」エントリと1つのサプリカントだけがある場合、すべてのトラフィックがブロックされます。

バージョン 15.x の 802.1x とフィルタ ID ACL による IP デバイストラッキング

また、IETF 属性 filter-id [11] を使用できます。AAAサーバは、スイッチ上でローカルに定義されたACL名を返します。 ISEプロファイルは次のようになります。

方向（入力または出力）を指定する必要があることに注意してください。そのためには、属性を手動で追加する必要があります。



その後、デバッグでは、次のように表示されます。

<#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
```

このACLは、認証されたセッションに対しても表示されます。

<#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
```

また、ACL がインターフェイスにバインドされているため、次のようになります。

<#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
```

この ACL は同じインターフェイス上の他のタイプの ACL とマージできることに注意してください。たとえば、同じスイッチポートに、ISEからDACLを取得する別のサプリカント「permit ip any any」を設定すると、次のように表示されます。

```
<#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 デバイストラッキングによって、各送信元（サプリカント）の送信元 IP が書き換えられることに注意してください。

「出力」フィルタリストについては、どうでしょうか。ここでも（ユーザごとのACLとして）、スイッチはこのACLを使用しません。

IP デバイストラッキング：デフォルトとベストプラクティス

15.2(1)E より前のリリースの場合、いずれかの機能で IPDT を使用するには、まず、次の CLI コマンドを使用してグローバルに有効にする必要があります。

```
<#root>

(config)#

ip device tracking
```

リリース 15.2(1)E 以降では、ip device tracking コマンドは不要になりました。IPDT は、IPDT に依存する機能によって有効にされた場合にのみ有効になります。

IPDT を有効にする機能がない場合、IPDT は無効になります。「no ip device tracking」コマンドの効果はありません。特定の機能には、IPDT を有効または無効にする制御があります。

IPDT を有効にする場合は、「重複 IP アドレス」の問題に注意する必要があります。詳細については、『Troubleshoot "Duplicate IP Address 0.0.0.0" Error Messages』を参照してください。

トランクポートでは IPDT を無効にすることをお勧めします。

<#root>

```
(config-if)#
```

no ip device tracking

後の Cisco IOS では、これは別のコマンドです。

<#root>

```
(config-if)#
```

ip device tracking maximum 0

「重複 IP アドレス」の問題を回避するために、アクセスポートで IPDT を有効にし、ARP プローブを遅延させることをお勧めします。

<#root>

```
(config-if)#
```

ip device tracking probe delay 10

バージョン 15.x のインターフェイス ACL の書き換え

インターフェイス ACL の場合は、認証前に動作します。

<#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
```

ただし、認証に成功すると、AAA サーバーから返された ACL（DACL、ip:inacl、filterid のいずれでもかまいません）によって書き換えられます（上書きされます）。

このACL(test1)はトラフィックをブロックできますが（通常はオープンモードで許可されます）、認証後は問題になりません。

AAA サーバーから ACL が返されない場合でも、インターフェイス ACL は書き換えられ、フルアクセスが提供されます。

TCAM（Ternary Content Addressable Memory）は、ACL が引き続きインターフェイスレベルでバインドされていることを示すため、これは少し誤解を招く可能性があります。

3750X 上のバージョン 15.2.2 からの例を、次に示します。

```
<#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
```

この情報は、セッションレベルではなく、インターフェイスレベルでのみ有効です。いくつかの追加情報（複合 ACL を提供）を、次から推測できます。

```
<#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
```

最初のエントリは「permit ip any any」として作成され、認証に成功すると DACL が返されます（また、「any」はデバイス トラッキング テーブルのエントリによって置き換えられます）。

2 番目のエントリは、インターフェイス ACL の結果であり、すべての新しい認証に適用されます（許可前）。

残念ながら、（これもプラットフォームに依存しますが）両方の ACL が連結されます。これは、3750X 上のバージョン 15.2.2 で発生します。

つまり、許可されたセッションでは、両方が適用されます。1 つ目は DACL、2 つ目はインターフェイス ACL です。

そのため、明示的な「deny ip any any」を追加しても、DACLはインターフェイスACLを考慮しません。

通常、DACL には明示的な拒否がなく、その後にインターフェイス ACL が適用されます。

3750Xのバージョン15.0.2の動作は同じですが、sh ip access-list interfaceコマンドでインターフェイスACLが表示されなくなりました（ただし、DACLに明示的なdenyが存在しない限り、インターフェイスACLと連結されたままです）。

802.1x に使用されるデフォルト ACL

デフォルト ACL には次の 2 つのタイプがあります。

- auth-default-ACL-OPEN：オープンモードに使用
- auth-default-ACL：クローズドアクセスに使用

ポートが無許可ステートの場合、auth-default-ACLとauth-default-ACL-OPENの両方が使用されます。 デフォルトでは、クローズドアクセスが使用されます。

つまり、認証前は、auth-default-ACL で許可されたトラフィックを除くすべてのトラフィックがドロップされます。

このようにして、許可が成功する前に DHCP トラフィックが許可されます。

IP アドレスが割り当てられ、ダウンロードされた DACL を正しく適用できます。

この ACL は自動的に作成され、設定内にはありません。

```
<#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
```

これは最初の認証（認証フェーズと許可フェーズの間）のために動的に作成され、最後のセッションが削除された後に削除されます。

auth-default-ACL は DHCP トラフィックのみを許可します。認証が成功し、新しいDACLがダウンロードされると、そのセッションに適用されます。

モードがopen auth-default-ACL-OPENに変更されると、これが表示されて使用され、Auth-Default-ACLとまったく同じように動作します。

```
<#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
```

両方のACLはカスタマイズできますが、設定には表示されません。

```
<#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#
```

open モード

前のセクションでは、ACL の動作について説明しました（これには、オープンモードの場合にデフォルトで使用されるものが含まれます）。オープンモードの動作は、次のとおりです。

- セッションが未許可状態の場合、すべてのトラフィックを許可します（デフォルトの auth-default-ACL-OPEN に従う）。
- セッションは、認証/許可時（暗号化アプライアンスモデル E（PXE）ブートシナリオに適しています）またはそのプロセスが失敗した後（「低影響モード」と呼ばれるシナリオに適しています）に未許可状態になります。
- 複数のプラットフォームの場合にセッションが許可状態に移行すると、ACL が連結されて、最初の DACL が使用され、その後にインターフェイス ACL が使用されます。
- マルチ認証またはマルチドメインの場合、異なる状態で同時に複数のセッションが存在する可能性があります（その場合、セッションごとに異なるACLタイプが適用されます）。

インターフェイス ACL が必須の場合

複数の 6500/4500 プラットフォームの場合、インターフェイス ACL は、DACL を正しく適用するために必須です。

次に、4500 sup2 12.2.53SG6、インターフェイス ACL なしの例を示します。

```
<#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
```

ホストが認証されると、DACL がダウンロードされます。これは適用されず、認可は失敗します。

<#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
```

インターフェイス ACLが追加されると、次のようになります。

```
<#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
```

認証と認可が成功し、DACLが正しく適用されます。

```
<#root>
```

```
brisk#
show authentication sessions


Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE
 Authz Success
  0A304345000000008001A2CE4
```

この動作は「authentication open」に依存しません。DACL を受け入れるには、オープン/クローズモードの両方でインターフェイス ACL が必要です。

4500/6500 の DACL

4500/6500 では、DACL が acl_snoop DACL によって適用されます。次に、4500 sup2 12.2.53SG6（電話 + PC）の例を示します。音声（10）VLAN とデータ（100）VLAN には個別の ACL があります。

```
<#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
```

IPDT に正しいエントリがあるため、ACL は特定されます。

```
<#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
```

認証されたセッションがアドレスを確認します。

```
<#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
```

この段階では、PC と電話機の両方が ICMP エコーに応答しますが、インターフェイス ACL は次のみを提示します。

<#root>

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

192.168.10.12

```
 any
```

これは、なぜですか。これは、DACL が電話機 (192.168.10.12) についてのみプッシュされているためです。PC については、オープンモードのインターフェイス ACL が使用されます。

<#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)
```

要約すると、acl_snoopはPCと電話の両方に対して作成されますが、DACLは電話に対してのみ返されます。このため、その ACL はインターフェイスにバインドされていると見なされます。

802.1x の MAC アドレスステータス

802.1x 認証が開始されても、MAC アドレスは引き続き動的として認識されますが、そのパケットに対するアクションはドロップです。

```
<#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
```

認証に成功すると、MAC アドレスは静的になり、ポート番号が提供されます。

```
<#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

  C0A800010000596479F4DCE

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
```

これは、両方のドメイン（音声/データ）のすべての mab/dot1x セッションに当てはまります。

トラブルシュート

ご使用のソフトウェアバージョンおよびプラットフォーム用の 802.1x コンフィギュレーションガイドを必ずお読みください。

TAC ケースをオープンする場合は、次のコマンドの出力を提供してください。

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

また、SPAN ポートパケットキャプチャと次のデバッグを収集することもお勧めします。

- debug radius verbose
- debug epm all
- debug authentication all
- debug dot1x all
- debug authentication feature <yy> all
- debug aaa authentication
- debug aaa authorization

関連情報

- 『802.1X Authentication Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』
- 『Catalyst 3750-X and Catalyst 3560-X Switch Software Configuration Guide, Cisco IOS

Release 15.2(1)E』
- 『Catalyst 3750-X and 3560-X Software Configuration Guide, Release 15.0(1)SE』
- 『Catalyst 3560 Software Configuration Guide, Release 12.2(52)SE』
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。