802.1x DACL, por usuario ACL, id del filtro, y comportamiento de seguimiento del dispositivo

Contenido

[Introducción](#)
[Teoría de seguimiento del dispositivo](#)
[Configuración de seguimiento del dispositivo](#)
[Dispositivo que sigue las pruebas](#)
[Debugs de la versión 12.2.33, seguimiento del dispositivo IP actualizado por el snooping del DHCP](#)
[Sonda y snooping ARP](#)
[Dispositivo IP que sigue para la versión 12.2.55 - Comando oculto](#)
[Dispositivo IP que sigue para la versión 12.2.55 - IP estático ejemplo](#)
[Dispositivo IP que sigue para la versión 15.x](#)
[Dispositivo IP que sigue para el ® del Cisco IOS XE](#)
[Dispositivo IP que sigue con el 802.1x y DACL para la versión 12.2.55](#)
[Dispositivo IP que sigue con el 802.1x y DACL para la versión 15.x](#)
[Entrada ACL específica](#)
[Control-dirección](#)
[Dispositivo IP que sigue con el 802.1x y por usuario el ACL para la versión 15.x](#)
[Diferencia cuando está comparado al DACL](#)
[Dispositivo IP que sigue con el 802.1x y el id del filtro ACL para la versión 15.x](#)
[Seguimiento del dispositivo IP - Valores por defecto y mejores prácticas](#)
[Reescritura de la interfaz ACL para la versión 15.x](#)
[ACL predeterminado usado para el 802.1x](#)
[Abra el modo](#)
[Cuando la interfaz ACL es obligatoria](#)
[DACL en 4500/6500](#)
[Estatus de la dirección MAC para el 802.1x](#)
[Troubleshooting](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo la característica de seguimiento del dispositivo IP trabaja, que incluye cuáles son los activadores agregar y quitar un host. También, el impacto del dispositivo que sigue en la lista de control de acceso transferible del 802.1x (DACL) se explica. Los cambios del comportamiento entre las versiones y las Plataformas.

La segunda parte de que el documento se centra en la lista de control de acceso (ACL) devuelta

por el servidor del Authentication, Authorization, and Accounting (AAA) y aplicada al 802.1x la sesión. Una comparación entre el DACL, por usuario ACL y el id del filtro ACL se presenta. También, algunas advertencias con respecto a la reescritura ACL y el ACL predeterminado se discuten.

Teoría de seguimiento del dispositivo

El seguimiento del dispositivo agrega una entrada cuando:

- aprende la nueva entrada vía el snooping del DHCP.
- aprende la nueva entrada vía una petición de Address Resolution Protocol (ARP) (lee la dirección MAC del remitente y la dirección IP del remitente del paquete ARP). Que las funciones a veces están llamadas inspección ARP, pero le no es lo mismo que la inspección ARP dinámica (DAI). Que la característica está habilitada por abandono y no puede ser inhabilitada. También se llama snooping ARP, pero los debugs no lo mostrarán después de que “se habilite el snooping arp del debug”. El snooping ARP se habilita por abandono y no puede ser inhabilitado o ser controlado.

El seguimiento del dispositivo quita una entrada cuando no hay respuesta para un pedido ARP (que envía la sonda para cada host en el dispositivo que sigue la tabla, por abandono cada 30 segundos).

Configuración de seguimiento del dispositivo

```
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
```

Dispositivo que sigue las pruebas

```
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
```

Debugs de la versión 12.2.33, seguimiento del dispositivo IP actualizado por el snooping del DHCP

El snooping del DHCP puebla la tabla de vinculación:

```
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
```

Después de que el atar del DHCP se agregue a la base de datos, acciona la notificación para el seguimiento del dispositivo:

```
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
```

Las sondas ARP se envían por abandono cada 30 segundos:

```
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
```

Después de que la entrada se quite del dispositivo que sigue la tabla, el DHCP correspondiente que ata la entrada todavía está allí:

```
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
```

Hay el problema cuando usted tiene una respuesta ARP, pero el dispositivo que sigue la entrada se quita de todos modos. Que el bug aparece estar en la versión 12.2.33 y no ha aparecido en el software de la versión 12.2.55 o 15.x.

También hay algunas diferencias al dirigir con el puerto L2 (puerto de acceso) y el L3 vira hacia el lado de babor (ningún switchport).

Sonda y snooping ARP

Dispositivo que sigue con la característica del snooping ARP:

```
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
```

Dispositivo IP que sigue para la versión 12.2.55 - Comando oculto

Para la versión 12.2 pudo haber una necesidad de utilizar un comando oculto para activarla:

```
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
```

Dispositivo IP que sigue para la versión 12.2.55 - IP estático ejemplo

En este ejemplo, el PC se ha configurado con un IP Address estático. Los debugs muestran que después de que usted consiga una respuesta ARP (MSG=2), el dispositivo que sigue la entrada es actualizado.

```
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
```

Tan cada pedido ARP del PC pone al día el dispositivo que sigue la tabla (la dirección MAC del remitente y la dirección IP del remitente del paquete ARP).

Dispositivo IP que sigue para la versión 15.x

Es importante recordar que algunas de las características tales como DACL para el 802.1x no están soportadas en la versión LAN Lite (guárdese - el Cisco Feature Navigator no muestra siempre la información correcta).

El comando oculto de la versión 12.2 puede ser ejecutado, pero no tendrá ningún efecto. En la versión de software 15.x, el dispositivo IP que sigue (IPDT) por abandono se habilita solamente para las interfaces que tienen 802.1x habilitado:

```
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
```

Después de que el retiro de la configuración del 802.1x del puerto, IPDT también sea quitado de ese puerto. El estado del puerto pudo ser “TRAGAR”, así que es necesario tener el “acceso de modo del switchport” y “auto del puerto-control del authenticaion” para tener seguimiento del dispositivo IP activado en ese puerto. El límite máximo del dispositivo de la interfaz se establece a 10:

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

Dispositivo IP que sigue para el ® del Cisco IOS XE

Una vez más el comportamiento en el Cisco IOS XE 3.3 ha cambiado cuando está comparado a la versión deL Cisco IOS 15.x. El comando oculto de la versión 12.2 es Obsoleto, pero ahora este error será vuelto:

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

En el Cisco IOS XE, el seguimiento del dispositivo se activa para todas las interfaces (incluso las que no tienen 802.1x configurado):

```
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)
```

También, no hay límites para las entradas máximas por el puerto (0 significa discapacitado).

Dispositivo IP que sigue con el 802.1x y DACL para la versión 12.2.55

Si el 802.1x se configura con DACL, el dispositivo que sigue la entrada se utiliza para llenar la dirección IP del dispositivo. Este ejemplo muestra el trabajo de seguimiento del dispositivo para un IP estáticamente configurado:

```
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
```

Esto es una sesión del 802.1x construida con el “ICMP del permiso cualquier cualquier” DACL:

```
BSNS-3560-1# sh authentication sessions  interface fa0/1
           Interface:  FastEthernet0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.0.244
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  2
```

```
              ACS ACL:  xACSACLx-IP-DACL-516c2694
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A3042A900000008008900C5
     Acct Session ID:  0x0000000D
              Handle:  0x19000008

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

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

Esto muestra un ACL aplicado:

```
 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)
```

También, el ACL en la interfaz fa0/1 es lo mismo:

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

Aunque el valor por defecto es el dot1x ACL:

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

Puede ser que sea esperado para que el ACL utilice “ningunos” como 192.168.0.244. Que los trabajos como esto para el proxy del auth, sino para el src “ninguno” del 802.1x DACL no están cambiados al IP detectado del PC.

Para el proxy del auth, un ACL original del ACS se oculta y mostrado con el comando show ip access-list y (por usuario con el IP específico) un ACL específico se aplica en la interfaz con el comando de la interfaz fa0/1 de la lista de acceso del IP de la demostración. Sin embargo, el auténtico-proxy no utiliza el seguimiento IP del dispositivo.

¿Qué si la dirección IP no se detecta correctamente? Después de seguir del dispositivo se inhabilita:

```
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
```

Entonces no se asocia tan ninguna dirección IP, pero el DACL todavía se aplica:

```
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
```

En este escenario, el dispositivo que sigue para el 802.1x no se requiere. La única diferencia es ésa que conoce la dirección IP del cliente por adelantado se puede utilizar para un pedido de acceso RADIUS. Después del atributo 8 se asocia:

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

Existirá en el pedido de acceso y en el ACS será posible crear reglas más granulares de la autorización:

```
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
```

Tenga presente que TrustSec también necesita el dispositivo IP que sigue para el IP a los atascamientos SGT.

Dispositivo IP que sigue con el 802.1x y DACL para la versión 15.x

¿Cuál es la diferencia entre la versión 15.x y la versión 12.2.55 en DACL? En el software Version15.x, trabaja lo mismo que para el auténtico-proxy. El ACL genérico puede ser visto cuando ingresan al **comando show ip access-list** (respuesta ocultada del AAA), pero después de que el comando de la **interfaz fa0/1 de la lista de acceso del IP de la demostración**, el src "ninguno" es substituido por la dirección IP de origen del host (sabido vía el dispositivo IP que sigue).

Éste es el ejemplo para un teléfono y un PC en un puerto (g1/0/1), la versión de software 15.0.2SE2 en 3750X:

```
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
```

El teléfono se autentica vía puente de la autenticación de MAC (MAB), mientras que el PC utiliza el dot1x. El teléfono y el PC utilizan el mismo ACL:

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

Sin embargo, cuando está verificada en el nivel de la interfaz la fuente ha sido substituida por la dirección IP del dispositivo. Los activadores de seguimiento del dispositivo IP que cambian y ella pueden ocurrir en cualquier momento (mucho más adelante que la sesión de la autenticación y la descarga del ACL):

```
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
```

Ambas direcciones MAC se deben marcar como parásitos atmosféricos:

```
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
```

Entrada ACL específica

¿Cuándo la fuente “ninguna” en el DACL se substituye por la dirección IP del host? Solamente cuando hay por lo menos dos sesiones sobre el mismo puerto (dos suplicantes).

No hay necesidad de substituir la fuente “” cuando hay solamente una sesión. Los problemas pudieron aparecer cuando hay sesiones múltiples, y para no todos el seguimiento del dispositivo IP conoce la dirección IP del host. En ese escenario todavía será “ninguno” para algunas entradas.

Ese comportamiento es diferente en algunas Plataformas. Por ejemplo, en el 2960X con la versión 15.0(2)EX el ACL será siempre específico incluso cuando hay apenas una sesión de la autenticación por el puerto. Sin embargo, para la versión 15.0(2)SE 3560X y 3750X, usted necesita tener por lo menos dos sesiones para hacer ese específico ACL.

Control-dirección

Por abandono, la control-dirección es tipo ambos:

```
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
```

Eso significa que antes de que se autentique el supplicant, el tráfico no se puede enviar a o desde el puerto. Para “en” el modo, el tráfico se habría podido enviar del puerto al supplicant, pero no del supplicant al puerto (podría ser útil para la ESTELA en la característica LAN).

No obstante, el Switch aplica el ACL apenas en “en” la dirección. No importa se utiliza qué modo.

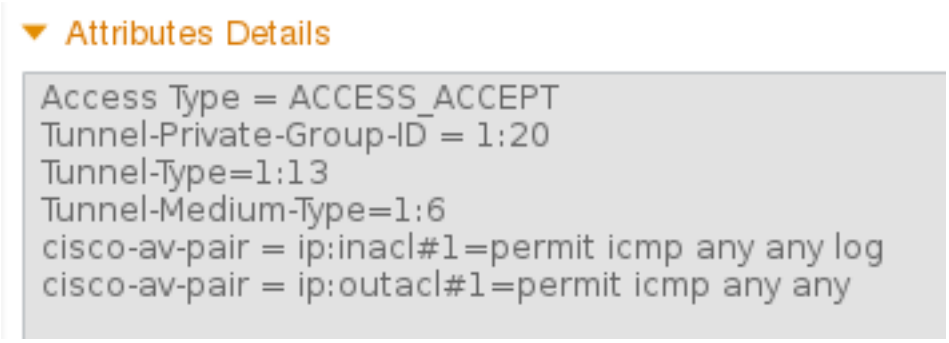
```
bsns-3750-5#sh ip access-lists interface g1/0/1 out
bsns-3750-5#sh ip access-lists interface g1/0/1 in
    permit ip host 192.168.2.200 any
    permit ip host 192.168.10.12 any
```

Eso significa básicamente que después de que la autenticación el ACL sea aplicada para el tráfico al puerto (en la dirección) y todo el tráfico se permite del puerto (hacia fuera dirección).

Dispositivo IP que sigue con el 802.1x y por usuario el ACL para la versión 15.x

Es también posible utilizar por usuario un ACL que se pase en IP del Cisco-av-pair “: inacl” y “IP: outacl”.

Este ejemplo de configuración es similar a una configuración previa, pero este vez el teléfono utiliza DACL y el PC utiliza por usuario el ACL. El perfil ISE para el PC es:



El teléfono todavía tiene el DACL aplicado:

```
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
```

Sin embargo, el PC en el mismo puerto utiliza por usuario el ACL:

```
    Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
          IP Address:  192.168.2.200
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  20
        Per-User ACL:  permit icmp any any log
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A800100000574311400B
     Acct Session ID:  0x000006D1
              Handle:  0x9D000568
```

Para verificar cómo eso se combina en el puerto gig1/0/1:

```
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
```

La primera entrada se ha tomado por usuario del ACL (nota la palabra clave del registro) y la segunda entrada se toma del DACL. Ambos ellos son reescritas por el dispositivo IP que sigue para la dirección IP específica.

Por usuario el ACL se podía verificar con el **comando all del epm del debug**:

```
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
```

Y también vía el **comando show ip access-lists**:

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

Qué sobre el IP: ¿atributo del outacl? Se omite totalmente en la versión 15.x. Se ha recibido el atributo, pero el Switch no hace aplicarse/proceso que atribuye.

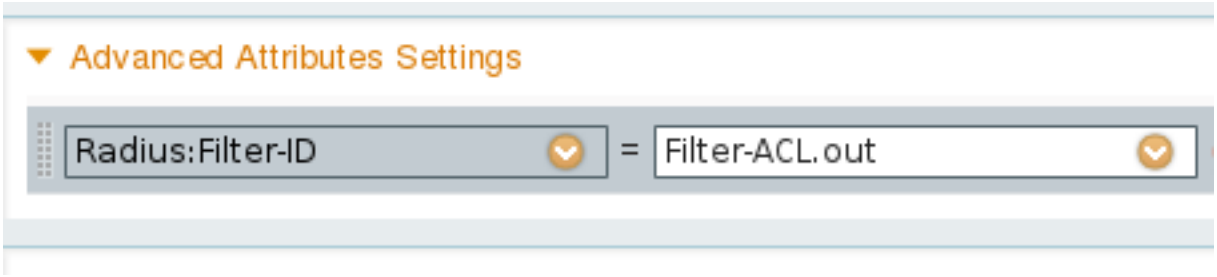
Diferencia cuando está comparado al DACL

Como se apunta en el Id. de bug Cisco CSCut25702, por usuario el ACL se comporta diferentemente que DACL. DACL con apenas una entrada (“IP cualquier ninguno del permiso”) y un supplicant conectado con un puerto puede trabajar correctamente sin el seguimiento del dispositivo IP habilitado. El “ningún” argumento no será substituido y todo el tráfico será permitido. Sin embargo, porque por usuario el ACL es obligatorio hacer el seguimiento del dispositivo IP habilitar. Si se inhabilita y tiene apenas el “IP del permiso cualquier cualquier” entrada y un supplicant, después todo el tráfico será bloqueado.

Dispositivo IP que sigue con el 802.1x y el id del filtro ACL para la versión 15.x

También, la filtro-identificación del atributo IETF [11] puede ser utilizada. El servidor de AAA vuelve el nombre ACL, que se debe definir localmente en el Switch. El perfil ISE podía parecer esto:

Observe que usted necesita specifiy la dirección (en o hacia fuera). Para eso es necesario agregar el atributo manualmente:



Entonces las demostraciones del debug:

```
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
```

Ese ACL también será mostrado para la sesión autenticada:

```
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
```

Y, pues el ACL es binded a la interfaz:

```
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
```

Observe que este ACL se puede combinar con otros tipos de ACL en la misma interfaz. Por ejemplo, teniendo en el mismo puerto del switch otro supplicant que consigue DACL del ISE: "IP cualquier ninguno del permiso" que usted podría ver:

```
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
```

Observe que el seguimiento del dispositivo IP reescribe el IP de la fuente para cada fuente (supplicant).

¿Qué sobre "hacia fuera" la lista de filtros? Otra vez (como por usuario ACL), no será utilizada por el Switch.

Seguimiento del dispositivo IP - Valores por defecto y mejores prácticas

Para las versiones anterior que 15.2(1)E, antes de que cualquier característica pueda utilizar IPDT él necesita ser habilitado global primero con este comando CLI:

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

Para las versiones 15.2(1)E y posterior, el comando de **seguimiento del dispositivo del IP** no se necesita más. Se habilita IPDT solamente si una característica que confía en él lo habilita. Si ninguna característica habilita IPDT, se inhabilita IPDT. El "ningún comando de seguimiento del dispositivo del IP" no tiene ningún efecto. La característica específica tiene habilitar/neutralización IPDT del control.

Cuando usted habilita IPDT, usted tiene que recordar sobre el problema de la "dirección IP duplicada" encendido. Vea de "los mensajes de error 0.0.0.0 de la dirección IP duplicada" del Troubleshooting para más información.

Se recomienda para inhabilitar IPDT en un puerto troncal:

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

En el Cisco IOS posterior, es un diverso comando:

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

Se recomienda para permitir a IPDT en el puerto de acceso y las sondas del retardo ARP para evitar el problema de la "dirección IP duplicada":

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

Reescritura de la interfaz ACL para la versión 15.x

Para la interfaz ACL, trabaja antes de la autenticación:

```
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
```

Sin embargo, después de que la autenticación tenga éxito es reescrita (invalidación) por el ACL vuelto del servidor de AAA (no importa si es DACL, IP: inacl, o filterid).

Ese ACL (test1) puede bloquear el tráfico (que sería permitido normalmente en el modo abierto), pero después de que no importe la autenticación más. Incluso cuando no se vuelve ningún ACL del servidor de AAA, la interfaz ACL está sobregrabada y se proporciona el acceso total. Eso es un bit que se engaña puesto que el Ternary Content Addressable Memory (TCAM) indica que el ACL es todavía binded en el nivel de la interfaz. Aquí está un ejemplo de la versión 15.2.2 en 3750X:

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

Port based ACL: (asic 1)
---------------------------
 Input Label:  5    Op Select Index: 255
   Interface(s): Gi1/0/2
   Access Group: test1, 4 VMRs
   Ip Portal: 0 VMRs
   IP Source Guard: 0 VMRs
   LPIP: 0 VMRs
   AUTH: 0 VMRs
   C3PLACL: 0 VMRs
   MAC Access Group: (none), 0 VMRs
```

Esa información es válida solamente para el nivel de la interfaz, no para el nivel de la sesión. Más información (presenta un ACL compuesto) se puede deducir de:

```
bsns-3750-6#show ip access-lists interface g1/0/2
    permit ip host 192.168.1.203 any
Extended IP access list test1
    10 permit icmp host 2.2.2.2 host 1.1.1.1
```

La primera entrada se crea como “IP del permiso que cualquier cualquier” DACL se vuelve para la autenticación satisfactoria (y “” es substituido por una entrada del dispositivo que sigue la tabla). La segunda entrada es el resultado de la interfaz ACL y es aplicada para todas las nuevas autenticaciones (antes de la autorización).

Desafortunadamente, (otra vez dependiente de la plataforma) se concatenan ambos ACL. Eso sucede en la versión 15.2.2 en 3750X. Eso significa eso para la sesión autorizada, ambos ellos es aplicado. Primero el DACL y segundo la interfaz ACL. Por eso cuando usted agrega el “deny ip any any explícito”, el DACL no tomará en la consideración la interfaz ACL. Generalmente hay no explícito niega en el DACL y entonces la interfaz ACL es aplicada después que.

El comportamiento para la versión 15.0.2 en 3750X es lo mismo, pero el **comando interface sh de la lista de acceso del IP** no muestra la interfaz ACL más (solamente él todavía será concatenado con la interfaz ACL a menos que sea explícito niegan en el DACL existe).

ACL predeterminado usado para el 802.1x

Hay dos tipos del valor por defecto ACL:

- Auténtico-valor por Defecto-ACL-ABIERTO - utilizado para el modo abierto
- Auténtico-valor por defecto-ACL - usado para el acceso cerrado

Se utilizan el auténtico-valor por defecto-ACL y auténtico-valor por defecto-ACL-ABIERTOS cuando el puerto está en el estado desautorizado. Por abandono, se utiliza el acceso cerrado. Eso significa que antes de que se caiga la autenticación todo el tráfico a menos que el permitiera por el auténtico-valor por defecto-ACL. Este tráfico del DHCP de la manera se permite antes de la autorización exitosa. Se afecta un aparato la dirección IP y el DACL descargado puede ser aplicado correctamente. Que el ACL está creado automáticamente y no se puede encontrar en la configuración.

```
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
```

Se crea dinámicamente para la primera autenticación (entre la fase de la autenticación y autorización) y se quita después de que se quite la sesión más reciente.

El Auténtico-Valor por defecto-ACL permite solamente el tráfico del DHCP. Después de que la autenticación tenga éxito y se descarga el nuevo DACL, se aplica a esa sesión. Cuando aparece el modo se cambia para abrir auténtico-valor por defecto-ACL-ABIERTO y se utiliza y trabaja de la misma manera como Auténtico-Valor por defecto-ACL:

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

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

Ambos ACL pueden ser personalizados, pero nunca serán vistos en la configuración.

```
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#
```

Abra el modo

La sección anterior describió el comportamiento para ACL (que incluye el que está usado por abandono para el modo abierto). El comportamiento para el modo abierto es:

- permite todo el tráfico (según el valor por defecto auténtico-valor por defecto-ACL-ABIERTO) cuando la sesión está en un estado desautorizado.
- la sesión está en un estado desautorizado durante la autenticación/la autorización (buenas para los escenarios del inicio del modelo E (PXE) del dispositivo) del cifrado o ese proceso falla después (bueno para los escenarios llamados “modo bajo del impacto”).
- cuando la sesión se mueve al estado autorizado para las plataformas múltiples, se concatenan los ACL y se utiliza el primer DACL, después la interfaz ACL.
- para el multi-auth o el multi-dominio pudo haber sesiones múltiples al mismo tiempo en diversos estados (entonces el diverso tipo ACL solicitará cada sesión).

Cuando la interfaz ACL es obligatoria

Para el múltiplo 6500/4500 Plataformas, la interfaz ACL es obligatoria para aplicar el DACL correctamente.

Aquí está un ejemplo con 4500 sup2 12.2.53SG6, ninguna interfaz ACL:

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

Entonces después de que se autentique el host, se descarga el DACL. No será aplicado y la autorización falla.

```
*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
```

Después de la interfaz se agrega el ACL:

```
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
```

La autenticación y autorización tendrá éxito y el DACL será aplicado correctamente:

```
brisk#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE    Authz Success  0A3043450000000008001A2CE4
```

El comportamiento no es dependiente en la “autenticación abierta”. Para validar el DACL, usted necesita la interfaz ACL para ambos abre/cerró el modo.

DACL en 4500/6500

En el 4500/6500, el DACL se aplica con el acl_snoop DACLs. Un ejemplo con 4500 sup2 12.2.53SG6 (teléfono + PC) se muestra aquí. Hay un ACL separado para la Voz (10) y VLA N de los datos (100):

```
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
```

Los ACL son específicos porque IPDT tiene las entradas correctas:

```
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
```

Las sesiones autenticadas confirman los direccionamientos:

```
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
```

En esta etapa el PC y el teléfono responde al eco ICMP, pero a los presentes de la interfaz ACL

solamente:

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

¿por qué? Porque el DACL se ha avanzado solamente para el teléfono (192.168.10.12). Para el PC, la interfaz ACL con el modo abierto se utiliza:

```
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)
```

En resumen, el acl_snoop será creado para el PC y el teléfono, pero el DACL se vuelve apenas para el teléfono. Ése es porqué ese ACL se ve como binded a la interfaz.

Estatus de la dirección MAC para el 802.1x

Cuando la autenticación del 802.1x comienza, la dirección MAC todavía se considera como DINÁMICO pero la acción para ese paquete es DESCENSO:

```
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
```

Después de que se convierta la autenticación satisfactoria la dirección MAC se proporciona los parásitos atmosféricos y el número del puerto:

```
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
```

Eso es verdad para toda la sesión mab/dot1x para ambos dominios (VOICE/DATA).

Troubleshooting

Recuerde leer la guía de configuración del 802.1x para su versión de software y plataforma específicas.

Si usted abre un caso TAC, proporcione la salida de estos comandos:

- show tech
- muestre el detalle del <xx> de la interfaz de la sesión de la autenticación
- muestre el <xx> de la interfaz de la tabla de direcciones del mac

Es también bueno recoger una captura de paquetes del puerto SPAN y estos debugs:

- radio del debug prolijo
- epm todo del debug
- debug authentication todo
- dot1x todo del debug
- <yy> todo de la característica del debug authentication
- debug aaa authentication
- **debug aaa authorization**

Información Relacionada

- servicios de autenticación guía de configuración del 802.1x, versión 3SE (Catalyst 3850 Switch) del Cisco IOS XE
- Catalyst 3750-X y guía de configuración de software del Catalyst 3560-X Switch, Cisco IOS Release 15.2(1)E
- Guía de configuración de software 3750-X y 3560-X del Catalyst, versión 15.0(1)SE
- Guía de configuración de software del Catalyst 3560, versión 12.2(52)SE
- Soporte Técnico y Documentación - Cisco Systems