

Comprensión del comportamiento de seguimiento de dispositivos, ID de filtro, ACL por usuario y DACL 802.1x

Contenido

[Introducción](#)

[Teoría del seguimiento de dispositivos](#)

[Configuración de rastreo de dispositivos](#)

[Pruebas de rastreo de dispositivos](#)

[Depuraciones de la versión 12.2.33, seguimiento de dispositivos IP actualizado por indagación DHCP](#)

[Sondeo y indagación ARP](#)

[Seguimiento de Dispositivos IP para la Versión 12.2.55 - Comando Oculto](#)

[Ejemplo de Seguimiento de Dispositivos IP para la Versión 12.2.55 - IP Estática](#)

[Seguimiento de dispositivos IP para la versión 15.x](#)

[Seguimiento de dispositivos IP para Cisco IOS-XE®](#)

[Seguimiento de dispositivos IP con 802.1x y DACL para la versión 12.2.55](#)

[Seguimiento de dispositivos IP con 802.1x y DACL para la versión 15.x](#)

[Entrada de ACL específica](#)

[Dirección de control](#)

[Seguimiento de dispositivos IP con 802.1x y ACL por usuario para la versión 15.x](#)

[Diferencia con respecto a la DACL](#)

[Seguimiento de dispositivos IP con 802.1x y ACL con ID de filtro para la versión 15.x](#)

[Seguimiento de dispositivos IP: valores predeterminados y prácticas recomendadas](#)

[Reescritura de ACL de Interfaz para la Versión 15.x](#)

[ACL predeterminada utilizada para 802.1x](#)

[Modo abierto](#)

[Cuando la ACL de Interfaz es Obligatoria](#)

[DACL en 4500/6500](#)

[Estado de la dirección MAC para 802.1x](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la función de seguimiento de dispositivos IP, los activadores para agregar y quitar un host y el impacto del seguimiento de dispositivos en la DACL 802.1x.

Teoría del seguimiento de dispositivos

En este documento se describe cómo funciona el seguimiento de dispositivos IP, que incluye los activadores para agregar y eliminar un host.

Además, se explica el impacto del seguimiento de dispositivos en la lista de control de acceso descargable (DACL) 802.1x.

El comportamiento cambia entre las versiones y las plataformas.

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

autenticación, autorización y contabilidad (AAA) y aplicada a la sesión 802.1x.

Se presenta una comparación entre la DACL, la ACL por usuario y la ACL con ID de filtro.

Además, se discuten algunas advertencias con respecto a la reescritura de ACL y la ACL predeterminada.

El seguimiento de dispositivos agrega una entrada cuando:

- aprende la nueva entrada a través de la indagación DHCP.
- aprende la nueva entrada a través de una solicitud de protocolo de resolución de direcciones (ARP) (lee la dirección MAC del remitente y la dirección IP del remitente del paquete ARP).

Esta funcionalidad se denomina a veces inspección ARP, pero no es la misma que Inspección ARP dinámica (DAI).

Esta función está activada de forma predeterminada y no se puede desactivar. También se denomina indagación ARP, pero las depuraciones no la muestran después de habilitar "debug arp snooping".

La indagación ARP está habilitada de forma predeterminada y no se puede deshabilitar ni controlar.

El seguimiento de dispositivos elimina una entrada cuando no hay respuesta para una solicitud ARP (enviando sonda para cada host en la tabla de seguimiento de dispositivos, de forma predeterminada cada 30 segundos).

Configuración de rastreo de dispositivos

```
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
```

Pruebas de rastreo de dispositivos

```
<#root>
```

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

```
show ip dhcp binding
```

IP address	Client-ID/ Hardware address	Lease expiration	Type
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
```

Depuraciones de la versión 12.2.33, seguimiento de dispositivos IP actualizado por indagación DHCP

La indagación DHCP rellena la tabla de enlace:

<#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: DHCP Snooping(hlfm_set_if_input): Setting if_input to Fa0/1 for pak. Was V11
02:31:12: DHCP Snooping(hlfm_set_if_input): Setting if_input to V11 for pak. Was Fa0/1
02:31:12: DHCP Snooping(hlfm_set_if_input): Setting if_input to Fa0/1 for pak. Was V11
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    Id Type=dhcp-snooping Vlan=1 If=FastEthernet0/1
```

Después de agregar el enlace DHCP a la base de datos, se activa la notificación para el seguimiento de dispositivos:

```
<#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

Los sondeos ARP se envían de forma predeterminada cada 30 segundos:

<#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	

Una vez que se elimina la entrada de la tabla de seguimiento de dispositivos, la entrada de enlace DHCP correspondiente permanece allí:

<#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/ Hardware address	Lease expiration	Type
192.168.0.241	0100.5056.994e.a1	Mar 02 1993 03:06 AM	Automatic

Existe el problema cuando tiene una respuesta ARP, pero la entrada de seguimiento del dispositivo se elimina de todos modos.

Ese bug parece estar en la versión 12.2.33 y no ha aparecido en la versión 12.2.55 o 15.x del software.

También hay algunas diferencias al manejar con el puerto L2 (puerto de acceso) y el puerto L3 (sin puerto de switch).

Sondeo y indagación ARP

Seguimiento de dispositivos con la función de indagación ARP:

```
<#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
```

Seguimiento de Dispositivos IP para la Versión 12.2.55 - Comando Oculto

Para la versión 12.2, utilice un comando oculto para activarla:

```
<#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
```

Ejemplo de Seguimiento de Dispositivos IP para la Versión 12.2.55 - IP Estática

En este ejemplo, el PC se ha configurado con una dirección IP estática. Las depuraciones muestran que después de obtener una respuesta ARP (MSG=2), se actualiza la entrada de seguimiento del dispositivo.

```
<#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
```

Por lo tanto, cada solicitud ARP de la PC actualiza la tabla de seguimiento de dispositivos (la dirección MAC del remitente y la dirección IP del remitente del paquete ARP).

Seguimiento de dispositivos IP para la versión 15.x

Es importante recordar que algunas de las funciones, como DACL para 802.1x, no son compatibles con la versión de LAN Lite (tenga en cuenta que Cisco Feature Navigator no siempre muestra la información correcta).

El comando oculto de la versión 12.2 se puede ejecutar, pero no tiene ningún efecto. En la versión de software 15.x, el seguimiento de dispositivos IP (IPDT) está habilitado de forma predeterminada sólo para las interfaces que tienen habilitado 802.1x:

```
<#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
```

Después de quitar la configuración 802.1x del puerto, IPDT también se quita de ese puerto.

Es posible que el estado del puerto sea "INACTIVO", por lo que es necesario tener "acceso en modo de puerto de switch" y "autenticación automática de control de puerto" para tener activado el seguimiento de dispositivos IP en ese puerto.

El límite máximo de dispositivos de interfaz se establece en 10:

```
<#root>
```

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

```
ip device tracking maximum
```

```
?
```

```
<1-10> Maximum devices
```

Seguimiento de dispositivos IP para Cisco IOS-XE®

Una vez más, el comportamiento en Cisco IOS-XE 3.3 ha cambiado en comparación con la versión 15.x del IOS de Cisco.

El comando oculto de la versión 12.2 está obsoleto, pero ahora se devuelve este error:

```
<#root>
```

```
3850-1#
```

```
no ip device tracking int g1/0/48
```

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

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

```
<#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)

```

Además, no hay límites para las entradas máximas por puerto (0 significa inhabilitado).

Seguimiento de dispositivos IP con 802.1x y DACL para la versión 12.2.55

Si 802.1x se configura con DACL, se utiliza la entrada de seguimiento del dispositivo para llenar la

dirección IP del dispositivo.

Este ejemplo muestra el funcionamiento del seguimiento de dispositivos para una IP configurada estáticamente:

```
<#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
```

Esta es una sesión 802.1x construida con DACL "permit icmp any any":

```
<#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

Esto muestra una ACL aplicada:

<#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)
```

Además, la ACL en la interfaz fa0/1 es la misma:

<#root>

BSNS-3560-1#

show ip access-lists interface fa0/1

```
permit icmp any any
```

Aunque el valor predeterminado es dot1x ACL:

```
<#root>
```

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

```
show ip interface fa0/1
```

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

Se espera que la ACL utilice "any" como **192.168.0.244**. Esto funciona así para el proxy de autenticación, pero para 802.1x DACL src "any" no se cambia a la IP detectada del PC.

Para el proxy de autenticación, una ACL original del ACS se almacena en caché y se muestra con el comando **show ip access-list** y una ACL específica (por usuario con IP específica) se aplica en la interfaz con el comando **show ip access-list interface fa0/1**. Sin embargo, auth-proxy no utiliza el seguimiento de IP del dispositivo.

¿Qué sucede si la dirección IP no se detecta correctamente? Después de deshabilitar el seguimiento de dispositivos:

```
<#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: 0A3042A900000000000000C775  
Acct Session ID: 0x00000001  
Handle: 0xB0000000
```

```
Runnable methods list:  
Method State
```

```
dot1x Authc Success
```

Por lo tanto, no se adjunta ninguna dirección IP, pero se sigue aplicando la DACL:

```
<#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
```

En esta situación, no se requiere el seguimiento de dispositivos para 802.1x. La única diferencia es que conocer la dirección IP del cliente por adelantado se puede utilizar para una solicitud de acceso RADIUS. Después de adjuntar el atributo 8:

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

Existe en Access-Request y en ACS es posible crear reglas de autorización más granulares:

```
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 en cuenta que TrustSec también necesita el seguimiento de dispositivos IP para las vinculaciones de IP a SGT.

Seguimiento de dispositivos IP con 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 la versión de software 15.x, funciona igual que para auth-proxy.

La ACL genérica se puede ver cuando se ingresa el comando **show ip access-list** (respuesta en caché de AAA), pero después del comando **show ip access-list interface fa0/1**, el src "any" se reemplaza por la dirección IP de origen del host (conocida a través del seguimiento de dispositivos IP).

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

<#root>

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

Interface: GigabitEthernet1/0/1
MAC Address:

0007.5032.6941

IP Address:

192.168.10.12

User-Name: 00-07-50-32-69-41
Status: Authz Success
Domain:

VOICE

Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy:

100

ACS ACL:

xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2

Session timeout: N/A
Idle timeout: N/A
Common Session ID: C0A80001000001012B680D23
Acct Session ID: 0x0000017B
Handle: 0x99000102

Runnable methods list:

Method	State
dot1x	Failed over

mab

Authc Success

Interface: GigabitEthernet1/0/1
MAC Address:

0050.5699.4ea1

IP Address:

192.168.2.200

User-Name:

cisco

Status: Authz Success

Domain:

DATA

Security Policy: Should Secure

Security Status: Unsecure

Oper host mode: multi-auth

Oper control dir: both

Authorized By: Authentication Server

Vlan Policy:

20

ACS ACL:

xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2

Session timeout: N/A

Idle timeout: N/A

Common Session ID: C0A80001000001BD336EC4D6

Acct Session ID: 0x000002F9

Handle: 0xF80001BE

Runnable methods list:

Method State

dot1x Authc Success

mab Not run

El teléfono se autentica mediante la derivación de autenticación MAC (MAB), mientras que el PC utiliza dot1x. Tanto el teléfono como el PC utilizan la misma ACL:

<#root>

bsns-3750-5#

show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2

Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2 (

per-user

)

10

```
permit ip any any
```

Sin embargo, cuando se verifica en el nivel de interfaz, la fuente se ha reemplazado por la dirección IP del dispositivo.

El seguimiento de dispositivos IP desencadena ese cambio y puede ocurrir en cualquier momento (mucho más tarde que la sesión de autenticación y la descarga de la ACL):

```
<#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
```

Ambas direcciones MAC están marcadas como estáticas:

```
<#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
```

Entrada de ACL específica

¿Cuándo se reemplaza el "cualquiera" de origen en la DACL por la dirección IP del host? Solo cuando hay al menos dos sesiones en el mismo puerto (dos suplicantes).

No es necesario reemplazar el origen "any" cuando solo hay una sesión.

Los problemas aparecen cuando hay varias sesiones y, para no todas ellas, el seguimiento del dispositivo IP conoce la dirección IP del host. En ese escenario sigue siendo "cualquiera" para algunas entradas.

Ese comportamiento es diferente en algunas plataformas. Por ejemplo, en el 2960X con la versión 15.0(2)EX, la ACL siempre es específica, incluso cuando solo hay una sesión de autenticación por puerto.

Sin embargo, para los 3560X y 3750X versión 15.0(2)SE, debe tener al menos dos sesiones para que esa ACL sea específica.

Dirección de control

De forma predeterminada, la dirección de control es del tipo:

```
<#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
```

Esto significa que antes de que el solicitante sea autenticado, el tráfico no puede ser enviado hacia o desde el puerto. Para el modo "in", el tráfico podría haberse enviado del puerto al suplicante, pero no del suplicante al puerto (podría ser útil para la función WAKE on LAN).

Aún así, el switch aplica la ACL justo en la dirección "en". No importa qué modo se utilice.

```
<#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
```

Básicamente, esto significa que después de la autenticación, la ACL se aplica para el tráfico al puerto (en dirección) y todo el tráfico se permite desde el puerto (dirección de salida).

Seguimiento de dispositivos IP con 802.1x y ACL por usuario para la versión 15.x

También es posible utilizar una ACL por usuario que se pasa en cisco-av-pair "ip:inacl" e "ip:outacl".

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

▼ Attributes Details

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

El teléfono todavía tiene la DACL aplicada:

<#root>

bsns-3750-5#

show authentication sessions interface g1/0/1

```
Interface: GigabitEthernet1/0/1
MAC Address: 0007.5032.6941
IP Address:
```

192.168.10.12

```
User-Name: 00-07-50-32-69-41
Status: Authz Success
Domain:
```

VOICE

```
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 100
ACS ACL:
```

xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2

```
Session timeout: N/A
Idle timeout: N/A
Common Session ID: C0A8000100000568431143D8
Acct Session ID: 0x000006D2
Handle: 0x84000569
```

Runnable methods list:

```
Method  State
dot1x   Failed over
mab     Authc Success
```

bsns-3750-5#

```
sh ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
```

```
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2 (per-user)
10
```

```
permit ip any any
```

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

<#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: C0A80001000005674311400B
Acct Session ID: 0x000006D1
Handle: 0x9D000568
```

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

<#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
```

La primera entrada se tomó de la ACL por usuario (observe la palabra clave log) y la segunda entrada se tomó de la DACL.

Ambos se reescriben mediante el seguimiento de dispositivos IP para la dirección IP específica.

La ACL por usuario se pudo verificar con el comando **debug epm all**:

```
<#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
```

Y también a través del comando **show ip access-lists**:

```
<#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
```

¿Qué ocurre con el atributo ip:outacl? Se omite por completo en la versión 15.x. El atributo ha sido recibido, pero el switch no aplica/procesa ese atributo.

Diferencia con respecto a la DACL

Como se indicó en el ID de bug de Cisco [CSCut25702](#), la ACL por usuario se comporta de manera diferente que la DACL.

La DACL con una sola entrada ("permit ip any any") y un suplicante conectado a un puerto puede funcionar correctamente sin el seguimiento de dispositivos IP habilitado.

El argumento "any" no se sustituye y se permite todo el tráfico. Sin embargo, para la ACL por usuario es obligatorio tener habilitado el seguimiento de dispositivos IP.

Si está inhabilitado y solo tiene la entrada "permit ip any any" y un suplicante, todo el tráfico se bloquea.

Seguimiento de dispositivos IP con 802.1x y ACL con ID de filtro para la versión 15.x

Además, se puede utilizar el atributo de IETF filter-id [11]. El servidor AAA devuelve el nombre ACL, que se define localmente en el switch. El perfil de ISE podría tener este aspecto:



▼ Common Tasks

DACL Name

VLAN Tag ID 1 Edit Tag ID/Name 20

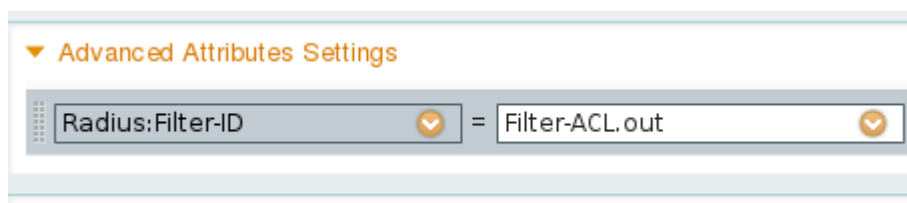
Voice Domain Permission

Web Authentication

Auto Smart Port

Filter-ID Filter-ACL.in

Tenga en cuenta que debe especificar la dirección (hacia dentro o hacia fuera). Para eso es necesario agregar el atributo manualmente:



▼ Advanced Attributes Settings

Radius:Filter-ID = Filter-ACL.out

Luego, el comando debug muestra:

```
<#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
```

Esa ACL también se muestra para la sesión autenticada:

<#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
```

Y, como la ACL está enlazada a la interfaz:

<#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
```

Tenga en cuenta que esta ACL se puede combinar con otros tipos de ACL en la misma interfaz. Por ejemplo, si tiene en el mismo puerto de switch otro suplicante que obtiene DACL de ISE: "permit ip any any", podría ver:

<#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
```

Tenga en cuenta que el seguimiento de dispositivos IP reescribe la IP de origen para cada origen (solicitante).

¿Qué pasa con la lista de filtros "fuera"? De nuevo (como ACL por usuario), el switch no la utiliza.

Seguimiento de dispositivos IP: valores predeterminados y prácticas recomendadas

Para las versiones anteriores a 15.2(1)E, antes de que cualquier función pueda utilizar IPDT, debe activarse globalmente primero con este comando CLI:

```
<#root>
```

```
(config)#
```

```
ip device tracking
```

Para las versiones 15.2(1)E y posteriores, el comando **ip device tracking** ya no es necesario. IPDT se habilita sólo si una función que depende de ella lo habilita.

Si ninguna función activa IPDT, IPDT se desactiva. El comando "no ip device tracking" no tiene ningún efecto. La función específica tiene el control para habilitar/deshabilitar IPDT.

Cuando habilite IPDT, debe recordar el problema "Duplicar dirección IP" en . Consulte [Troubleshooting de Mensajes de Error "Duplicate IP Address 0.0.0.0"](#) para obtener más información.

Se recomienda inhabilitar IPDT en un puerto trunk:

```
<#root>
```

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

```
no ip device tracking
```

En el último Cisco IOS, es un comando diferente:

```
<#root>
```

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

```
ip device tracking maximum 0
```

Se recomienda habilitar IPDT en el puerto de acceso y demorar los sondeos ARP para evitar el problema de "Dirección IP duplicada":

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

Reescritura de ACL de Interfaz para la Versión 15.x

Para la ACL de interfaz, funciona antes de la autenticación:

```
<#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
```

Sin embargo, después de que la autenticación sea exitosa, la ACL devuelta desde el servidor AAA la reescribe (invalida) (no importa si es DACL, ip:inacl o filterid).

Esa ACL (prueba 1) puede bloquear el tráfico (que normalmente se permitiría en el modo abierto), pero después de la autenticación, ya no importa.

Incluso cuando no se devuelve ninguna ACL del servidor AAA, se sobrescribe la ACL de interfaz y se proporciona acceso completo.

Esto es un poco engañoso ya que la Memoria Direccionable de Contenido Ternario (TCAM) indica que la ACL todavía está enlazada en el nivel de interfaz.

Este es un ejemplo de la versión 15.2.2 en 3750X:

```
<#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
```

Esa información es válida solamente para el nivel de interfaz, no para el nivel de sesión. Se puede deducir algo más de información (presenta una ACL compuesta) de:

```
<#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
```

La primera entrada se crea cuando se devuelve la DACL "permit ip any any" para una autenticación correcta (y "any" se sustituye por una entrada de la tabla de seguimiento de dispositivos).

La segunda entrada es el resultado de la ACL de la interfaz y se aplica para todas las nuevas autenticaciones (antes de la autorización).

Desafortunadamente, (de nuevo, depende de la plataforma) ambas ACL están concatenadas. Esto sucede en la versión 15.2.2 en 3750X.

Esto significa que para una sesión autorizada, se aplican ambos. Primero la DACL y luego la ACL de interfaz.

Es por eso que cuando agrega "deny ip any any" explícito, la DACL no tiene en cuenta la ACL de la interfaz.

Por lo general, no hay una negación explícita en la DACL y luego se aplica la ACL de interfaz después de eso.

El comportamiento para la versión 15.0.2 en 3750X es el mismo, pero el comando **sh ip access-list interface** ya no muestra la ACL de la interfaz (pero sigue concatenada con la ACL de la interfaz a menos que exista una negación explícita en la DACL).

ACL predeterminada utilizada para 802.1x

Existen dos tipos de ACL predeterminadas:

- auth-default-ACL-OPEN: se utiliza para el modo abierto
- auth-default-ACL: se utiliza para el acceso cerrado

Tanto auth-default-ACL como auth-default-ACL-OPEN se utilizan cuando el puerto se encuentra en estado no autorizado. De forma predeterminada, se utiliza el acceso cerrado.

Esto significa que antes de la autenticación todo el tráfico se descarta excepto el permitido por auth-default-ACL.

De esta manera, el tráfico DHCP se permite antes de la autorización exitosa.

La dirección IP está asignada y la DACL descargada se puede aplicar correctamente.

Esa ACL se crea automáticamente y no se puede encontrar en la configuración.

```
<#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
```

Se crea dinámicamente para la primera autenticación (entre la fase de autenticación y la de autorización) y se elimina después de que se elimina la última sesión.

Auth-Default-ACL permite sólo el tráfico DHCP. Una vez que la autenticación se realiza correctamente y se descarga la nueva DACL, se aplica a esa sesión.

Cuando se cambia el modo para abrir auth-default-ACL-OPEN aparece y se utiliza y funciona exactamente

de la misma manera que Auth-Default-ACL:

```
<#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
```

Ambas ACL se pueden personalizar, pero nunca se ven en la configuración.

```
<#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#
```

Modo abierto

En la sección anterior se describió el comportamiento de las ACL (que incluye la que se utiliza de forma predeterminada para el modo abierto). El comportamiento para el modo abierto es:

- permite todo el tráfico (según default auth-default-ACL-OPEN) cuando la sesión se encuentra en un estado no autorizado.
- la sesión se encuentra en un estado no autorizado durante la autenticación/autorización (adecuado para

los escenarios de arranque del dispositivo de cifrado modelo E (PXE)) o después de que el proceso falle (adecuado para los escenarios denominados "modo de bajo impacto").

- cuando la sesión se mueve al estado autorizado para varias plataformas, las ACL se concatenan y se utiliza la primera DACL y, a continuación, la ACL de interfaz.
- para multi-auth o multi-domain posiblemente hay varias sesiones al mismo tiempo en diferentes estados (entonces el tipo de ACL diferente se aplica para cada sesión).

Cuando la ACL de Interfaz es Obligatoria

Para varias plataformas 6500/4500, la ACL de interfaz es obligatoria para aplicar la DACL correctamente.

Aquí hay un ejemplo con 4500 sup2 12.2.53SG6, sin ACL de interfaz:

```
<#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
```

Después de autenticar el host, se descarga la DACL. No se aplica y la autorización falla.

```
<#root>
*Apr 25 04:38:05.239: RADIUS: Received from id 1645/19 10.48.66.74:1645,
Access-Accept,
len 209
*Apr 25 04:38:05.239: RADIUS: authenticator 35 8E 59 E4 D5 CF 8F 9A -
EE 1C FC 5A 9F 67 99 B2
*Apr 25 04:38:05.239: RADIUS: User-Name [1] 41
"
#ACSAcl#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
"
*Apr 25 04:38:05.239: RADIUS: State [24] 40
*Apr 25 04:38:05.239: RADIUS: 52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 61
[ReauthSession:0a]
*Apr 25 04:38:05.239: RADIUS: 33 30 34 32 34 61 30 30 30 45 46 35 30 46 35 33
[30424a000EF50F53]
*Apr 25 04:38:05.239: RADIUS: 35 41 36 36 39 33 [ 5A6693]
*Apr 25 04:38:05.239: RADIUS: Class [25] 54
*Apr 25 04:38:05.239: RADIUS: 43 41 43 53 3A 30 61 33 30 34 32 34 61 30 30 30
```

```

[CACS:0a30424a000]
*Apr 25 04:38:05.239: RADIUS: 45 46 35 30 46 35 33 35 41 36 36 39 33 3A 69 73
[EF50F535A6693:is]
*Apr 25 04:38:05.239: RADIUS: 65 32 2F 31 38 30 32 36 39 35 33 38 2F 31 32 38
[e2/180269538/128]
*Apr 25 04:38:05.239: RADIUS: 36 35 35 33 [ 6553]
*Apr 25 04:38:05.239: RADIUS: Message-Authenticato[80] 18
*Apr 25 04:38:05.239: RADIUS: AF 47 E2 20 65 2F 59 39 72 9A 61 5C C5 8B ED F5
[ G e/Y9ra\]
*Apr 25 04:38:05.239: RADIUS: Vendor, Cisco [26] 36
*Apr 25 04:38:05.239: RADIUS: Cisco AVpair [1] 30
"

```

```
ip:inacl#1=permit ip any any
```

```

"
*Apr 25 04:38:05.239: RADIUS(00000000): Received from id 1645/19
*Apr 25 04:38:05.247:

```

```
EPM_SESS_ERR:Failed to apply ACL to interface
```

```

*Apr 25 04:38:05.247: EPM_API:In function epm_send_message_to_client
*Apr 25 04:38:05.247: EPM_SESS_EVENT:Sending response message to process
AUTH POLICY Framework
*Apr 25 04:38:05.247: EPM_SESS_EVENT:Returning feature config
*Apr 25 04:38:05.247: EPM_API:In function epm_acl_feature_free
*Apr 25 04:38:05.247: EPM_API:In function epm_policy_aaa_response
*Apr 25 04:38:05.247: EPM_FSM_EVENT:Event epm_ip_wait_event state changed from
policy-apply to ip-wait
*Apr 25 04:38:05.247: EPM_API:In function epm_session_action_ip_wait
*Apr 25 04:38:05.247: EPM_API:In function epm_send_ipwait_message_to_client
*Apr 25 04:38:05.247: EPM_SESS_ERR:NULL feature list for client ctx 1B2694B0
for type DOT1X
*Apr 25 04:38:05.247:

```

```

%AUTHMGR-5-FAIL: Authorization failed for client
(0007.5032.6941) on Interface Gi2/3
AuditSessionID 0A304345000000060012C050

```

```
brisk#
```

```
show authentication sessions
```

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

```
Authz Failed
```

```
0A304345000000060012C050
```

Después de agregar la ACL de interfaz:

```
<#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
```

La autenticación y autorización se realizan correctamente y la DACL se aplica correctamente:

```
<#root>
```

```
brisk#
```

```
show authentication sessions
```

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

```
Authz Success
```

```
0A30434500000008001A2CE4
```

El comportamiento no depende de la "autenticación abierta". Para aceptar la DACL, necesita la ACL de interfaz para ambos modos abierto/cerrado.

DACL en 4500/6500

En el 4500/6500, la DACL se aplica con las DACL acl_snoop. Aquí se muestra un ejemplo con 4500 sup2 12.2.53SG6 (teléfono + PC). Hay una ACL independiente para VLAN de voz (10) y de datos (100):

```
<#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
```

Las ACL son específicas porque IPDT tiene las entradas correctas:

```
<#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
```

Las sesiones autenticadas confirman las direcciones:

```
<#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

En esta etapa, tanto el PC como el teléfono responden al eco ICMP, pero la ACL de interfaz presenta solamente:

<#root>

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

192.168.10.12

any

¿Por qué? Debido a que la DACL sólo se ha presionado para el teléfono (192.168.10.12). Para el PC, se utiliza la ACL de interfaz con modo abierto:

```
<#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)
```

En resumen, acl_snoop se crea tanto para el PC como para el teléfono, pero la DACL se devuelve sólo para el teléfono. Es por eso que esa ACL se ve como vinculada a la interfaz.

Estado de la dirección MAC para 802.1x

Cuando se inicia la autenticación 802.1x, la dirección MAC se sigue viendo como DINÁMICA, pero la acción para ese paquete es DROP:

```
<#root>
```

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

```
show authentication sessions
```

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

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

```
show mac address-table interface g1/0/1
```

```
Mac Address Table
```

```
-----
Vlan    Mac Address      Type      Ports
----    -
100
```

```
0007.5032.6941    DYNAMIC    Drop
```

Total Mac Addresses for this criterion: 1

Después de la autenticación exitosa, la dirección MAC se vuelve estática y se proporciona el número de puerto:

```
<#root>
```

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

```
show authentication sessions
```

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

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

```
show mac address-table interface g1/0/1
```

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

Esto se aplica a todas las sesiones mab/dot1x de ambos dominios (VOZ/DATOS).

Troubleshoot

No olvide leer la guía de configuración de 802.1x correspondiente a su versión de software y plataforma específicas.

Si abre un caso TAC, proporcione el resultado de estos comandos:

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

También es bueno recopilar una captura de paquetes de puerto SPAN y estas depuraciones:

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

Información Relacionada

- [Guía de Configuración de Servicios de Autenticación 802.1X, Cisco IOS XE Release 3SE \(Switches Catalyst 3850\)](#)
- [Guía de Configuración del Software del Switch Catalyst 3750-X y Catalyst 3560-X, Cisco IOS Release 15.2\(1\)E](#)
- [Guía de Configuración del Software Catalyst 3750-X y 3560-X, Release 15.0\(1\)SE](#)
- [Guía de Configuración del Software Catalyst 3560, Versión 12.2\(52\)SE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).