

Entender a DACL 802.1x, a ACL por usuário, a ID de filtro e o comportamento de rastreamento do dispositivo

Contents

[Introdução](#)

[Teoria de rastreamento de dispositivo](#)

[Configuração de rastreamento de dispositivo](#)

[Testes de Rastreamento de Dispositivos](#)

[Depurações da versão 12.2.33, Rastreamento de dispositivo IP atualizado pelo rastreamento de DHCP](#)

[Sondagem e rastreamento ARP](#)

[Rastreamento de Dispositivo IP para Versão 12.2.55 - Comando Oculto](#)

[Rastreamento de dispositivo IP para a versão 12.2.55 - Exemplo de IP estático](#)

[Rastreamento de dispositivo IP para a versão 15.x](#)

[Rastreamento de dispositivo IP para Cisco IOS-XE®](#)

[Rastreamento de dispositivo IP com 802.1x e DACL para a versão 12.2.55](#)

[Rastreamento de dispositivo IP com 802.1x e DACL para versão 15.x](#)

[Entrada específica da ACL](#)

[Controle-direção](#)

[Rastreamento de dispositivo IP com 802.1x e ACL por usuário para a versão 15.x](#)

[Diferença quando comparado ao DACL](#)

[Rastreamento de dispositivo IP com 802.1x e ACL de ID de filtro para a versão 15.x](#)

[Rastreamento de dispositivo IP - Padrões e práticas recomendadas](#)

[Interface ACL Rewrite for Version 15.x \(Reescrita de ACL de interface para a versão 15.x\)](#)

[ACL padrão usada para 802.1x](#)

[Modo aberto](#)

[Quando a ACL de interface é obrigatória](#)

[DACL em 4500/6500](#)

[Status do Endereço MAC para 802.1x](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o recurso de rastreamento de dispositivo IP, os disparadores para adicionar e remover um host e o impacto do rastreamento de dispositivo no 802.1x DACL.

Teoria de rastreamento de dispositivo

Este documento descreve como o recurso de rastreamento de dispositivo IP funciona, que inclui o que são os disparadores para adicionar e remover um host.

Além disso, é explicado o impacto do rastreamento de dispositivo na lista de controle de acesso (DACL) 802.1x para download.

O comportamento muda entre versões e plataformas.

A segunda parte do documento concentra-se na ACL (Access Control List, lista de controle de acesso)

retornada pelo servidor AAA (Authentication, Authorization, and Accounting) e aplicada à sessão 802.1x.

Uma comparação entre a DACL, a ACL por usuário e a ACL de ID de filtro é apresentada.

Além disso, algumas advertências em relação à regravação da ACL e à ACL padrão são discutidas.

O rastreamento de dispositivo adiciona uma entrada quando:

- ele aprende a nova entrada através do rastreamento de DHCP.
- ele aprende a nova entrada através de uma solicitação ARP (Address Resolution Protocol) (lê o endereço MAC do remetente e o endereço IP do remetente do pacote ARP).

Essa funcionalidade às vezes é chamada de inspeção ARP, mas não é a mesma que a Inspeção ARP Dinâmica (DAI).

Esse recurso está habilitado por padrão e não pode ser desabilitado. Ele também é chamado de rastreamento ARP, mas as depurações não o mostram depois que "debug arp snooping" é habilitado.

O rastreamento ARP é habilitado por padrão e não pode ser desabilitado ou controlado.

O rastreamento de dispositivo remove uma entrada quando não há resposta para uma solicitação ARP (enviando sonda para cada host na tabela de rastreamento de dispositivo, por padrão a cada 30 segundos).

Configuração de rastreamento de 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
```

Testes de Rastreamento 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
```

Depurações da versão 12.2.33, Rastreamento de dispositivo IP atualizado pelo rastreamento de DHCP

O rastreamento de DHCP preenche a tabela de vinculação:

<#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_SNOOP(hl_fm_set_if_input): Setting if_input to Fa0/1 for pak. Was V11
02:31:12: DHCP_SNOOP(hl_fm_set_if_input): Setting if_input to V11 for pak. Was Fa0/1
02:31:12: DHCP_SNOOP(hl_fm_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
```

Depois que a associação DHCP é adicionada ao banco de dados, ela aciona a notificação para o rastreamento de dispositivo:

```
<#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
```

Os testes ARP são enviados por padrão a 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	

Depois que a entrada é removida da tabela de controle de dispositivos, a entrada de ligação DHCP correspondente ainda está lá:

```
<#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

Há um problema quando você tem uma resposta ARP, mas a entrada de rastreamento de dispositivo é removida de qualquer forma.

Esse bug parece estar na versão 12.2.33 e não apareceu na versão 12.2.55 ou no software 15.x.

Também há algumas diferenças ao lidar com a porta L2 (porta de acesso) e a porta L3 (sem switchport).

Sondagem e rastreamento ARP

Rastreamento de dispositivos com o recurso de rastreamento 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
```

Rastreamento de Dispositivo IP para Versão 12.2.55 - Comando Oculto

Para a Versão 12.2, use um comando oculto para ativá-la:

```
<#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
```

Rastreamento de dispositivo IP para a versão 12.2.55 - Exemplo de IP estático

Neste exemplo, o PC foi configurado com um endereço IP estático. As depurações mostram que, depois que você obtém uma resposta ARP (MSG=2), a entrada de rastreamento de dispositivo é atualizada.

```
<#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
```

Assim, cada solicitação ARP do PC atualiza a tabela de rastreamento do dispositivo (o endereço MAC do remetente e o endereço IP do remetente do pacote ARP).

Rastreamento de dispositivo IP para a versão 15.x

É importante lembrar que alguns dos recursos, como o DACL para 802.1x, não são suportados na versão LAN Lite (cuidado - o Cisco Feature Navigator nem sempre mostra as informações corretas).

O comando oculto da versão 12.2 pode ser executado, mas não tem efeito. Na versão de software 15.x, o rastreamento de dispositivo IP (IPDT), por padrão, está habilitado apenas para as interfaces que têm 802.1x habilitado:

```
<#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

```

Após a remoção da configuração 802.1x da porta, o IPDT também é removido dessa porta.

O status da porta é possivelmente "DOWN", portanto, é necessário ter "switchport mode access" e "authentication port-control auto" para ativar o rastreamento de dispositivo IP nessa porta.

O limite máximo do dispositivo de interface é definido como 10:

```

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

```

Rastreamento de dispositivo IP para Cisco IOS-XE®

Novamente, o comportamento no Cisco IOS-XE 3.3 mudou quando comparado ao Cisco IOS versão 15.x.

O comando oculto da versão 12.2 está obsoleto, mas agora este erro é retornado:

```
<#root>
```

```
3850-1#
```

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

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

No Cisco IOS-XE, o rastreamento de dispositivo é ativado para todas as interfaces (mesmo aquelas que não têm 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)

```

Além disso, não há limites para o máximo de entradas por porta (0 significa desabilitado).

Rastreamento de dispositivo IP com 802.1x e DACL para a versão 12.2.55

Se 802.1x estiver configurado com DACL, a entrada de rastreamento de dispositivo será usada para preencher o endereço IP do dispositivo.

Este exemplo mostra o rastreamento de dispositivo funcionando para um IP configurado estaticamente:

```

<#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 é uma sessão 802.1x criada com a 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

Mostra uma 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)
```

Além disso, a ACL na interface fa0/1 é a mesma:

```
<#root>
```

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

```
show ip access-lists interface fa0/1
```

```
permit icmp any any
```

Embora o padrão seja a ACL dot1x:

```
<#root>
```

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

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

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

Espera-se que a ACL use "any" como **192.168.0.244**. Isso funciona assim para o proxy de autenticação, mas para o 802.1x DACL src "any" não é alterado para o IP detectado do PC.

Para proxy de autenticação, uma ACL original do ACS é armazenada em cache e mostrada com o comando **show ip access-list** e uma ACL específica (Por usuário com IP específico) é aplicada na interface com o comando **show ip access-list interface fa0/1**. No entanto, auth-proxy não usa rastreamento de IP do dispositivo.

E se o endereço IP não for detectado corretamente? Depois que o rastreamento do dispositivo for desabilitado:

```
<#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:  0A3042A90000000000000000C775
      Acct Session ID:   0x00000001
      Handle:            0xB0000000
```

```
Runnable methods list:
```

```
  Method  State
  dot1x   Authc Success
```

Então, nenhum endereço IP é anexado, mas a DACL ainda é 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 (4 matches)
Extended IP access list
 xACSACLx-IP-DACL-516c2694 (per-user)

 10 permit icmp any any
```

Neste cenário, o rastreamento de dispositivo para 802.1x não é necessário. A única diferença é que saber o endereço IP do cliente com antecedência pode ser usado para uma solicitação de acesso RADIUS. Após anexar o atributo 8:

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

Ele existe em Access-Request e no ACS é possível criar regras de autorização mais 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
```

Lembre-se de que o TrustSec também precisa de rastreamento de dispositivo IP para vinculações IP a SGT.

Rastreamento de dispositivo IP com 802.1x e DACL para versão 15.x

Qual é a diferença entre a versão 15.x e a versão 12.2.55 na DACL? Na versão 15.x do software, ele funciona da mesma forma que para auth-proxy.

A ACL genérica pode ser vista quando o comando **show ip access-list** é inserido (resposta em cache de AAA), mas depois do comando **show ip access-list interface fa0/1**, o src "any" é substituído pelo endereço IP origem do host (conhecido através do rastreamento de dispositivo IP).

Este é o exemplo para um telefone e um PC em uma porta (g1/0/1), software Versão 15.0.2SE2 em 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:

~~x~~ACSACLx-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

O telefone é autenticado via MAC Authentication Bypass (MAB), enquanto o PC usa dot1x. Tanto o telefone quanto o PC usam a mesma 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

No entanto, quando verificado no nível da interface, a origem foi substituída pelo endereço IP do dispositivo.

O rastreamento de dispositivo IP aciona essa alteração e ela pode ocorrer a qualquer momento (muito depois da sessão de autenticação e do download da 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

```

Os dois endereços MAC são marcados como estáticos:

```

<#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 específica da ACL

Quando a origem "any" no DACL é substituída pelo endereço IP do host? Somente quando houver pelo menos duas sessões na mesma porta (dois suplicantes).

Não há necessidade de substituir a origem "any" quando há apenas uma sessão.

Os problemas aparecem quando há várias sessões e, para nem todas, o rastreamento de dispositivo IP conhece o endereço IP do host. Nesse cenário, ainda é "qualquer" para algumas entradas.

Esse comportamento é diferente em algumas plataformas. Por exemplo, no 2960X com a versão 15.0(2)EX, a ACL é sempre específica mesmo quando há apenas uma sessão de autenticação por porta.

No entanto, para o 3560X e o 3750X versão 15.0(2)SE, você precisa ter pelo menos duas sessões para tornar essa ACL específica.

Controle-direção

Por padrão, a direção do controle é do tipo ambos:

```
<#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
```

Isso significa que, antes que o requerente seja autenticado, o tráfego não pode ser enviado de ou para a porta. Para o modo "in", o tráfego poderia ter sido enviado de porta para requerente, mas não do solicitante para a porta (poderia ser útil para o recurso WAKE on LAN).

Ainda assim, o switch aplica a ACL apenas na direção "in". Não importa qual modo é usado.

```
<#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
```

Isso significa basicamente que, após a autenticação, a ACL é aplicada ao tráfego para a porta (na direção) e todo o tráfego é permitido a partir da porta (na direção de saída).

Rastreamento de dispositivo IP com 802.1x e ACL por usuário para a versão 15.x

Também é possível usar uma ACL por usuário que é passada em cisco-av-pair "ip:inacl" e "ip:outacl".

Esta configuração de exemplo é semelhante a uma configuração anterior, mas desta vez o telefone usa

DAACL e o PC usa ACL por usuário. O perfil do ISE para o PC é:

▼ 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
```

O telefone ainda tem o DAACL aplicado:

<#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
```

No entanto, o PC na mesma porta usa a ACL por usuário:

```
<#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 como isso é mesclado na porta 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
```

A primeira entrada foi obtida da ACL por usuário (observe a palavra-chave log) e a segunda entrada é obtida da DACL.

Ambos são regravados pelo rastreamento de dispositivo IP para o endereço IP específico.

A ACL por usuário pode ser verificada com o 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

E também através do 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

E o atributo ip:outacl? Ele é completamente omitido na versão 15.x. O atributo foi recebido, mas o switch não aplica/processa esse atributo.

Diferença quando comparado ao DACL

Como observado na ID de bug Cisco [CSCut25702](#), a ACL por usuário se comporta de forma diferente da DACL.

A DACL com apenas uma entrada ("permit ip any any") e um solicitante conectado a uma porta pode funcionar corretamente sem o rastreamento de dispositivo IP habilitado.

O argumento "any" não é substituído e todo o tráfego é permitido. No entanto, para a ACL por usuário, é obrigatório ter o rastreamento de dispositivo IP habilitado.

Se ele estiver desativado e tiver apenas a entrada "permit ip any any" e um solicitante, todo o tráfego será bloqueado.

Rastreamento de dispositivo IP com 802.1x e ACL de ID de filtro para a versão 15.x

Além disso, o atributo IETF filter-id [11] pode ser usado. O servidor AAA retorna o nome da ACL, que é definida localmente no switch. O perfil do ISE pode ser assim:

The screenshot shows the 'Common Tasks' section of the ISE configuration interface. It contains several checkboxes: 'DACL Name' (unchecked), 'VLAN' (checked), 'Voice Domain Permission' (unchecked), 'Web Authentication' (unchecked), 'Auto Smart Port' (unchecked), and 'Filter-ID' (checked). The 'VLAN' checkbox is associated with 'Tag ID 1' and an 'Edit Tag' button. The 'ID/Name' field next to it contains the value '20'. The 'Filter-ID' checkbox is associated with a text input field containing 'Filter-ACL' and a '.in' suffix.

Observe que você precisa especificar a direção (dentro ou fora). Para isso, é necessário adicionar o atributo manualmente:

The screenshot shows the 'Advanced Attributes Settings' section. It features a configuration row with a dropdown menu on the left containing 'Radius:Filter-ID', an equals sign, and another dropdown menu on the right containing 'Filter-ACL.out'. Both dropdown menus have a downward arrow icon.

Em seguida, o comando debug mostra:

```
<#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
```

Essa ACL também é mostrada para a sessão 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
```

E, como a ACL está vinculada à interface:

```
<#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
```

Observe que essa ACL pode ser mesclada com outros tipos de ACL na mesma interface. Por exemplo, tendo na mesma porta de switch outro solicitante que obtém a DACL do ISE: "permit ip any any" você pode 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
```

Observe que o rastreamento do dispositivo IP registra o IP de origem para cada origem (suplicante).

E a lista de filtros "out"? Novamente (como ACL por usuário), ele não é usado pelo switch.

Rastreamento de dispositivo IP - Padrões e práticas recomendadas

Para versões anteriores à 15.2(1)E, antes que qualquer recurso possa usar o IPDT, ele precisa ser ativado globalmente primeiro com este comando CLI:

```
<#root>
(config)#
ip device tracking
```

Para as versões 15.2(1)E e posteriores, o **comando ip device tracking** não é mais necessário. O IPDT é habilitado somente se um recurso que depende dele o habilitar.

Se nenhum recurso ativar o IPDT, ele será desativado. O comando "no ip device tracking" não tem efeito. O recurso específico tem o controle para ativar/desativar o IPDT.

Quando você habilita o IPDT, é necessário lembrar-se do problema "Duplicate IP Address" (Duplicar endereço IP) no . Consulte [Troubleshooting de Mensagens de Erro "Duplicate IP Address 0.0.0.0"](#) para obter mais informações.

É recomendável desativar o IPDT em uma porta de tronco:

```
<#root>
(config-if)#
no ip device tracking
```

No Cisco IOS posterior, é um comando diferente:

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

Recomenda-se ativar o IPDT na porta de acesso e retardar as sondas ARP para evitar o problema "Duplicate IP Address" (Endereço IP duplicado):

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

Interface ACL Rewrite for Version 15.x (Reescrita de ACL de interface para a versão 15.x)

Para a interface ACL, ela funciona antes da autenticação:

```
<#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
```

No entanto, após a autenticação ser bem-sucedida, ela é reescrita (substituição) pela ACL retornada do servidor AAA (não importa se é DACL, ip:inacl ou filterid).

Essa ACL (test1) pode bloquear o tráfego (que normalmente seria permitido no modo aberto), mas após a autenticação, isso não importa mais.

Mesmo quando nenhuma ACL é retornada do servidor AAA, a ACL da interface é substituída e o acesso completo é fornecido.

Isso é um pouco enganador, pois a memória endereçável de conteúdo ternário (TCAM) indica que a ACL ainda está vinculada no nível da interface.

Aqui está um exemplo da versão 15.2.2 no 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
```

Essas informações são válidas somente para o nível de interface, não para o nível de sessão. Mais algumas informações (apresenta uma ACL composta) podem ser deduzidas 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
```

A primeira entrada é criada quando a DACL "permit ip any any" é retornada para uma autenticação bem-sucedida (e "any" é substituído por uma entrada da tabela de controle de dispositivos).

A segunda entrada é o resultado da ACL de interface e é aplicada a todas as novas autenticações (antes da autorização).

Infelizmente, (novamente dependente da plataforma) ambas as ACLs são concatenadas. Isso acontece na versão 15.2.2 no 3750X.

Isso significa que, para sessões autorizadas, ambas são aplicadas. Primeiro a DACL e depois a ACL de interface.

É por isso que quando você adiciona "deny ip any any" explícito, a DACL não leva em consideração a ACL de interface.

Geralmente, não há nenhuma negação explícita na DACL e, em seguida, a ACL de interface é aplicada depois disso.

O comportamento para a versão 15.0.2 no 3750X é o mesmo, mas o comando **sh ip access-list interface** não mostra mais a ACL de interface (mas ainda é concatenado com a ACL de interface, a menos que exista uma negação explícita na DACL).

ACL padrão usada para 802.1x

Há dois tipos de ACLs padrão:

- auth-default-ACL-OPEN - usado para o modo aberto
- auth-default-ACL - usado para acesso fechado

Tanto auth-default-ACL quanto auth-default-ACL-OPEN são usados quando a porta está em estado não autorizado. Por padrão, o acesso fechado é usado.

Isso significa que, antes da autenticação, todo o tráfego é descartado, exceto aquele permitido pela ACL padrão de autenticação.

Dessa forma, o tráfego DHCP é permitido antes da autorização bem-sucedida.

O endereço IP é alocado e o DACL baixado pode ser aplicado corretamente.

Essa ACL é criada automaticamente e não pode ser encontrada na configuração.

```
<#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
```

Ele é criado dinamicamente para a primeira autenticação (entre as fases de autenticação e autorização) e removido após a última sessão ser removida.

Auth-Default-ACL permite apenas tráfego DHCP. Depois que a autenticação for bem-sucedida e o novo DACL for baixado, ele será aplicado a essa sessão.

Quando o modo é alterado para open auth-default-ACL-OPEN aparece e é usado e funciona exatamente da mesma forma 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 as ACLs podem ser personalizadas, mas nunca são vistas na configuração.

```
<#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 aberto

A seção anterior descreveu o comportamento das ACLs (que inclui o usado por padrão para o modo aberto). O comportamento do modo aberto é:

- ele permite todo o tráfego (de acordo com auth-default-ACL-OPEN padrão) quando a sessão está em um estado não autorizado.
- a sessão está em um estado não autorizado durante a autenticação/autorização (adequado para cenários de inicialização do PXE (Encryption Appliance Model E)) ou depois que o processo falha (adequado para cenários chamados de "modo de baixo impacto").
- quando a sessão se move para o estado autorizado de várias plataformas, as ACLs são concatenadas e o primeiro DACL é usado, depois a interface ACL.
- para multiauth ou multidomain, possivelmente há várias sessões ao mesmo tempo em estados diferentes (o tipo de ACL diferente se aplica a cada sessão).

Quando a ACL de interface é obrigatória

Para várias plataformas 6500/4500, a interface ACL é obrigatória para aplicar a DACL corretamente.

Aqui está um exemplo com 4500 sup2 12.2.53SG6, sem ACL de interface:

```
<#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
```

Depois que o host é autenticado, o DACL é baixado. Não é aplicado e a autorização falha.

```
<#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
```

Depois que a interface ACL for adicionada:

```
<#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
```

A autenticação e a autorização são bem-sucedidas e a DACL é aplicada corretamente:

```
<#root>
```

```
brisk#
```

```
show authentication sessions
```

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

```
Authz Success
```

```
0A3043450000008001A2CE4
```

O comportamento não depende da "autenticação aberta". Para aceitar a DACL, você precisa da ACL de interface para o modo aberto/fechado.

DACL em 4500/6500

No 4500/6500, a DACL é aplicada com DACLs `acl_snoop`. Um exemplo com 4500 sup2 12.2.53SG6 (telefone + PC) é mostrado aqui. Há uma ACL separada para VLAN de voz (10) e dados (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
```

As ACLs são específicas porque o IPDT tem as entradas corretas:

```
<#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
```

As sessões autenticadas confirmam os endereços:

```
<#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
```

Nesse estágio, o PC e o telefone respondem ao eco ICMP, mas a ACL da interface apresenta apenas:

<#root>

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

192.168.10.12

any

Por quê? Porque a DACL foi enviada somente para o telefone (192.168.10.12). Para o PC, a interface ACL com modo aberto é usada:

<#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)
```

Em resumo, acl_snoop é criado para o PC e o telefone, mas a DACL é retornada apenas para o telefone. É por isso que essa ACL é vista como vinculada à interface.

Status do Endereço MAC para 802.1x

Quando a autenticação 802.1x começa, o endereço MAC ainda é visto como DYNAMIC, mas a ação para esse pacote é 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
```

Após a autenticação bem-sucedida, o endereço MAC torna-se estático e o número da porta é fornecido:

```
<#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
```

Isso é verdadeiro para todas as sessões mab/dot1x para ambos os domínios (VOZ/DADOS).

Troubleshooting

Lembre-se de ler o guia de configuração 802.1x para a sua versão de software e plataforma específicas.

Se você abrir um caso de TAC, forneça a saída destes comandos:

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

Também é bom coletar uma captura de pacote de porta SPAN e estas depurações:

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

Informações Relacionadas

- [Guia de configuração de serviços de autenticação 802.1X, Cisco IOS XE versão 3SE \(switches Catalyst 3850\)](#)

- [Guia de configuração de software do switch Catalyst 3750-X e Catalyst 3560-X, Cisco IOS versão 15.2\(1\)E](#)
- [Guia de configuração de software do Catalyst 3750-X e 3560-X, versão 15.0\(1\)SE](#)
- [Guia de configuração do software Catalyst 3560, versão 12.2\(52\)SE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.