Begrijp 802.1x DACL, ACL per gebruiker, filter-id en gedrag voor apparaattracering

Inhoud

Inleiding
Theorie voor apparaattracering
Configuratie van apparaattracering
Apparaattraceringstests
Debugs from versie 12.2.3, IP Device Tracking bijgewerkt door DHCP-controle
Sonde en ARP-controle
IP-apparaattracering voor versie 12.2.5 - verborgen opdracht
IP-apparaattracering voor versie 12.2.5 - Statisch IP-voorbeeld
IP-apparaattracering voor versie 15.x
IP-apparaattracering voor Cisco IOS-XE®
IP-apparaattracering met 802.1x en DACL voor versie 12.2.5
IP-apparaattracering met 802.1x en DACL voor versie 15.x
Specifieke ACL-vermeldingen
Control-directie
IP-apparaattracering met 802.1x en ACL per gebruiker voor versie 15.x
Verschil in vergelijking met DACL
IP-apparaattracering met 802.1x en filter-ID ACL voor versie 15.x
IP-apparaattracering - standaardwaarden en beste praktijken
Interface ACL-herschrijvingen voor versie 15.x
Standaard ACL gebruikt voor 802.1x
Open-modus
Wanneer interface-ACL verplicht is
DACL-code op 4500/6500
MAC-adresstatus voor 802.1x
Problemen oplossen
Gerelateerde informatie

Inleiding

Dit document beschrijft de functie voor het bijhouden van IP-apparaten, de triggers om een host toe te voegen en te verwijderen en het effect van het volgen van apparaten op de 802.1x DACL.

Theorie voor apparaattracering

In dit document wordt beschreven hoe de functie voor het traceren van IP-apparaten werkt en met welke triggers u een host kunt toevoegen en verwijderen.

Ook wordt het effect van het bijhouden van apparaten op de 802.1x Downloadbare Access Control List (DACL) toegelicht.

Het gedrag verandert tussen versies en platforms.

Het tweede deel van het document concentreert zich op de toegangscontrolelijst (ACL) die door de verificatie-, autorisatie- en accounting (AAA) server is geretourneerd en die op de 802.1x-sessie is toegepast.

Er wordt een vergelijking gemaakt tussen de DACL, ACL per gebruiker en ACL van filter-id.

Ook worden enkele voorbehouden met betrekking tot de ACL herschrijven en standaard ACL besproken.

Apparaattracering voegt een gegeven toe wanneer:

- het leert de nieuwe ingang via het snooping van DHCP.
- het leert de nieuwe ingang via een verzoek van het Protocol van de Resolutie van het Adres (ARP) (leest het adres van afzenderMAC en het afzenderIP adres van het ARP pakket).

Die functionaliteit wordt soms ARP-inspectie genoemd, maar het is niet hetzelfde als Dynamic ARP Inspection (DAI).

Deze optie is standaard ingeschakeld en kan niet worden uitgeschakeld. Het wordt ook ARP snooping genoemd, maar debugs tonen het niet nadat "debug arp snooping" is ingeschakeld.

ARP-snooping is standaard ingeschakeld en kan niet worden uitgeschakeld of gecontroleerd.

Het volgen van het apparaat verwijdert een ingang wanneer er geen reactie voor een ARP verzoek is (verzendend sonde voor elke gastheer in de apparaat het volgen lijst, door gebrek elke 30 seconden).

Configuratie van apparaattracering

```
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
```

Apparaattraceringstests

<#root>

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

show ip dhcp binding

```
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.0.241    0100.5056.994e.a1       Mar 02 1993 02:31 AM    Automatic

BSNS-3560-1#
```

show ip device tracking all

```
IP Device Tracking = Enabled
------------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
------------------------------------------------------------
192.168.0.241   0050.5699.4ea1 FastEthernet0/1        ACTIVE
```

Debugs from versie 12.2.3, IP Device Tracking bijgewerkt door DHCP-controle

DHCP-spionage vult de bindende tabel in:

<#root>

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

show debugging

```
DHCP Snooping packet debugging is on
DHCP Snooping event debugging is on
DHCP server packet debugging is on.
DHCP server event debugging is on.
track:
  IP device-tracking redundancy events debugging is on
  IP device-tracking cache entry Creation debugging is on
  IP device-tracking cache entry Destroy debugging is on
  IP device-tracking cache events debugging is on

02:30:57: DHCP_SNOOPING: checking expired snoop binding entries
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak.  Was Vl1
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Vl1 for pak.  Was Fa0/1
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak.  Was Vl1
02:31:12:
```

DHCP_SNOOPING: received new DHCP packet from input interface

```
 (FastEthernet0/1)
02:31:12:
```

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input
interface: Fa0/1, MAC da: 001f.27e6.cfc0, MAC sa: 0050.5699.4ea1, IP da: 192.168.0.2,
IP sa: 192.168.0.241, DHCP ciaddr:

```
 192.168.0.241, DHCP yiaddr: 0.0.0.0,
 DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.5699.4ea1
02:31:12:
```

DHCP_SNOOPING: add relay information option

```
.
02:31:12: DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port format
02:31:12: DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format
02:31:12: DHCP_SNOOPING: binary dump of relay info option, length: 20 data&colon;
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0x1 0x1 0x3 0x2 0x8 0x0 0x6 0x0 0x1F 0x27 0xE6 0xCF 0x80
02:31:12: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: 001F.27E6.CFC0,
 packet is flooded to ingress VLAN: (1)
02:31:12: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan1.
02:31:12:
```

DHCPD: DHCPREQUEST received from client 0100.5056.994e.a1

```
.
02:31:12:
```

DHCPD: Sending DHCPACK to client 0100.5056.994e.a1 (192.168.0.241)

```
.
02:31:12: DHCPD: unicasting BOOTREPLY to client 0050.5699.4ea1 (192.168.0.241).
02:31:12: DHCP_SNOOPING: received new DHCP packet from input interface (Vlan1)
02:31:12:
```

DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK

```
, input interface:
 Vl1, MAC da: 0050.5699.4ea1, MAC sa: 001f.27e6.cfc0, IP da: 192.168.0.241,
 IP sa: 192.168.0.2, DHCP ciaddr: 192.168.0.241, DHCP yiaddr: 192.168.0.241,
 DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.5699.4ea1
02:31:12:
```

DHCP_SNOOPING: add binding on port FastEthernet0/1

```
.
02:31:12: DHCP_SNOOPING: added entry to table (index 189)
02:31:12: DHCP_SNOOPING: dump binding entry: Mac=00:50:56:99:4E:A1 Ip=192.168.0.241
 Lease=86400     ld Type=dhcp-snooping Vlan=1 If=FastEthernet0/1
```

Nadat de DHCP-binding is toegevoegd aan de database, wordt de melding voor het bijhouden van het apparaat geactiveerd:

<#root>

```
02:31:12:
```

**sw_host_track-ev:host_track_notification: Add event for host 0050.5699.4ea1,
 192.168.0.241 on interface FastEthernet0/1**

```
02:31:12: sw_host_track-ev:Async Add event for host 0050.5699.4ea1, 192.168.0.241
 on interface FastEthernet0/1
02:31:12: sw_host_track-ev:MSG = 2
02:31:12: DHCP_SNOOPING_SW no entry found for 0050.5699.4ea1 0.0.0.1 FastEthernet0/1
02:31:12:
```

**DHCP_SNOOPING_SW host tracking not found for update add dynamic
 (192.168.0.241, 0.0.0.0, 0050.5699.4ea1) vlan 1**

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

sw_host_track-ev:Add event: 0050.5699.4ea1, 192.168.0.241, FastEthernet0/1

```
02:31:12: sw_host_track-obj_create:0050.5699.4ea1(192.168.0.241) Cache entry created
02:31:12:
```

**sw_host_track-ev:Activating host 0050.5699.4ea1, 192.168.0.241 on
 interface FastEthernet0/1**

```
02:31:12: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
```

ARP-sondes worden standaard elke 30 seconden verzonden:

<#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

Nadat de ingang wordt verwijderd uit de apparaat volgende lijst, is de overeenkomstige bindende ingang van DHCP nog daar:

<#root>

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

show ip device tracking all

```
IP Device Tracking = Enabled
---------------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
---------------------------------------------------------------

BSNS-3560-1#
```

show ip dhcp binding

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

```
                Hardware address
192.168.0.241    0100.5056.994e.a1       Mar 02 1993 03:06 AM    Automatic
```

Er is het probleem als je een ARP-reactie hebt, maar het apparaat tracking-ingangstoch wordt verwijderd.

Die bug lijkt te zijn in Versie 12.2.33 en is niet verschenen in Versie 12.2.5 of 15.x software.

Er zijn ook enkele verschillen bij de omgang met de L2-poort (access-poort) en de L3-poort (geen switchpoort).

Sonde en ARP-controle

Het volgen van het apparaat met de ARP het snooping eigenschap:

<#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
```

IP-apparaattracering voor versie 12.2.5 - verborgen opdracht

Gebruik voor versie 12.2 daar een verborgen opdracht om deze te activeren:

<#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

IP-apparaattracering voor versie 12.2.5 - Statisch IP-voorbeeld

In dit voorbeeld is de pc geconfigureerd met een statisch IP-adres. Debugs tonen aan dat nadat u een ARP-respons (MSG=2) krijgt, het apparaat tracking-item wordt bijgewerkt.

<#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
```

Zo werkt elk ARP verzoek van PC de apparaat het volgen lijst (het adres van afzenderMAC en afzender IP adres van het ARP pakket) bij.

IP-apparaattracering voor versie 15.x

Het is belangrijk om te onthouden dat sommige functies zoals DACL voor 802.1x niet worden ondersteund in de LAN Lite-versie (let op - Cisco Feature Navigator toont niet altijd de juiste informatie).

De verborgen opdracht van Versie 12.2 kan worden uitgevoerd, maar heeft geen effect. In de softwareversie 15.x, wordt IP apparaat het volgen (IPDT) door gebrek slechts toegelaten voor de interfaces die 802.1x toegelaten hebben:

<#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
```

Na verwijdering van 802.1x configuratie uit de poort, IPDT wordt ook verwijderd uit die poort.

De poortstatus is mogelijk "DOWN", dus het is noodzakelijk om "switchport mode access" en "authenticatie poort-control auto" te hebben om IP apparaat tracking geactiveerd te hebben op die poort.

De maximum grens van het interfaceapparaat wordt geplaatst aan 10:

```
<#root>

bsns-3750-5(config-if)#
ip device tracking maximum

 ?
  <1-10>  Maximum devices
```

IP-apparaattracering voor Cisco IOS-XE®

Opnieuw is het gedrag op Cisco IOS-XE 3.3 gewijzigd in vergelijking met Cisco IOS versie 15.x.

De verborgen opdracht van Versie 12.2 is verouderd, maar nu wordt deze fout teruggegeven:

```
<#root>
```

```
3850-1#
```

no ip device tracking int g1/0/48

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

In Cisco IOS-XE is het volgen van apparaten geactiveerd voor alle interfaces (zelfs voor de interfaces waarvoor 802.1x niet is geconfigureerd):

<#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)
```

Er zijn ook geen limieten voor de maximale invoer per poort (0 betekent uitgeschakeld).

IP-apparaattracering met 802.1x en DACL voor versie 12.2.5

Als 802.1x is geconfigureerd met DACL, wordt de apparaattraceringsvermelding gebruikt om het IP-adres van het apparaat in te vullen.

In dit voorbeeld wordt getoond hoe een apparaat kan worden gevolgd voor een statisch geconfigureerd IP:

<#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
```

Dit is een 802.1x-sessie die is gebouwd met DACL-toegangscontrole (om het even welk type):

<#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
```

Dit toont toegepaste ACL:

<#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)
```

Ook is de ACL op de fa0/1 interface hetzelfde:

<#root>

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

show ip access-lists interface fa0/1

```
     permit icmp any any
```

Zelfs als de standaardinstelling dot1x ACL is:

<#root>

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

show ip interface fa0/1

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

Verwacht wordt dat ACL de waarde "willekeurige" zal gebruiken als **192.168.0.244**. Dat werkt als dit voor auth proxy, maar voor 802.1x DACL src "geen" wordt gewijzigd in de gedetecteerde IP van de PC.

Voor een automatische proxy wordt één oorspronkelijke ACL van de ACS gecacheeerd en weergegeven met de opdracht **IP-toegangslijst tonen** en wordt een specifieke (Per-Gebruiker met specifieke IP) ACL toegepast op de interface met de opdracht **fa0/1 voor** de **IP-toegangslijst tonen**. Auth-proxy maakt echter geen gebruik van IP-tracking van apparaten.

Wat als het IP-adres niet goed wordt gedetecteerd? Nadat het apparaat traceren is uitgeschakeld:

```
<#root>

BSNS-3560-1#

show authentication sessions interface fa0/1


           Interface:  FastEthernet0/1
         MAC Address:  0050.5699.4ea1


 IP Address:  Unknown


           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  2


ACS ACL:  xACSACLx-IP-DACL-516c2694


      Session timeout:  N/A
         Idle timeout:  N/A
   Common Session ID:  0A3042A9000000000000C775
     Acct Session ID:  0x00000001
              Handle:  0xB0000000

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

Er is dus geen IP-adres als bijlage toegevoegd, maar de DACL wordt nog steeds toegepast:

```
<#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
```

In dit scenario is apparaattracering voor 802.1x niet vereist. Het enige verschil is dat het weten van het IP-adres van de client vooraf kan worden gebruikt voor een RADIUS-toegangsverzoek. Nadat kenmerk 8 is toegevoegd:

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

Het bestaat in Access-request en op ACS is het mogelijk om meer korrelige autorisatieregels te creëren:

```
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
```

Houd in gedachten dat TrustSec ook IP-apparaattracering nodig heeft voor IP-naar-SGT-banden.

IP-apparaattracering met 802.1x en DACL voor versie 15.x

Wat is het verschil tussen Versie 15.x en Versie 12.2.5 in DACL? In software Version15.x, werkt het hetzelfde als voor auth-proxy.

Generieke ACL kan worden gezien wanneer het bevel van de **show ip toegang-lijst** is ingegaan (cached reactie van AAA), maar na de **show ip toegang-lijst interface fa0/1** bevel, wordt src "om het even welk"vervangen door het bron IP adres van de gastheer (die via IP apparatenvolgen wordt bekend).

Dit is het voorbeeld voor een telefoon en pc op één poort (g1/0/1), software versie 15.0.2SE2 op 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
```

De telefoon wordt geverifieerd via MAC-verificatie-omleiding (MAB), terwijl de pc dot1x gebruikt. Zowel de telefoon als de PC gebruiken dezelfde 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
```

Na verificatie op interfaceniveau is de bron echter vervangen door het IP-adres van het apparaat.

IP-apparaattracering triggers die veranderen en het kan op elk moment gebeuren (veel later dan de authenticatiesessie en download van de 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
```

Beide MAC-adressen zijn als statisch gemarkeerd:

```
<#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
```

Specifieke ACL-vermeldingen

Wanneer wordt de bron "enige" in de DACL vervangen door het IP-adres van de host? Alleen wanneer er ten minste twee sessies op dezelfde poort zijn (twee smeekbeden).

Het is niet nodig de bron "enige" te vervangen wanneer er slechts één sessie is.

De problemen verschijnen wanneer er meerdere sessies zijn, en voor niet al deze IP-apparaat tracking kent het IP-adres van de host. In dat scenario is het nog "om het even welk"voor sommige ingangen.

Dat gedrag is anders op sommige platformen. Op de 2960X met versie 15.0(2)EX is de ACL bijvoorbeeld altijd specifiek, zelfs wanneer er slechts één verificatiesessie per poort is.

Voor de 3560X en 3750X, versie 15.0(2)SE, moet u echter ten minste twee sessies hebben om die ACL specifiek te maken.

Control-directie

De standaardinstelling is dat de besturingsrichting beide typen is:

<#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

Dit betekent dat voordat de aanvrager wordt geauthenticeerd, geen verkeer naar of van de haven kan worden verzonden. In de "in"-modus kan het verkeer van poort naar aanvrager zijn verzonden, maar niet van aanvrager naar poort (dit kan handig zijn voor de WAKE on LAN-functie).

Niettemin past de switch de ACL toe enkel op de "in" richting. Het maakt niet uit welke modus wordt gebruikt.

<#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
```

Dat betekent in principe dat na verificatie de ACL wordt toegepast op verkeer naar de poort (in richting) en al het verkeer is toegestaan vanuit de poort (in richting).

IP-apparaattracering met 802.1x en ACL per gebruiker voor versie 15.x

Het is ook mogelijk om per-gebruiker ACL te gebruiken die in cisco-av-paar "ip:inacl" en "ip:outacl" wordt doorgegeven.

Deze voorbeeldconfiguratie is vergelijkbaar met een vorige configuratie, maar deze keer gebruikt de telefoon DACL en de pc gebruikt ACL per gebruiker. Het ISE-profiel voor de pc is:

Op de telefoon is nog steeds DACL toegepast:

<#root>

bsns-3750-5#

show authentication sessions interface g1/0/1

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

192.168.10.12

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

VOICE

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

xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2

```
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A800010000568431143D8
      Acct Session ID:  0x000006D2
               Handle:  0x84000569

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

bsns-3750-5#

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

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

permit ip any any

De pc op dezelfde poort gebruikt echter de ACL van de per gebruiker:

<#root>

```
    Interface:  GigabitEthernet1/0/1
          MAC Address:  0050.5699.4ea1
           IP Address:
```

192.168.2.200

```
            User-Name:  cisco
               Status:  Authz Success
               Domain:
```

DATA

```
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  20
```

Per-User ACL: permit icmp any any log

```
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A800010000056743114008
      Acct Session ID:  0x000006D1
               Handle:  0x9D000568
```

Zo controleert u hoe dit wordt samengevoegd op de gig1/0/1-poort:

<#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
```

De eerste ingang is genomen van de per-gebruiker ACL (merk het logboeksleutelwoord op) en de tweede ingang wordt genomen van DACL.

Beide worden herschreven door IP-apparaattracering voor het specifieke IP-adres.

ACL per gebruiker kan worden geverifieerd met de opdracht **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

En ook via de opdracht **IP-toegangslijsten tonen**:

<#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
```

En het kenmerk ip:outacl? Het wordt volledig weggelaten in Versie 15.x. De eigenschap is ontvangen, maar de switch past die eigenschap niet toe/verwerkt.

Verschil in vergelijking met DACL

Zoals vermeld in Cisco-bug-id CSC25702, gedraagt de ACL per gebruiker zich anders dan DACL.

DACL met slechts één ingang ("vergunning ip om het even welk") en één die supplicant met een haven wordt verbonden kan correct werken zonder IP apparatenvolgen toegelaten.

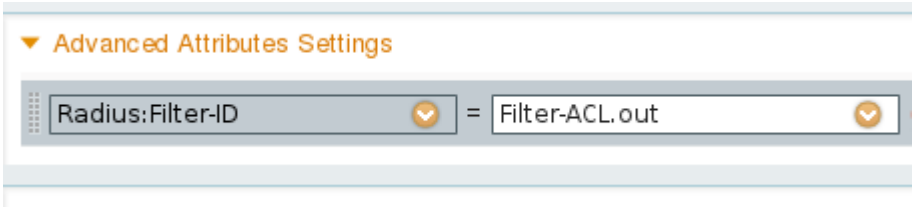
Het 'any'-argument wordt niet vervangen en al het verkeer is toegestaan. Voor de ACL per gebruiker is het echter verplicht om de tracering van IP-apparaten in te schakelen.

Als het is uitgeschakeld en alleen de "permissie ip elke" ingang en een supplicant heeft, dan wordt al het verkeer geblokkeerd.

IP-apparaattracering met 802.1x en filter-ID ACL voor versie 15.x

Ook kan de IETF-attribuut filter-id [11] worden gebruikt. De AAA-server retourneert de ACL-naam, die lokaal op de switch is gedefinieerd. Het ISE-profiel ziet er zo uit:

Let op dat u de richting (in of uit) moet opgeven. Hiervoor is het nodig om het attribuut handmatig toe te voegen:



Dan toont debug:

<#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
```

Die ACL wordt ook getoond voor de geverifieerde sessie:

<#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
```

En, aangezien ACL aan de interface wordt gebonden:

<#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
```

Merk op dat deze ACL kan worden samengevoegd met andere typen ACLâ€™s op dezelfde interface. Bijvoorbeeld, met op dezelfde switch poort een andere supplicant die DACL krijgt van ISE: "laat ip elke willekeurige" u kon zien:

<#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
```

Merk op dat het IP apparaat volgen herschrijft de bron IP voor elke bron (supplicant).

En de lijst met 'uit'-filters? Nogmaals (als ACL per gebruiker): deze wordt niet gebruikt door de switch.

IP-apparaattracering - standaardwaarden en beste praktijken

Voor releases eerder dan 15.2(1)E, voordat een functie IPDT kan gebruiken, moet deze wereldwijd eerst worden ingeschakeld met deze CLI-opdracht:

```
<#root>

(config)#

ip device tracking
```

Voor releases 15.2(1)E en hoger is de opdracht **voor het bijhouden van ip-apparaten** niet meer nodig. IPDT wordt alleen ingeschakeld als een functie die erop vertrouwt het toelaat.

Als geen functie IPDT inschakelt, wordt IPDT uitgeschakeld. De opdracht "Geen ip-apparaat bijhouden" heeft geen effect. De specifieke functie heeft de controle om IPDT in/uit te schakelen.

Wanneer u IPDT inschakelt, moet u zich herinneren over het probleem "Dubbel IP-adres" op . Zie Probleemoplossing "Dubbel IP-adres 0.0.0" voor meer informatie.

Het wordt aanbevolen om IPDT op een trunkpoort uit te schakelen:

```
<#root>

(config-if)#

no ip device tracking
```

Op het latere Cisco IOS is een andere opdracht:

```
<#root>

(config-if)#

 ip device tracking maximum 0
```

Het wordt aanbevolen om IPDT in te schakelen op de toegangspoort en ARP-probes uit te stellen om het probleem met "Duplicate IP Address" te voorkomen:

```
<#root>

(config-if)#

 ip device tracking probe delay 10
```

Interface ACL-herschrijvingen voor versie 15.x

Voor de interface ACL werkt deze vóór verificatie:

<#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
```

Nadat de verificatie is geslaagd, wordt deze echter herschreven (overschrijven) door de ACL die is geretourneerd van de AAA-server (het is niet van belang of dit DACL, ip:inacl of filterid is).

Dat ACL (test1) het verkeer kan blokkeren (wat normaal op open mode zou zijn toegestaan), maar na authenticatie, is niet meer van belang.

Zelfs wanneer geen ACL wordt teruggegeven van de AAA-server, wordt de interface-ACL overschreven en wordt volledige toegang verleend.

Dat is een beetje misleidend aangezien Ternary Content Adressable Memory (TCAM) aangeeft dat de ACL nog steeds op interfaceniveau is gebonden.

Hier is een voorbeeld van versie 15.2.2 op 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
```

Die informatie is alleen geldig voor het interfaceniveau, niet voor het sessieniveau. Wat meer informatie (stelt samengestelde ACL voor) kan worden afgeleid uit:

<#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

De eerste ingang wordt gemaakt als "permissie ip om het even welke" DACL voor succesvolle authentificatie is teruggekeerd (en "om het even welk" wordt vervangen door een ingang van de apparaat volgende lijst).

De tweede ingang is het resultaat van interface ACL en wordt toegepast voor alle nieuwe authentificaties (vóór vergunning).

Helaas (opnieuw afhankelijk van platform) worden beide ACLâ€™s aaneengeschakeld. Dat gebeurt op versie 15.2.2 op 3750X.

Dat betekent dat voor geautoriseerde sessies beide worden toegepast. Eerst DACL en tweede de interface ACL.

Dat is waarom wanneer u expliciet "ontkent ip om het even welk" toevoegt, DACL geen rekening houdt met de interface ACL.

Gewoonlijk is er geen expliciete ontkenning in DACL en dan wordt de interface ACL toegepast daarna.

Het gedrag voor Versie 15.0.2 op 3750X is hetzelfde, maar het opdracht **voor** de **sh IP-toegangslijst interface** toont de interface-ACL niet meer (maar het wordt nog steeds aaneengeschakeld met de interface-ACL, tenzij expliciet ontkennen in de DACL bestaat).

Standaard ACL gebruikt voor 802.1x

Er zijn twee soorten standaard ACLâ€™s:

- Auto-default-ACL-OPEN - gebruikt voor open modus
- Auto-default-ACL - gebruikt voor gesloten toegang

Zowel auth-default-ACL als auth-default-ACL-OPEN worden gebruikt wanneer de poort zich in de ongeautoriseerde toestand bevindt. Standaard wordt gesloten toegang gebruikt.

Dat betekent dat voor de verificatie al het verkeer wordt gedropt behalve het verkeer dat is toegestaan door de auth-default-ACL.

Op deze manier wordt DHCP-verkeer toegestaan voordat de autorisatie succesvol is.

Het IP-adres wordt toegewezen en de gedownloade DACL kan correct worden toegepast.

Die ACL wordt automatisch gemaakt en kan niet in de configuratie worden gevonden.

```
<#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
```

Het wordt dynamisch gemaakt voor de eerste verificatie (tussen verificatie en autorisatiefase) en verwijderd nadat de laatste sessie is verwijderd.

Auth-Default-ACL maakt alleen DHCP-verkeer mogelijk. Nadat de verificatie is geslaagd en de nieuwe DACL is gedownload, wordt deze toegepast op die sessie.

Wanneer de modus wordt gewijzigd in openen van auth-default-ACL-OPEN wordt weergegeven en wordt deze gebruikt en werkt op precies dezelfde manier als 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
```

Beide ACLâ€™s kunnen worden aangepast, maar ze worden nooit in de configuratie gezien.

<#root>

```
bsns-3750-5(config)#
ip access-list extended Auth-Default-ACL

bsns-3750-5(config-ext-nacl)#permit udp any any
bsns-3750-5#
sh ip access-lists

Extended IP access list Auth-Default-ACL
    10 permit udp any range bootps 65347 any range bootpc 65348 (22 matches)
    20 permit udp any any range bootps 65347 (16 matches)
    30 deny ip any any
    40 permit udp any any
bsns-3750-5#
sh run | i Auth-Def

bsns-3750-5#
```

Open-modus

In de vorige sectie werd het gedrag voor ACLâ€™s beschreven (waaronder de standaardmodus voor open modus). Het gedrag voor de open modus is:

- het staat voor al verkeer (volgens standaard auth-default-ACL-OPEN) toe wanneer de sessie in een onbevoegde staat is.
- de sessie is onbevoegd tijdens de verificatie/autorisatie (goed voor de opstartscenario's van Encryption Applicatie Model E (PXE)) of na het mislukken van dat proces (goed voor scenario's die "low impact mode" worden genoemd).
- wanneer de sessie naar de geautoriseerde status voor meerdere platforms wordt verplaatst, worden ACLâ€™s aaneengeschakeld en wordt de eerste DACL gebruikt, en vervolgens de interface-ACL.
- voor multi-auth of multi-domein zijn er mogelijk meerdere sessies tegelijkertijd in verschillende toestanden (dan is het verschillende ACL-type van toepassing voor elke sessie).

Wanneer interface-ACL verplicht is

Voor meerdere 6500/4500-platforms is de interface-ACL verplicht om de DACL correct toe te passen.

Hier is een voorbeeld met 4500 sup2 12.2.53SG6, geen interface ACL:

<#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
```

Nadat de host is geverifieerd, wordt de DACL gedownload. Het wordt niet toegepast en autorisatie mislukt.

<#root>

*Apr 25 04:38:05.239: RADIUS: Received from id 1645/19 10.48.66.74:1645,

Access-Accept,

```
 len 209
*Apr 25 04:38:05.239: RADIUS:  authenticator 35 8E 59 E4 D5 CF 8F 9A -
 EE 1C FC 5A 9F 67 99 B2
*Apr 25 04:38:05.239: RADIUS:  User-Name           [1]   41
  "
```

#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1

```
"
*Apr 25 04:38:05.239: RADIUS:  State               [24]  40
*Apr 25 04:38:05.239: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 61
  [ReauthSession:0a]
*Apr 25 04:38:05.239: RADIUS:   33 30 34 32 34 61 30 30 30 45 46 35 30 46 35 33
  [30424a000EF50F53]
*Apr 25 04:38:05.239: RADIUS:   35 41 36 36 39 33            [ 5A6693]
*Apr 25 04:38:05.239: RADIUS:  Class               [25]  54
*Apr 25 04:38:05.239: RADIUS:   43 41 43 53 3A 30 61 33 30 34 32 34 61 30 30 30
  [CACS:0a30424a000]
*Apr 25 04:38:05.239: RADIUS:   45 46 35 30 46 35 33 35 41 36 36 39 33 3A 69 73
  [EF50F535A6693:is]
*Apr 25 04:38:05.239: RADIUS:   65 32 2F 31 38 30 32 36 39 35 33 38 2F 31 32 38
  [e2/180269538/128]
*Apr 25 04:38:05.239: RADIUS:   36 35 35 33              [ 6553]
*Apr 25 04:38:05.239: RADIUS:  Message-Authenticato[80]  18
*Apr 25 04:38:05.239: RADIUS:   AF 47 E2 20 65 2F 59 39 72 9A 61 5C C5 8B ED F5
         [ G e/Y9ra\]
*Apr 25 04:38:05.239: RADIUS:  Vendor, Cisco       [26]  36
*Apr 25 04:38:05.239: RADIUS:   Cisco AVpair       [1]   30
  "
```

ip:inacl#1=permit ip any any

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

EPM_SESS_ERR:Failed to apply ACL to interface

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

%AUTHMGR-5-FAIL: Authorization failed for client
(0007.5032.6941) on Interface Gi2/3
AuditSessionID 0A3043450000000060012C050

```
brisk#
```

show authentication sessions

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

Authz Failed

```
   0A3043450000000060012C050
```

Nadat de interface ACL is toegevoegd:

<#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
```

De verificatie en autorisatie worden uitgevoerd en de DACL wordt correct toegepast:

<#root>

```
brisk#
```

show authentication sessions

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

Authz Success

```
  0A3043450000008001A2CE4
```

Het gedrag is niet afhankelijk van "open authentificatie". Om DACL te accepteren hebt u de interface-ACL nodig voor zowel open als gesloten modus.

DACL-code op 4500/6500

Op de 4500/6500 wordt DACL toegepast met acl_snoop DACLâ€™s. Hier wordt een voorbeeld met 4500 sup2 12.2.53SG6 (phone + PC) weergegeven. Er is een afzonderlijke ACL voor spraak (10) en gegevens (100) VLAN:

<#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
```

ACLâ€™s zijn specifiek omdat IPDT de juiste vermeldingen heeft:

<#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
```

Geverifieerde sessies bevestigen de adressen:

<#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
```

In dit stadium reageren zowel de pc als de telefoon op ICMP-echo, maar de interface-ACL bevat alleen:

<#root>

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

192.168.10.12

```
 any
```

Waarom? Omdat DACL alleen voor de telefoon is ingedrukt (192.168.10.12). Voor de PC wordt de interface-ACL met open modus gebruikt:

<#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)
```

Samenvattend, wordt acl_snoop gemaakt voor zowel de PC als de telefoon, maar DACL wordt alleen voor de telefoon teruggegeven. Dat is waarom die ACL als gebonden aan de interface wordt gezien.

MAC-adresstatus voor 802.1x

Wanneer 802.1x-verificatie start, wordt het MAC-adres nog steeds als DYNAMIC gezien, maar actie voor dat pakket is 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
```

Na succesvolle verificatie wordt het MAC-adres statisch en wordt het poortnummer opgegeven:

```
<#root>
bsns-3750-5#
```

```
show authentication sessions


Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/0/1

0007.5032.6941

  mab      VOICE

Authz Success

  C0A800010000596479F4DCE

bsns-3750-5#

show mac address-table interface g1/0/1


          Mac Address Table
-------------------------------------------

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

0007.5032.6941    STATIC      Gi1/0/1
```

Dat geldt voor alle mab/dot1x-sessies voor beide domeinen (SPRAAK/DATA).

Problemen oplossen

Vergeet niet om de 802.1x configuratiegids te lezen voor uw specifieke softwareversie en platform.

Als u een TAC-case opent, specificeert u de uitvoer van deze opdrachten:

- show tech
- details van verificatiesessie-interface weergeven <xx>
- MAC-adrestabelinterface tonen <xx>

Het is ook goed om een SPAN-poortpakketopname te verzamelen en deze debuggen:

- debug radius verbose
- debug epm all
- debug verificatie alle
- debug dot1x alles
- Debug verificatiefunctie <yy> all
- debug aaa authentication
- debug aaa-autorisatie

Gerelateerde informatie

- **802.1X security servicesconfiguratiehandleiding, Cisco IOS XE release 3SE (Catalyst 3850 Switches)**

- **Catalyst 3750-X en Catalyst 3560-X Switch softwareconfiguratiehandleiding, Cisco IOS-softwarerelease 15.2(1)E**
- **Catalyst 3750-X en 3560-X softwareconfiguratiehandleiding, release 15.0(1)SE**
- **Catalyst 3560 softwareconfiguratiehandleiding, release 12.2(52)SE**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.