Comprensione del comportamento di DACL 802.1x, ACL per utente, Filter-ID e Device Tracking

Sommario

Introduzione

In questo documento viene descritta la funzione di rilevamento dei dispositivi IP, i trigger per l'aggiunta e la rimozione di un host e l'impatto del rilevamento dei dispositivi sull'elenco DACL 802.1x.

Teoria di Device Tracking

In questo documento vengono descritti la funzionalità di monitoraggio dei dispositivi IP e i trigger per aggiungere o rimuovere un host.

Inoltre, viene spiegato l'impatto del rilevamento dei dispositivi sull'elenco DACL (Downloadable Access Control List) 802.1x.

Il comportamento cambia tra le versioni e le piattaforme.

La seconda parte del documento si concentra sull'Access Control List (ACL) restituito dal server Authentication, Authorization, and Accounting (AAA) e applicato alla sessione 802.1x.

Viene presentato un confronto tra l'ACL DACL, l'ACL Per Utente e l'ACL Filter-ID.

Inoltre, vengono discussi alcuni avvertimenti relativi alla riscrittura dell'ACL e all'ACL predefinito.

Il rilevamento dispositivi aggiunge una voce quando:

- impara la nuova voce tramite lo snooping DHCP.
- impara la nuova voce tramite una richiesta ARP (Address Resolution Protocol) (legge l'indirizzo MAC del mittente e l'indirizzo IP del mittente dal pacchetto ARP).

Questa funzionalità è talvolta denominata ispezione ARP, ma non è la stessa della funzione DAI (Dynamic ARP Inspection).

Questa funzionalità è abilitata per impostazione predefinita e non può essere disabilitata. Viene anche denominato snooping ARP, ma i debug non lo mostrano dopo l'attivazione di "debug arp snooping".

Lo snooping ARP è abilitato per impostazione predefinita e non può essere disabilitato o controllato.

La voce viene rimossa quando non vi è risposta per una richiesta ARP (per impostazione predefinita, ogni 30 secondi viene inviata una sonda per ciascun host nella tabella di rilevamento dei dispositivi).

Configurazione di Device Tracking

```
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
```

Test di Device Tracking

<#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
```

Debug della versione 12.2.33, rilevamento dispositivi IP aggiornato dallo snooping DHCP

Lo snooping DHCP popola la tabella di binding:

<#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
```

Dopo l'aggiunta del binding DHCP al database, viene attivata la notifica per il rilevamento dei dispositivi:

```
<#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
```

Le sonde ARP vengono inviate per impostazione predefinita ogni 30 secondi:

<#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
```

Dopo la rimozione della voce dalla tabella di rilevamento dei dispositivi, la voce di binding DHCP corrispondente rimane disponibile:

<#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
```

Il problema si verifica quando si dispone di una risposta ARP, ma la voce di rilevamento del dispositivo viene rimossa comunque.

Tale bug è presente nella versione 12.2.3 e non è stato rilevato nel software versione 12.2.5 o 15.x.

Esistono inoltre alcune differenze quando si utilizza la porta L2 (access-port) e la porta L3 (no switchport).

Snooping probe e ARP

Tracciamento dei dispositivi con la funzione di snooping 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
```

IP Device Tracking per la versione 12.2.5 - Comando nascosto

Per la versione 12.2, usare un comando nascosto per attivarlo:

<#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
```

Tracciamento dispositivi IP per la versione 12.2.5 - Esempio di IP statico

Nell'esempio, il PC è stato configurato con un indirizzo IP statico. I debug mostrano che dopo aver ricevuto una risposta ARP (MSG=2), la voce di rilevamento del dispositivo viene aggiornata.

<#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
```

Ogni richiesta ARP proveniente dal PC aggiorna quindi la tabella di rilevamento del dispositivo (l'indirizzo MAC del mittente e l'indirizzo IP del mittente dal pacchetto ARP).

IP Device Tracking per la versione 15.x

È importante ricordare che alcune funzionalità, ad esempio DACL per 802.1x, non sono supportate nella versione LAN Lite (attenzione: Cisco Feature Navigator non mostra sempre le informazioni corrette).

Il comando nascosto della versione 12.2 può essere eseguito, ma non ha alcun effetto. Nel software versione 15.x, per impostazione predefinita il rilevamento dei dispositivi IP (IPDT) è abilitato solo per le interfacce con 802.1x abilitato:

<#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

Dopo la rimozione della configurazione 802.1x dalla porta, anche IPDT viene rimosso da tale porta.

Poiché lo stato della porta può essere "DOWN", è necessario disporre di "switchport mode access" e "authentication port-control auto" per attivare il rilevamento dei dispositivi IP su questa porta.

Il limite massimo di dispositivi di interfaccia è impostato su 10:

<#root>

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

ip device tracking maximum

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

Tracciamento dispositivi IP per Cisco IOS-XE®

Anche in questo caso, il comportamento di Cisco IOS-XE 3.3 è cambiato rispetto a quello di Cisco IOS versione 15.x.

Il comando nascosto della versione 12.2 è obsoleto, ma ora viene restituito questo errore:

<#root>

```
3850-1#
```

no ip device tracking int g1/0/48

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

In Cisco IOS-XE, il rilevamento dei dispositivi è attivato per tutte le interfacce (anche quelle in cui non è configurato 802.1x):

<#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)
```

Inoltre, non ci sono limiti alle voci massime per porta (0 significa disabilitato).

IP Device Tracking con 802.1x e DACL per la versione 12.2.5

Se 802.1x è configurato con DACL, la voce di rilevamento del dispositivo viene utilizzata per compilare l'indirizzo IP del dispositivo.

Nell'esempio viene mostrato come controllare il dispositivo che funziona con un IP configurato staticamente:

<#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
```

Questa è una sessione 802.1x compilata con il DACL "allow icmp any" (consenti icmp 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
```

Di seguito viene mostrato un ACL applicato:

```
<#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)
```

Inoltre, l'ACL sull'interfaccia fa0/1 è lo stesso:

```
<#root>

BSNS-3560-1#

show ip access-lists interface fa0/1


     permit icmp any any
```

Anche se l'impostazione predefinita è 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
```

Per l'ACL, è previsto l'uso di "qualsiasi" come 192.168.0.244. Funziona così per il proxy di autenticazione, ma per 802.1x DACL src "any" (qualsiasi) non viene modificato nell'IP rilevato del PC.

Per il proxy di autenticazione, un ACL originale viene memorizzato nella cache e mostrato con il comando show ip access-list e un ACL specifico (per utente con IP specifico) viene applicato all'interfaccia con il comando show ip access-list interface fa0/1. Tuttavia, auth-proxy non utilizza il

rilevamento IP dei dispositivi.

Cosa succede se l'indirizzo IP non viene rilevato correttamente? Dopo aver disattivato la funzione di rilevamento dei dispositivi:

<#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
```

Quindi non viene collegato alcun indirizzo IP, ma il DACL è ancora applicato:

<#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 questo scenario, non è necessario il rilevamento dei dispositivi per 802.1x. L'unica differenza è che la conoscenza anticipata dell'indirizzo IP del client può essere utilizzata per una richiesta di accesso RADIUS. Dopo aver applicato l'attributo 8:

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

Esiste in Access-Request e in ACS ed è possibile creare regole di autorizzazione più granulari:

```
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
```

Tenere presente che TrustSec richiede anche il rilevamento dei dispositivi IP per i binding IP a SGT.

IP Device Tracking con 802.1x e DACL per la versione 15.x

Qual è la differenza tra la versione 15.x e la versione 12.2.55 in DACL? Nel software versione 15.x, funziona come per auth-proxy.

L'ACL generico può essere visualizzato quando si immette il comando show ip access-list (risposta memorizzata nella cache dal server AAA), ma dopo il comando show ip access-list interface fa0/1, l'indirizzo src "any" viene sostituito dall'indirizzo IP di origine dell'host (noto come IP device tracking).

Questo è l'esempio di telefono e PC su una porta (g1/0/1), software versione 15.0.2SE2 su 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:  C0A800010000001012B680D23
      Acct Session ID:  0x0000017B
               Handle:  0x99000102

Runnable methods list:
       Method   State
       dot1x    Failed over
```

mab

Authc Success

```
----------------------------------------
            Interface:  GigabitEthernet1/0/1
          MAC Address:
```

0050.5699.4ea1

```
           IP Address:
```

192.168.2.200

```
            User-Name:
```

cisco

```
               Status:  Authz Success
               Domain:
```

DATA

```
      Security Policy:  Should Secure
      Security Status:  Unsecure
```

```
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:

 20


              ACS ACL:

xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2


      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80001000001BD336EC4D6
      Acct Session ID:  0x000002F9
               Handle:  0xF80001BE


Runnable methods list:
       Method   State


  dot1x    Authc Success


       mab      Not run
```

Il telefono viene autenticato tramite MAC Authentication Bypass (MAB), mentre il PC utilizza dot1x. Sia il telefono che il PC utilizzano lo stesso 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
```

Tuttavia, una volta verificata a livello di interfaccia, l'origine è stata sostituita dall'indirizzo IP del dispositivo.

Il rilevamento dei dispositivi IP attiva la modifica e può verificarsi in qualsiasi momento (molto più tardi rispetto alla sessione di autenticazione e al download dell'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
```

Entrambi gli indirizzi MAC sono contrassegnati come statici:

```
<#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
```

Voce ACL specifica

Quando l'origine "any" (qualsiasi) nel DACL viene sostituita con l'indirizzo IP dell'host? Solo quando vi sono almeno due sessioni sulla stessa porta (due supplicant).

Non è necessario sostituire l'origine "any" quando è presente una sola sessione.

I problemi si verificano quando sono presenti più sessioni e per non tutte le sessioni, il rilevamento dei dispositivi IP conosce l'indirizzo IP dell'host. In questo scenario è ancora "qualsiasi" per alcune voci.

Quel comportamento è diverso su alcune piattaforme. Ad esempio, sullo switch 2960X con versione 15.0(2)EX, l'ACL è sempre specifico anche quando è presente una sola sessione di autenticazione per porta.

Tuttavia, sugli switch 3560X e 3750X versione 15.0(2)SE, sono necessarie almeno due sessioni per rendere specifico l'ACL.

Control-Direction

Per impostazione predefinita, la direzione del controllo è di tipo both:

```
<#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
```

Ciò significa che prima dell'autenticazione del richiedente, il traffico non può essere inviato da o verso la porta. Per la modalità "in", il traffico avrebbe potuto essere inviato dalla porta al supplicant, ma non dal supplicant alla porta (potrebbe essere utile per la funzione WAKE on LAN).

Tuttavia, lo switch applica l'ACL solo nella direzione "in". Non importa quale modalità viene utilizzata.

```
<#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
```

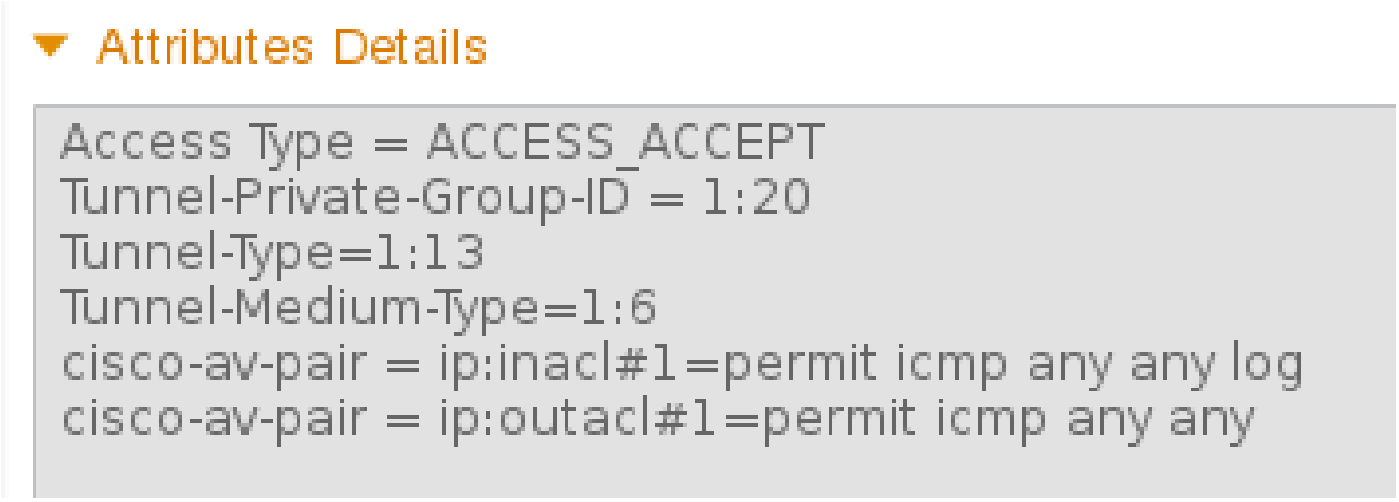
Ciò significa in pratica che dopo l'autenticazione, l'ACL viene applicato al traffico diretto alla porta

e tutto il traffico proveniente dalla porta (direzione in uscita).

Tracciamento dispositivi IP con 802.1x e ACL per utente per la versione 15.x

È possibile anche usare un ACL per utente, passato in "ip:inacl" e "ip:outacl" di cisco-av-pair.

Questa configurazione di esempio è simile a una precedente, ma questa volta il telefono usa il DACL e il PC usa l'ACL Per Utente. Il profilo ISE per il PC è:



Sul telefono è ancora applicato il DACL:

<#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

Tuttavia, il PC sulla stessa porta usa l'ACL Per Utente:

<#root>

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

192.168.2.200

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

DATA

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

Per-User ACL: permit icmp any any log

```
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8000100000056743114008
      Acct Session ID:  0x000006D1
               Handle:  0x9D000568
```

Per verificare in che modo viene unito sulla 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
```

La prima voce è stata presa dall'ACL Per-User (notare la parola chiave log), la seconda voce è stata presa dall'ACL.

Entrambe vengono riscritte dal rilevamento del dispositivo IP per l'indirizzo IP specifico.

È possibile verificare l'ACL per utente con il 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 anche tramite il 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
```

Informazioni sull'attributo ip:outacl È completamente omesso nella versione 15.x. L'attributo è stato ricevuto, ma lo switch non applica/elabora l'attributo.

Differenza rispetto all'elenco DACL

Come indicato nell'ID bug Cisco CSCut25702, il comportamento dell'ACL per utente è diverso da quello del DACL.

Un DACL con una sola voce ("allow ip any any") e un supplicant connesso a una porta può funzionare correttamente senza che sia abilitato il rilevamento dei dispositivi IP.

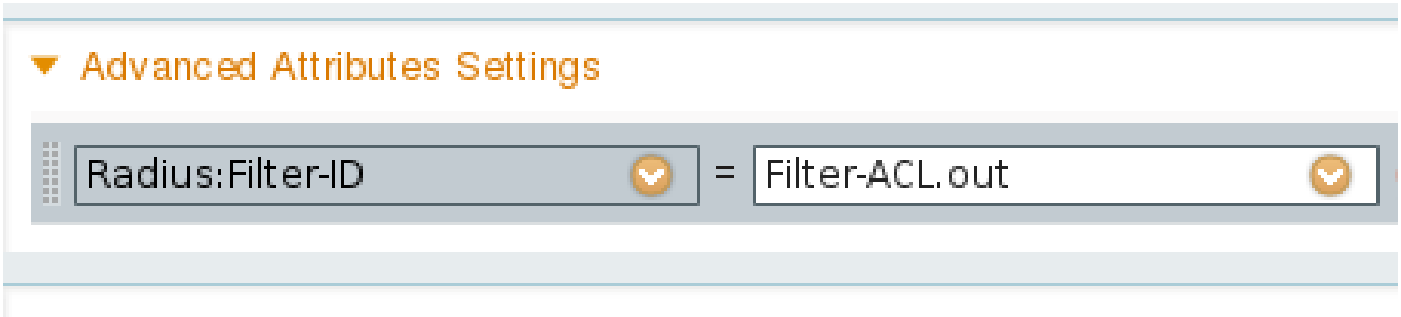
L'argomento "any" (qualsiasi) non viene sostituito e tutto il traffico è autorizzato. Tuttavia, per l'ACL per utente, è obbligatorio avere la registrazione dei dispositivi IP abilitata.

Se è disabilitata e ha solo la voce "allow ip any any" e un supplicant, tutto il traffico viene bloccato.

IP Device Tracking con 802.1x e ACL Filter-ID per la versione 15.x

Inoltre, è possibile utilizzare l'attributo IETF filter-id [11]. Il server AAA restituisce il nome ACL, definito localmente sullo switch. Il profilo ISE potrebbe avere questo aspetto:

È necessario specificare la direzione (in o out). A tale scopo, è necessario aggiungere l'attributo manualmente:



Quindi il 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
```

L'ACL viene mostrato anche per la sessione autenticata:

<#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
```

Inoltre, quando l'ACL è associato all'interfaccia:

```
<#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
```

È possibile unire questo ACL con altri tipi di ACL sulla stessa interfaccia. Ad esempio, se sulla stessa porta dello switch è presente un altro supplicant che ottiene il DACL dall'ISE: "allow ip any any", è possibile visualizzare:

```
<#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
```

Notare che il rilevamento del dispositivo IP riscrive l'IP di origine per ciascuna origine (supplicant).

E per quanto riguarda l'elenco dei filtri di uscita? Anche in questo caso (come ACL per utente), non viene utilizzato dallo switch.

Tracciamento dispositivi IP - Valori predefiniti e best practice

Per le versioni precedenti alla 15.2(1)E, prima di poter usare IPDT, una funzionalità deve essere abilitata a livello globale con questo comando CLI:

```
<#root>

(config)#

ip device tracking
```

Nelle versioni 15.2(1)E e successive, il comando ip device tracking non è più necessario. IPDT è abilitato solo se è abilitato da una funzionalità che si basa su di esso.

Se nessuna funzionalità abilita IPDT, IPDT è disabilitato. Il comando "no ip device tracking" non ha alcun effetto. La funzionalità specifica dispone del controllo per abilitare/disabilitare IPDT.

Quando si abilita IPDT, è necessario tenere presente il problema relativo al duplicato dell'indirizzo IP in . Per ulteriori informazioni, vedere Risoluzione dei messaggi di errore "Duplicate IP Address

0.0.0.0".

Si consiglia di disabilitare IPDT su una porta trunk:

<#root>

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

Nelle versioni successive di Cisco IOS, il comando è diverso:

<#root>

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

Si consiglia di abilitare IPDT sulla porta di accesso e ritardare le sonde ARP in modo da evitare il problema di "Duplicate IP Address" (Duplicazione indirizzo IP):

<#root>

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

Riscrittura ACL di interfaccia per la versione 15.x

Per l'ACL di interfaccia, funziona prima dell'autenticazione:

<#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
```

Tuttavia, dopo l'autenticazione riuscita, l'ACL viene riscritto (sovrascritto) dall'ACL restituito dal server AAA (non importa se è DACL, ip:inacl o filterid).

L'ACL (test1) può bloccare il traffico (che normalmente sarebbe autorizzato in modalità aperta), ma dopo l'autenticazione non è più importante.

Anche se il server AAA non restituisce alcun ACL, l'ACL dell'interfaccia viene sovrascritto e viene fornito l'accesso completo.

Ciò è leggermente fuorviante in quanto la memoria TCAM (Ternary Content Addressable Memory) indica che l'ACL è ancora associato a livello di interfaccia.

Di seguito è riportato un esempio della versione 15.2.2 su 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
```

Queste informazioni sono valide solo per il livello di interfaccia e non per il livello di sessione. Di seguito vengono riportate alcune ulteriori informazioni (con un ACL composto):

```
<#root>

bsns-3750-6#

show ip access-lists interface g1/0/2
```

```
permit ip host 192.168.1.203 any

Extended IP access list
test1

 10 permit icmp host x.x.x.x host n.n.n.n
```

La prima voce viene creata come DACL "allow ip any any" (consenti ip qualsiasi) e viene restituita per la corretta autenticazione (e "any" viene sostituito da una voce della tabella di rilevamento dei dispositivi).

La seconda voce è il risultato dell'ACL dell'interfaccia e viene applicata a tutte le nuove autenticazioni (prima dell'autorizzazione).

Sfortunatamente, (anche in questo caso dipende dalla piattaforma) entrambi gli ACL sono concatenati. Ciò accade nella versione 15.2.2 del 3750X.

Ciò significa che per le sessioni autorizzate vengono applicate entrambe. Posizionare il primo ACL sull'elenco DACL e il secondo ACL sull'interfaccia.

Ecco perché quando si aggiunge l'esplicito "deny ip any any", il DACL non prende in considerazione l'ACL dell'interfaccia.

In genere, nell'elenco DACL non è presente alcuna negazione esplicita e quindi l'ACL dell'interfaccia viene applicato dopo tale negazione.

Il comportamento della versione 15.0.2 sullo switch 3750X è lo stesso, ma il comando sh ip access-list interface non visualizza più l'ACL dell'interfaccia (ma è ancora concatenato all'ACL dell'interfaccia, a meno che non esista un rifiuto esplicito nell'ACL).

ACL predefinito usato per 802.1x

Sono disponibili due tipi di ACL predefiniti:

- auth-default-ACL-OPEN - utilizzato per la modalità open
- auth-default-ACL - utilizzato per l'accesso chiuso

Quando la porta è in stato non autorizzato, vengono utilizzati sia auth-default-ACL che auth-default-ACL-OPEN. Per impostazione predefinita, viene utilizzato l'accesso chiuso.

Ciò significa che prima dell'autenticazione tutto il traffico viene scartato, ad eccezione di quello autorizzato dall'ACL auth-default-ACL.

In questo modo, il traffico DHCP viene autorizzato prima del completamento dell'autorizzazione.

L'indirizzo IP viene allocato e l'elenco DACL scaricato può essere applicato correttamente.

L'ACL viene creato automaticamente e non può essere trovato nella configurazione.

<#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
```

Viene creata dinamicamente per la prima autenticazione (tra la fase di autenticazione e quella di autorizzazione) e rimossa dopo la rimozione dell'ultima sessione.

Auth-Default-ACL consente solo il traffico DHCP. Una volta completata l'autenticazione e scaricato il nuovo DACL, questo viene applicato alla sessione.

Quando la modalità viene modificata in open, viene visualizzato auth-default-ACL-OPEN, che viene utilizzato e funziona esattamente come 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
```

Entrambi gli ACL possono essere personalizzati, ma non vengono mai visualizzati nella configurazione.

```
<#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#
```

Modalità di apertura

Nella sezione precedente è stato descritto il comportamento degli ACL (incluso quello utilizzato per impostazione predefinita per la modalità di apertura). Il comportamento per la modalità di apertura è il seguente:

- consente tutto il traffico (in base all'impostazione predefinita, auth-default-ACL-OPEN) quando la sessione è in uno stato non autorizzato.
- la sessione si trova in uno stato non autorizzato durante l'autenticazione/autorizzazione (indicato per gli scenari di avvio di Encryption Appliance Model E (PXE)) o dopo che il processo ha esito negativo (indicato per gli scenari definiti "modalità a basso impatto").
- quando la sessione passa allo stato autorizzato per più piattaforme, gli ACL vengono concatenati e viene usato il primo DACL, quindi l'ACL di interfaccia.
- in modalità multi-auth o multi-dominio possono esistere più sessioni contemporaneamente in stati diversi (a ogni sessione viene applicato un tipo di ACL diverso).

Quando l'ACL dell'interfaccia è obbligatorio

Per più piattaforme 6500/4500, l'ACL dell'interfaccia è obbligatorio per applicare correttamente il DACL.

Di seguito è riportato un esempio di switch 4500 sup2 12.2.53SG6, senza ACL di interfaccia:

<#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
```

Dopo l'autenticazione dell'host, viene scaricato il DACL. Non viene applicata e l'autorizzazione non viene concessa.

<#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
```

Dopo aver aggiunto l'ACL dell'interfaccia:

<#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
```

L'autenticazione e l'autorizzazione hanno esito positivo e l'elenco DACL viene applicato correttamente:

```
<#root>

brisk#

show authentication sessions


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

 Authz Success

  0A30434500000008001A2CE4
```

Il comportamento non dipende da "authentication open". Per accettare l'elenco DACL, occorre avere l'ACL di interfaccia per la modalità aperta o chiusa.

DACL su 4500/6500

Sugli switch serie 4500/6500, il DACL viene applicato con gli ACL_snoop. Di seguito è riportato un esempio di switch 4500 sup2 12.2.53SG6 (telefono + PC). Esiste un ACL separato per la VLAN voce (10) e dati (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
```

Gli ACL sono specifici perché IPDT ha le voci corrette:

<#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
```

Le sessioni autenticate confermano gli indirizzi:

<#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 questa fase, sia il PC che il telefono rispondono all'eco ICMP, ma l'ACL dell'interfaccia presenta solo:

<#root>

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

192.168.10.12

```
 any
```

Perché? Perché è stato premuto il DACL solo per il telefono (192.168.10.12). Per il PC, viene usato l'ACL di interfaccia con modalità di apertura:

<#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)
```

Per riassumere, acl_snoop viene creato sia per il PC che per il telefono, ma l'elenco DACL viene restituito solo per il telefono. Ecco perché quell'ACL è visto come associato all'interfaccia.

Stato indirizzo MAC per 802.1x

Quando viene avviata l'autenticazione 802.1x, l'indirizzo MAC viene ancora visualizzato come DYNAMIC ma l'azione per il pacchetto è 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
```

Una volta completata l'autenticazione, l'indirizzo MAC diventa statico e viene fornito il numero di porta:

```
<#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
```

Ciò è valido per tutte le sessioni mab/dot1x per entrambi i domini (VOICE/DATA).

Risoluzione dei problemi

Leggere la guida alla configurazione 802.1x per la versione software e la piattaforma in uso.

Se si apre una richiesta TAC, fornire l'output dei seguenti comandi:

- show tech
- visualizzazione dettagli interfaccia sessione di autenticazione <xx>
- show mac address-table interface <xx>

Inoltre, è utile raccogliere un'acquisizione di pacchetti sulla porta SPAN e i seguenti debug:

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

Informazioni correlate

- Guida alla configurazione dei servizi di autenticazione 802.1X, Cisco IOS XE release 3SE (switch Catalyst 3850)
- Guida alla configurazione dei software degli switch Catalyst 3750-X e Catalyst 3560-X, Cisco IOS versione 15.2(1)E
- Guida alla configurazione del software Catalyst 3750-X e 3560-X, versione 15.0(1)SE
- Guida alla configurazione del software Catalyst 3560, versione 12.2(52)SE
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).