802.1x-DACL, benutzerspezifische ACL, Filter-ID und Geräteverfolgung

Inhalt

Einführung

In diesem Dokument wird die Funktionsweise der IP-Geräteverfolgungsfunktion beschrieben. Dazu gehört auch, was die Auslöser für das Hinzufügen und Entfernen eines Hosts sind. Außerdem werden die Auswirkungen der Geräteverfolgung auf die herunterladbare 802.1x-Zugriffskontrollliste (DACL) erläutert. Das Verhalten ändert sich zwischen Versionen und Plattformen.

Der zweite Teil des Dokuments konzentriert sich auf die Zugriffskontrollliste (ACL), die vom AAA-

Server (Authentication, Authorization, Accounting) zurückgegeben und auf die 802.1x-Sitzung angewendet wird. Es wird ein Vergleich zwischen der DACL, der benutzerspezifischen ACL und der Filter-ID-ACL angezeigt. Darüber hinaus werden einige Vorbehalte bezüglich der Neufassung von Zugriffskontrolllisten und der Standard-Zugriffskontrolllisten erörtert.

Geräteverfolgungstheorie

Die Geräteverfolgung fügt einen Eintrag hinzu, wenn:

- wird der neue Eintrag über DHCP Snooping abgerufen.
- Er empfängt den neuen Eintrag über eine ARP-Anfrage (Address Resolution Protocol) (liest die Absender-MAC-Adresse und die Absender-IP-Adresse aus dem ARP-Paket). Diese Funktion wird manchmal ARP-Inspektion genannt, ist jedoch nicht mit Dynamic ARP Inspection (DAI) identisch. Diese Funktion ist standardmäßig aktiviert und kann nicht deaktiviert werden. Sie wird auch ARP-Snooping genannt, wird aber nach Aktivierung von "debug arp snooping" nicht angezeigt. ARP-Snooping ist standardmäßig aktiviert und kann nicht deaktiviert oder gesteuert werden.

Die Geräteverfolgung entfernt einen Eintrag, wenn keine Antwort für eine ARP-Anfrage vorliegt (in der Geräteverfolgungstabelle wird standardmäßig alle 30 Sekunden eine Anfrage für jeden Host gesendet).

Geräteverfolgungskonfiguration

```
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
```

Geräteüberwachungstests

```
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 aus Version 12.2.33, IP-Geräteverfolgung aktualisiert durch DHCP-Snooping

DHCP Snooping füllt die Bindungstabelle aus:

```
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
```

Nachdem die DHCP-Bindung der Datenbank hinzugefügt wurde, wird die Benachrichtigung für die Geräteverfolgung ausgelöst:

```
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-Tests werden standardmäßig alle 30 Sekunden gesendet:

```
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
```

Nachdem der Eintrag aus der Geräteverfolgungstabelle entfernt wurde, ist der entsprechende DHCP-Bindungseintrag immer noch vorhanden:

```
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
```

Es besteht das Problem, wenn Sie eine ARP-Antwort haben, der Eintrag für die Geräteverfolgung jedoch trotzdem entfernt wird. Dieser Fehler scheint in Version 12.2.33 zu liegen und wurde in Version 12.2.55 oder 15.x nicht angezeigt.

Außerdem gibt es einige Unterschiede bei der Handhabung des L2-Ports (Access-Port) und des L3-Ports (kein Switch-Port).

Probe- und ARP-Snooping

Geräteverfolgung mit der ARP-Snooping-Funktion:

```
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-Geräteverfolgung für Version 12.2.55 - Versteckter Befehl

In Version 12.2 kann es erforderlich sein, einen ausgeblendeten Befehl zu verwenden, um ihn zu aktivieren:

```
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-Geräteverfolgung für Version 12.2.55 - Statisches IP-Beispiel

In diesem Beispiel wurde der PC mit einer statischen IP-Adresse konfiguriert. Debugs zeigen, dass der Eintrag für die Geräteverfolgung aktualisiert wird, nachdem Sie eine ARP-Antwort (MSG=2) erhalten haben.

```
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
```

So aktualisiert jede ARP-Anfrage vom PC die Geräteverfolgungstabelle (die Absender-MAC-Adresse und Absender-IP-Adresse vom ARP-Paket).

IP-Geräteverfolgung für Version 15.x

Beachten Sie, dass einige Funktionen wie DACL für 802.1x in der LAN Lite-Version nicht unterstützt werden (Vorsicht: Cisco Feature Navigator zeigt nicht immer die richtigen Informationen an).

Der ausgeblendete Befehl aus Version 12.2 kann ausgeführt werden, hat jedoch keine Auswirkungen. In der Softwareversion 15.x ist die IP-Geräteverfolgung (IPDT) standardmäßig nur für die Schnittstellen aktiviert, für die 802.1x aktiviert ist:

```
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
```

Nach dem Entfernen der 802.1x-Konfiguration aus dem Port wird IPDT ebenfalls aus diesem Port entfernt. Der Port-Status kann "DOWN" lauten. Daher ist es erforderlich, "switchport mode access" und "authentication port-control auto" zu haben, damit die IP-Geräteverfolgung an diesem Port aktiviert wird. Der Grenzwert für das Schnittstellengerät ist auf 10 festgelegt:

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

IP-Geräteverfolgung für Cisco IOS-XE®

Auch hier hat sich das Verhalten von Cisco IOS-XE 3.3 gegenüber Cisco IOS Version 15.x geändert. Der ausgeblendete Befehl aus Version 12.2 ist veraltet, aber jetzt wird dieser Fehler zurückgegeben:

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

In Cisco IOS-XE wird die Geräteverfolgung für alle Schnittstellen aktiviert (auch für die Schnittstellen, für die 802.1x nicht konfiguriert ist):

```
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)
```

Außerdem gibt es keine Beschränkungen für maximale Einträge pro Port (0 bedeutet deaktiviert).

IP-Geräteverfolgung mit 802.1x und DACL für Version 12.2.55

Wenn 802.1x mit DACL konfiguriert ist, wird der Geräteverfolgungseintrag verwendet, um die IP-Adresse des Geräts auszufüllen. Dieses Beispiel zeigt, wie die Geräteverfolgung für eine statisch konfigurierte IP funktioniert:

```
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
```

Dies ist eine 802.1x-Sitzung mit der Funktion "permit icmp any any"-DACL:

```
BSNS-3560-1# sh authentication sessions  interface fa0/1
           Interface:  FastEthernet0/1
         MAC Address:  0050.5699.4ea1
          IP Address:  192.168.0.244
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  2
              ACS ACL:  xACSACLx-IP-DACL-516c2694
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A3042A900000008008900C5
     Acct Session ID:  0x0000000D
              Handle:  0x19000008

Runnable methods list:
      Method   State
      dot1x    Authc Success

BSNS-3560-1#show epm session summary
EPM Session Information
-----------------------
Total sessions seen so far : 1
Total active sessions      : 1

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

Dies zeigt eine angewendete ACL:

```
 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)
```

Außerdem ist die ACL auf der Schnittstelle fa0/1 identisch:

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

Der Standardwert ist 802.1x ACL:

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

Es kann davon ausgegangen werden, dass die ACL "any" als 192.168.0.244 verwendet. Das funktioniert für den Authentifizierungsproxy, aber für 802.1x DACL src "any" wird nicht auf die erkannte IP des PCs geändert.

Für den Authentifizierungsproxy wird eine ursprüngliche ACL aus dem ACS zwischengespeichert und mit dem Befehl **show ip access-list** angezeigt. Auf der Schnittstelle mit dem Befehl **show ip access-list interface fa0/1** wird eine spezifische ACL (pro Benutzer mit spezifischer IP) angewendet. Der auth-Proxy verwendet jedoch keine Geräte-IP-Verfolgung.

Was geschieht, wenn die IP-Adresse nicht richtig erkannt wird? Nachdem die Geräteverfolgung deaktiviert wurde:

```
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
```

Es wird also keine IP-Adresse angehängt, aber die DACL wird weiterhin angewendet:

```
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 diesem Szenario ist die Geräteverfolgung für 802.1x nicht erforderlich. Der einzige Unterschied besteht darin, dass die IP-Adresse des Clients im Voraus für eine RADIUS-Zugriffsanfrage verwendet werden kann. Nachdem Attribut 8 angefügt wurde:

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

Es wird in Access Request und auf ACS möglich sein, detailliertere Autorisierungsregeln zu erstellen:

```
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
```

Beachten Sie, dass TrustSec auch die IP-Geräteverfolgung für IP-zu-SGT-Bindungen benötigt.

IP-Geräteverfolgung mit 802.1x und DACL für Version 15.x

Worin besteht der Unterschied zwischen Version 15.x und Version 12.2.55 in DACL? In der Software Version15.x funktioniert es genauso wie bei auth-proxy. Die generische ACL wird angezeigt, wenn der Befehl **show ip access-list** eingegeben wird (zwischengespeicherte Antwort von AAA). Nach dem Befehl **show ip access-list interface fa0/1** wird der Befehl src "any" durch die Quell-IP-Adresse des Hosts ersetzt (bekannt über IP-Geräte-Tracking).

Dies ist das Beispiel für ein Telefon und einen PC an einem Port (g1/0/1), Softwareversion 15.0.2SE2 auf 3750X:

```
bsns-3750-5#sh authentication sessions interface g1/0/1
           Interface:  GigabitEthernet1/0/1
         MAC Address:  0007.5032.6941
          IP Address:  192.168.10.12
           User-Name:  00-07-50-32-69-41
              Status:  Authz Success
              Domain:  VOICE
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  100
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  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
```

Das Telefon wird über MAB (MAC Authentication Bypass) authentifiziert, während der PC dot1x verwendet. Telefon und PC verwenden dieselbe Zugriffskontrollliste:

```
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
```

Bei Überprüfung auf Schnittstellenebene wurde die Quelle jedoch durch die IP-Adresse des Geräts ersetzt. IP-Geräterückverfolgung löst Änderungen aus, die jederzeit auftreten können (viel später als die Authentifizierungssitzung und der Download der ACL):

```
bsns-3750-5#show ip access-lists interface g1/0/1
    permit ip host 192.168.2.200 any (5 matches)
    permit ip host 192.168.10.12 any
```

Beide MAC-Adressen sollten als statisch gekennzeichnet werden:

```
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
```

Spezifischer ACL-Eintrag

Wann wird die Quelle "any" in der DACL durch die Host-IP-Adresse ersetzt? Nur wenn es mindestens zwei Sitzungen auf demselben Port gibt (zwei Supplicants).

Es ist nicht erforderlich, die Quelle "any" zu ersetzen, wenn es nur eine Sitzung gibt. Die Probleme können auftreten, wenn mehrere Sitzungen stattfinden, und für nicht alle IP-Geräte-Tracking kennt die IP-Adresse des Hosts. In diesem Szenario wird es für einige Einträge immer noch "any" sein.

Dieses Verhalten ist auf einigen Plattformen anders. Beispielsweise ist die ACL auf dem 2960X mit Version 15.0(2)EX immer spezifisch, auch wenn es nur eine Authentifizierungssitzung pro Port gibt. Für die 3560X- und 3750X-Version 15.0(2)SE müssen jedoch mindestens zwei Sitzungen vorhanden sein, um die jeweilige Zugriffskontrollliste zu definieren.

Steuerungsrichtung

Standardmäßig ist die Steuerelementrichtung vom Typ Both (Beide) festgelegt:

```
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
```

Das bedeutet, dass vor der Authentifizierung des Supplicants kein Datenverkehr vom oder zum Port gesendet werden kann. Im "In"-Modus hätte der Datenverkehr vom Port an die Komponente gesendet werden können, aber nicht von der Komponente an den Port (könnte für die WAKE-Funktion im LAN nützlich sein).

Dennoch wendet der Switch die ACL nur in Richtung "in" an. Es spielt keine Rolle, welcher Modus verwendet wird.

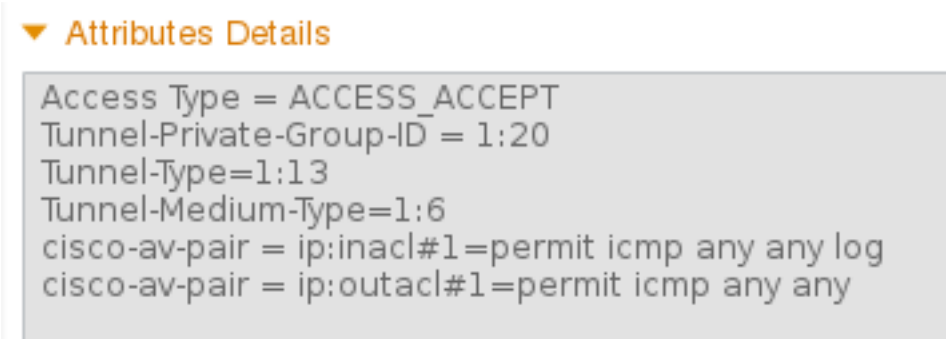
```
bsns-3750-5#sh ip access-lists interface g1/0/1 out
bsns-3750-5#sh ip access-lists interface g1/0/1 in
    permit ip host 192.168.2.200 any
    permit ip host 192.168.10.12 any
```

Das bedeutet im Prinzip, dass nach der Authentifizierung die ACL für den Datenverkehr zum Port (in Richtung) angewendet wird und der gesamte Datenverkehr vom Port (in Richtung Out) zugelassen wird.

IP-Geräteverfolgung mit 802.1x und benutzerspezifischer ACL für Version 15.x

Es ist auch möglich, eine benutzerspezifische ACL zu verwenden, die in cisco-av-pair "ip:inacl" und "ip:outacl" übergeben wird.

Diese Beispielkonfiguration ähnelt einer vorherigen Konfiguration, verwendet jedoch diesmal DACL und der PC verwendet eine benutzerspezifische ACL. Das ISE-Profil für den PC ist:



Auf dem Telefon ist noch die DACL angewendet:

```
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
```

Der PC am gleichen Port verwendet jedoch die benutzerspezifische ACL:

```
    Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
          IP Address:  192.168.2.200
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  20
        Per-User ACL:  permit icmp any any log
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000005674311400B
     Acct Session ID:  0x000006D1
              Handle:  0x9D000568
```

So überprüfen Sie die Zusammenführung auf dem Gig1/0/1-Port:

```
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
```

Der erste Eintrag wurde aus der benutzerspezifischen ACL (das Protokollschlüsselwort beachten) und der zweite aus der DACL übernommen. Beide werden durch die IP-Geräteverfolgung für die spezifische IP-Adresse neu geschrieben.

Die benutzerspezifische ACL kann mit dem Befehl **debug epm all** verifiziert werden:

```
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
```

Und auch über den Befehl **show ip access-lists**:

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

Was ist mit dem Attribut ip:outacl? Es wird in Version 15.x vollständig weggelassen. Das Attribut wurde empfangen, aber der Switch wendet dieses Attribut nicht an bzw. verarbeitet es nicht.

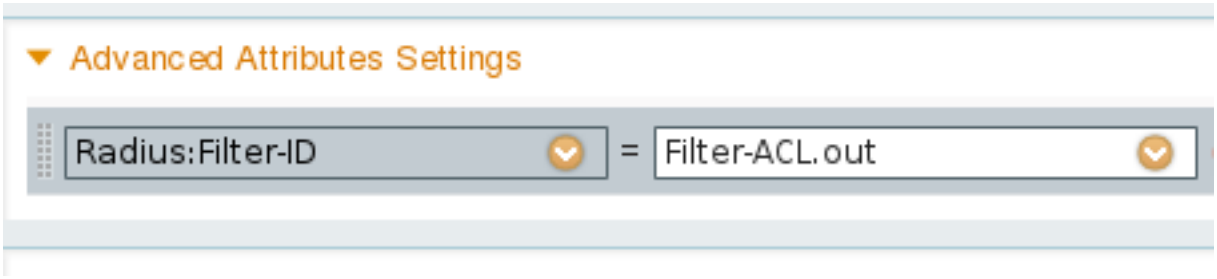
Unterschied im Vergleich zur DACL

Wie in der Cisco Bug-ID CSCut25702 angegeben, verhält sich die benutzerspezifische ACL anders als die DACL. DACL mit nur einem Eintrag ("permit ip any any") und eine an einen Port angeschlossene Komponente kann korrekt funktionieren, ohne dass die IP-Geräteverfolgung aktiviert ist. Das Argument "any" wird nicht ersetzt, und der gesamte Datenverkehr wird zugelassen. Für die benutzerspezifische ACL muss jedoch die IP-Geräterückverfolgung aktiviert sein. Wenn sie deaktiviert ist und nur über den Eintrag "permit ip any any" und einen Supplicant verfügt, wird der gesamte Datenverkehr blockiert.

IP-Geräteverfolgung mit 802.1x und Filter-ID-ACL für Version 15.x

Außerdem kann die IETF-Attribut filter-id [11] verwendet werden. Der AAA-Server gibt den Namen der ACL zurück, der lokal auf dem Switch definiert werden sollte. Das ISE-Profil könnte wie folgt aussehen:

Beachten Sie, dass Sie die Richtung (ein- oder ausgehend) angeben müssen. Dazu müssen Sie das Attribut manuell hinzufügen:



Anschließend wird Folgendes angezeigt:

```
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
```

Diese ACL wird auch für die authentifizierte Sitzung angezeigt:

```
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
```

Wenn die ACL an die Schnittstelle gebunden ist, gilt Folgendes:

```
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
```

Beachten Sie, dass diese ACL mit anderen Typen von ACLs auf derselben Schnittstelle zusammengeführt werden kann. Beispiel: Wenn auf demselben Switch-Port ein anderer Supplicant verwendet wird, der DACL von der ISE erhält: "permit ip any any" wird Folgendes angezeigt:

```
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
```

Beachten Sie, dass die IP-Geräteverfolgung die Quell-IP für jede Quelle (Supplicant) umschreibt.

Was ist mit der "Out"-Filterliste? Auch hier (als benutzerspezifische ACL) wird sie vom Switch nicht verwendet.

IP-Geräteverfolgung - Standardwerte und Best Practices

Bei Versionen vor 15.2(1)E muss IPDT erst mit diesem CLI-Befehl global aktiviert werden, bevor eine Funktion IPDT verwenden kann:

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

Für die Versionen 15.2(1)E und höher ist der Befehl **ip device tracking** nicht mehr erforderlich. IPDT wird nur aktiviert, wenn es von einer darauf basierenden Funktion aktiviert wird. Wenn keine Funktion IPDT aktiviert, wird IPDT deaktiviert. Der Befehl "no ip device tracking" hat keine Auswirkungen. Die spezifische Funktion verfügt über die Kontrolle zum Aktivieren/Deaktivieren von IPDT.

Wenn Sie IPDT aktivieren, müssen Sie sich an das Problem "Duplicate IP Address" (doppelte IP-Adresse) auf erinnern. Weitere Informationen finden Sie unter Fehlerbehebung bei Fehlermeldungen zu "Duplicate IP Address 0.0.0.0".

Es wird empfohlen, IPDT auf einem Trunk-Port zu deaktivieren:

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

Auf dem späteren Cisco IOS-Betriebssystem ist es ein anderer Befehl:

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

Es wird empfohlen, IPDT am Access-Port zu aktivieren und ARP-Tests zu verzögern, um das Problem "Duplizieren der IP-Adresse" zu vermeiden:

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

Interface ACL Rewrite für Version 15.x

Für die Schnittstelle ACL funktioniert sie vor der Authentifizierung:

```
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
```

Nach erfolgreicher Authentifizierung wird die Authentifizierung jedoch von der vom AAA-Server zurückgegebenen ACL umgeschrieben (überschrieben) (es spielt keine Rolle, ob es sich um DACL, ip:inacl oder filter-id handelt).

Diese ACL (Test1) kann den Datenverkehr blockieren (was normalerweise im offenen Modus zulässig ist), aber nach der Authentifizierung spielt diese Funktion keine Rolle mehr. Selbst wenn vom AAA-Server keine ACL zurückgegeben wird, wird die ACL der Schnittstelle überschrieben

und der vollständige Zugriff erfolgt. Dies ist ein wenig irreführend, da Ternary Content Addressable Memory (TCAM) anzeigt, dass die ACL noch auf der Schnittstellenebene gebunden ist. Hier ein Beispiel aus Version 15.2.2 für 3750X:

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

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

Diese Informationen gelten nur für die Schnittstellenebene, nicht für die Sitzungsebene. Weitere Informationen (präsentiert eine zusammengefasste ACL) können abgeleitet werden von:

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

Der erste Eintrag wird erstellt als "permit ip any any" DACL wird für eine erfolgreiche Authentifizierung zurückgegeben (und "any" wird durch einen Eintrag aus der Geräteliste ersetzt). Der zweite Eintrag ist das Ergebnis der Schnittstelle-ACL und wird für alle neuen Authentifizierungen (vor der Autorisierung) angewendet.

Leider sind (wieder plattformabhängig) beide ACLs miteinander verknüpft. Dies geschieht in Version 15.2.2 auf 3750X. Das bedeutet, dass für autorisierte Sitzungen beide angewendet werden. Zuerst die DACL und dann die Schnittstelle-ACL. Wenn Sie explizit "deny ip any any any" hinzufügen, berücksichtigt die DACL daher die Schnittstelle-ACL nicht. In der Regel ist in der DACL keine explizite Ablehnung enthalten, und danach wird die Schnittstelle-ACL angewendet.

Das Verhalten für Version 15.0.2 auf 3750X ist identisch, aber der Befehl **sh ip access-list interface** zeigt die Schnittstelle-ACL nicht mehr an (es wird jedoch weiterhin mit der Schnittstelle-ACL verkettet, es sei denn, in der DACL ist eine explizite Verweigerung vorhanden).

Standard-ACL für 802.1x

Es gibt zwei Arten von Standard-ACLs:

- auth-default-ACL-OPEN - wird für den offenen Modus verwendet
- auth-default-ACL - wird für den geschlossenen Zugriff verwendet

Wenn sich der Port im nicht autorisierten Zustand befindet, werden sowohl auth-default-ACL als auch auth-default-ACL-OPEN verwendet. Standardmäßig wird der geschlossene Zugriff verwendet. Das bedeutet, dass vor der Authentifizierung der gesamte Datenverkehr mit Ausnahme des Datenverkehrs verworfen wird, der von der auth-default-ACL zugelassen wird. Auf diese Weise wird DHCP-Datenverkehr vor erfolgreicher Autorisierung zugelassen. Die IP-Adresse ist zugewiesen, und die heruntergeladene DACL kann korrekt angewendet werden. Diese ACL

wird automatisch erstellt und ist nicht in der Konfiguration enthalten.

```
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
```

Sie wird dynamisch für die erste Authentifizierung (zwischen Authentifizierungs- und Autorisierungsphase) erstellt und nach dem Entfernen der letzten Sitzung entfernt.

Auth-Default-ACL erlaubt nur DHCP-Datenverkehr. Nachdem die Authentifizierung erfolgreich war und die neue DACL heruntergeladen wurde, wird sie auf diese Sitzung angewendet.Wenn der Modus zum Öffnen von "auth-default-ACL-OPEN" geändert wird, wird sie verwendet und funktioniert genau wie die Auth-Default-ACL:

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

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

Beide ACLs können individuell angepasst werden, werden jedoch in der Konfiguration nie angezeigt.

```
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#
```

Offener Modus

Im vorherigen Abschnitt wurde das Verhalten für ACLs beschrieben (einschließlich des Verhaltens, das standardmäßig für den offenen Modus verwendet wird). Das Verhalten für den offenen Modus ist:

- Es ermöglicht den gesamten Datenverkehr (gemäß der Standardeinstellung "auth-default-ACL-OPEN"), wenn sich die Sitzung in einem nicht autorisierten Zustand befindet.
- Die Sitzung befindet sich während der Authentifizierung/Autorisierung in einem nicht autorisierten Zustand (gut für das Encryption Appliance Model E (PXE) Boot-Szenarien) oder nach dem Ausfall dieses Prozesses (gut für Szenarien, die als "Low Impact-Modus" bezeichnet werden).

- Wenn die Sitzung in den autorisierten Status für mehrere Plattformen wechselt, werden die ACLs verkettet, und die erste DACL wird verwendet, und anschließend die Schnittstelle ACL.
- Bei mehreren Autoren oder mehreren Domänen können mehrere Sitzungen gleichzeitig in unterschiedlichen Zuständen stattfinden (dann gilt für jede Sitzung der unterschiedliche ACL-Typ).

Wenn die Schnittstelle-ACL obligatorisch ist

Für mehrere 6500/4500-Plattformen ist die Schnittstellen-ACL erforderlich, um die DACL korrekt anzuwenden.

Im folgenden Beispiel wird 4500 sup2 12.2.53SG6 ohne Schnittstellen-ACL verwendet:

```
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
```

Nach der Authentifizierung des Hosts wird die DACL heruntergeladen. Sie wird nicht angewendet, und die Autorisierung schlägt fehl.

```
*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
```

Nach dem Hinzufügen der Schnittstelle wird die ACL wie folgt ergänzt:

```
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
```

Authentifizierung und Autorisierung sind erfolgreich, und die DACL wird korrekt angewendet:

```
brisk#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE    Authz Success  0A3043450000008001A2CE4
```

Das Verhalten ist nicht von "Authentifizierung offen" abhängig. Um die DACL zu akzeptieren, benötigen Sie die ACL für die Schnittstelle sowohl im offenen als auch im geschlossenen Modus.

DACL auf 4500/6500

Auf dem 4500/6500 wird die DACL mit acl_snoop-DACLs angewendet. Hier ist ein Beispiel mit 4500 sup2 12.2.53SG6 (Telefon + PC) dargestellt. Es gibt eine separate ACL für das VLAN Sprache (10) und Daten (100):

```
brisk#show ip access-lists
Extended IP access list acl_snoop_Gi2/3_10
   10 permit ip host 192.168.2.200 any
```

```
   20 deny ip any any
Extended IP access list acl_snoop_Gi2/3_100
   10 permit ip host 192.168.10.12 any
   20 deny ip any any
```

ACLs sind spezifisch, da IPDT die richtigen Einträge enthält:

```
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
```

Authentifizierte Sitzungen zur Bestätigung der Adressen:

```
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 dieser Phase antworten sowohl der PC als auch das Telefon auf ICMP-Echo, aber die Schnittstelle ACL enthält nur Folgendes:

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

Warum? Weil die DACL nur für das Telefon gedrückt wurde (192.168.10.12). Für den PC wird die Schnittstelle ACL mit dem offenen Modus verwendet:

```
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)
```

Insgesamt wird "acl_snoop" sowohl für den PC als auch für das Telefon erstellt, aber die DACL wird nur für das Telefon zurückgegeben. Aus diesem Grund wird die ACL als an die Schnittstelle gebunden betrachtet.

MAC-Adressstatus für 802.1x

Wenn die 802.1x-Authentifizierung beginnt, wird die MAC-Adresse weiterhin als DYNAMIC angesehen, die Aktion für dieses Paket ist jedoch DROP:

```
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
```

Nach erfolgreicher Authentifizierung wird die MAC-Adresse statisch und die Portnummer wird angegeben:

```
bsns-3750-5#show authentication sessions

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

bsns-3750-5#show mac address-table interface g1/0/1
         Mac Address Table
-------------------------------------------

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

Dies gilt für alle MAB/dot1x-Sitzungen für beide Domänen (VOICE/DATA).

Fehlerbehebung

Lesen Sie den 802.1x-Konfigurationsleitfaden für Ihre spezielle Softwareversion und Plattform.

Wenn Sie ein TAC-Ticket öffnen, geben Sie die Ausgabe der folgenden Befehle an:

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

Es ist auch gut, eine SPAN-Port-Paketerfassung und folgende Debugging-Meldungen zu sammeln:

- Debug-Radius Ausführlich
- debuggen epm all
- Debug-Authentifizierung
- debug dot1x alle
- Debug-Authentifizierungsfunktion <yy> alle
- debuggen aaa authentication
- debuggen aaa autorisierung

Zugehörige Informationen

- Konfigurationsleitfaden für 802.1X-Authentifizierungsdienste, Cisco IOS XE Release 3SE (Catalyst 3850-Switches)
- Catalyst 3750-X und Catalyst 3560-X Switch Software Configuration Guide, Cisco IOS Release 15.2(1)E
- Catalyst 3750-X und 3560-X Software Configuration Guide, Release 15.0(1)SE
- Catalyst 3560 Software Configuration Guide, Release 12.2(52)SE
- Technischer Support und Dokumentation - Cisco Systems