802.1x DACL, ACL de Par-utilisateur, Filtre-ID, et comportement de cheminement de périphérique

Contenu

Introduction

Ce document décrit comment les travaux de fonctionnalité de suivi de périphérique IP, qui comporte ce que sont les déclencheurs d'ajouter et retirer un hôte. En outre, l'incidence du périphérique dépistant sur la liste de contrôle d'accès téléchargeable de 802.1x (DACL) est expliquée. Le comportement change entre les versions et les Plateformes.

La deuxième partie du document se concentre sur la liste de contrôle d'accès (ACL) renvoyée par le serveur d'Authentification, autorisation et comptabilité (AAA) et appliquée au 802.1x la session.

Une comparaison entre le DACL, l'ACL de Par-utilisateur et l'ACL de Filtre-ID est présentée. En outre, quelques mises en garde en vue de l'ACL réécrivent et l'ACL de par défaut sont discutés.

Théorie de cheminement de périphérique

Le cheminement de périphérique ajoute une entrée quand :

- il apprend la nouvelle entrée par l'intermédiaire de la surveillance DHCP.
- il apprend la nouvelle entrée par l'intermédiaire d'une demande de Protocole ARP (Address Resolution Protocol) (lit l'adresse MAC d'expéditeur et l'adresse IP d'expéditeur du paquet d'ARP). Que la fonctionnalité s'appelle parfois inspection ARP, mais lui n'est pas identiques que l'inspection dynamique d'ARP (DAI). Que la caractéristique est activée par défaut et ne peut pas être désactivée. Ce s'appelle également ARP pillant, mais met au point ne l'affichera pas après que le « debug arp pillant » soit activé. Piller d'ARP est activé par défaut et ne peut pas être désactivé ou contrôlé.

Le cheminement de périphérique retire une entrée quand il n'y a aucune réponse pour une demande d'ARP (envoyant la sonde pour chaque hôte dans le périphérique dépistant la table, par défaut toutes les 30 secondes).

Configuration de cheminement de périphérique

```
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
```

Périphérique dépistant des tests

```
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 de version 12.2.33, cheminement de périphérique IP mis à jour par

surveillance DHCP

La surveillance DHCP remplit table de corrélation :

```
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
```

Après que la liaison DHCP soit ajoutée à la base de données, elle déclenche la notification pour le cheminement de périphérique :

```
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
```

Des sondes d'ARP sont envoyées par défaut toutes les 30 secondes :

```
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
```

Après que l'entrée soit retirée du périphérique dépistant la table, l'entrée correspondante de liaison DHCP est toujours là :

```
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 y a la question quand vous avez une réponse d'ARP, mais le périphérique dépistant l'entrée est retiré de toute façon. Que la bogue semble être dans la version 12.2.33 et n'est pas apparue dans le logiciel de version 12.2.55 ou 15.x.

Également il y a quelques différences en manipulant avec le port L2 (port d'accès) et L3 mettent en communication (aucun switchport).

Sonde et piller d'ARP

Périphérique dépistant avec la configuration pillante d'ARP :

```
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
```

Périphérique IP dépistant pour la version 12.2.55 - Commande masquée

Pour la version 12.2 il pourrait y a un besoin d'employer une commande masquée afin de la lancer :

```
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
```

Périphérique IP dépistant pour la version 12.2.55 - Exemple statique IP

Dans cet exemple, le PC a été configuré avec une adresse IP statique. Les debugs prouvent qu'après que vous obteniez une réponse d'ARP (MSG=2), le périphérique dépistant l'entrée est mis à jour.

```
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
```

Tellement chaque demande d'ARP du PC met à jour le périphérique dépistant la table (l'adresse MAC d'expéditeur et l'adresse IP d'expéditeur du paquet d'ARP).

Périphérique IP dépistant pour la version 15.x

Il est important de se souvenir que certaines des caractéristiques telles que DACL pour le 802.1x ne sont pas prises en charge dans la version de LAN Lite (prenez garde - Cisco comportent le navigateur n'affiche pas toujours les informations correctes).

La commande masquée de la version 12.2 peut être exécutée, mais n'aura aucun effet. Dans la version de logiciel 15.x, le périphérique IP dépistant (IPDT) par défaut est seulement activé pour les interfaces qui ont le 802.1x activé :

```
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
```

Après la suppression de la configuration de 802.1x du port, IPDT sera également enlevée de ce port. L'état de port pourrait être « RÉDUIT », ainsi il est nécessaire d'avoir le « switchport mode access » et « l'automatique de port-control d'authenticaion » afin d'avoir le cheminement de périphérique IP lancé sur ce port. La limite maximum de périphérique d'interface est fixée à 10 :

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

Périphérique IP dépistant pour le ® de Cisco IOS XE

De nouveau, le comportement sur le Cisco IOS XE 3.3 a changé une fois comparé au Cisco IOS la version 15.x. La commande masquée de la version 12.2 est Désuet(e), mais maintenant cette erreur sera retournée :

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

Dans le Cisco IOS XE, le cheminement de périphérique est lancé pour toutes les interfaces (même celles qui n'ont pas le 802.1x configuré) :

```
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)
```

En outre, il n'y a aucune limite pour les entrées maximum par port (0 signifie handicapé).

Périphérique IP dépistant avec le 802.1x et le DACL pour la version 12.2.55

Si le 802.1x est configuré avec DACL, le périphérique dépistant l'entrée est utilisé afin de remplir adresse IP de périphérique. Cet exemple affiche fonctionner de cheminement de périphérique pour un IP statiquement configuré :

```
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
```

C'est une session de 802.1x établie avec le « ICMP d'autorisation n'importe quel n'importe quel » 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
```

Ceci affiche un ACL appliqué :

```
 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)
```

En outre, l'ACL sur l'interface fa0/1 est identiques :

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

Quoique le par défaut soit ACL de dot1x :

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

Il en pourrait être prévu pour que l'ACL utilise « » comme 192.168.0.244. Que des travaux comme ceci pour le proxy authentique, mais pour le src « » du 802.1x DACL n'en est pas changés à l'IP détecté du PC.

Pour le proxy authentique, un ACL d'original de l'ACS est caché et affiché avec la commande de show ip access-list et (Par-utilisateur avec l'IP de particularité) un ACL spécifique est appliqué sur l'interface avec la commande de l'interface fa0/1 de show ip access-list. Cependant, le proxy d'authentification n'utilise pas le cheminement IP de périphérique.

Ce qui si l'adresse IP n'est pas détectée correctement ? Après périphérique le cheminement est désactivé :

```
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
```

Tellement aucune adresse IP n'est reliée alors, mais le DACL est encore appliqué :

```
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
```

Dans ce scénario, le périphérique dépistant pour le 802.1x n'est pas exigé. La seule différence est cela qui connaît l'adresse IP du client franc peut être utilisée pour une Access-demande de RAYON. Après attribut 8 est reliés :

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

Il existera dans l'Access-demande et sur ACS il sera possible de créer des règles plus granulaires d'autorisation :

```
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
```

Maintenez dans l'esprit que TrustSec a besoin également de périphérique IP dépistant pour l'IP aux attaches SGT.

Périphérique IP dépistant avec le 802.1x et le DACL pour la version 15.x

Quelle est la différence entre la version 15.x et la version 12.2.55 dans DACL ? En logiciel Version15.x, cela fonctionne les mêmes que pour le proxy d'authentification. L'ACL générique peut être vu quand la commande de **show ip access-list** est entré (réponse cachée d'AAA), mais après la commande de l'**interface fa0/1 de show ip access-list**, le src « » est remplacé par l'adresse IP source de l'hôte (connu par l'intermédiaire du périphérique IP dépistant).

C'est l'exemple pour un téléphone et un PC sur un port (g1/0/1), la version de logiciel 15.0.2SE2 sur 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
```

Le téléphone est authentifié par l'intermédiaire de la dérivation d'authentification MAC (MAB), alors que le PC utilise le dot1x. Le téléphone et le PC utilisent le même ACL :

```
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
```

Cependant, une fois vérifiée au niveau d'interface la source a été remplacée par l'adresse IP du périphérique. Le périphérique IP dépistant les déclencheurs qui changent et lui peuvent se produire à tout moment (beaucoup plus tard que la session d'authentification et le téléchargement de l'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
```

Les deux adresses MAC devraient être marquées comme charge statique :

```
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
```

Rubrique de liste ACL spécifique

Quand la source « une partie » dans le DACL est-elle remplacée par l'adresse IP d'hôte ? Seulement quand il y a au moins deux sessions sur le même port (deux suppliants).

Il n'y a aucun besoin de remplacer la source « » quand il y a seulement une session. Les problèmes pourraient apparaître quand il y a des plusieurs sessions, et pour pas tous le cheminement de périphérique IP connaît l'adresse IP de l'hôte. Dans ce scénario il en sera toujours « » pour quelques entrées.

Ce comportement est différent sur quelques Plateformes. Par exemple, sur le 2960X avec la version 15.0(2)EX l'ACL sera toujours spécifique même lorsqu'il y a juste une session d'authentification par port. Cependant, pour la version 15.0(2)SE 3560X et 3750X, vous devez avoir au moins deux sessions pour faire cette particularité d'ACL.

Contrôle-direction

Par défaut, la contrôle-direction est type chacun des deux :

```
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
```

Cela signifie qu'avant que le suppliant soit authentifié, le trafic ne peut pas être envoyé à ou du port. Pour « en » mode, le trafic pourrait avoir été envoyé du port au suppliant, mais pas du suppliant au port (pourrait être utile pour le SILLAGE sur la caractéristique de RÉSEAU LOCAL).

Toujours, le commutateur applique l'ACL juste sur « dans » la direction. Il n'importe pas quel mode est utilisé.

```
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
```

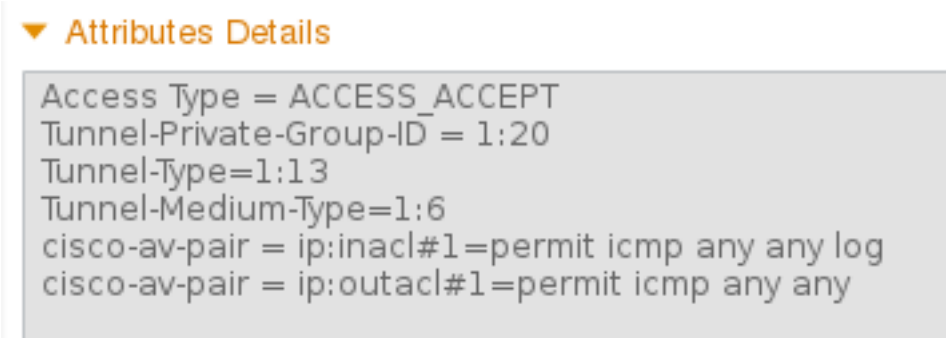
Cela signifie fondamentalement qu'après l'authentification l'ACL est appliquée pour le trafic au port (dans la direction) et on permet tout le trafic du port (direction).

Périphérique IP dépistant avec le 802.1x et l'ACL de Par-utilisateur pour la version 15.x

Il est également possible d'utiliser un ACL de Par-utilisateur qui est passé IP dans Cisco-poids du commerce-paires « : inacl » et « IP : outacl ».

Cet exemple de configuration est semblable à une configuration précédente, mais cette fois le

téléphone utilise DACL et le PC utilise l'ACL de Par-utilisateur. Le profil ISE pour le PC est :



Le téléphone a toujours le DACL appliqué :

```
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
```

Cependant, le PC sur le même port utilise l'ACL de Par-utilisateur :

```
    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
```

Afin de vérifier comment cela est fusionné sur le port gig1/0/1 :

```
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 première entrée a été prise du Par-utilisateur qu'ACL (notez le mot clé de journal) et la deuxième entrée est prise du DACL. Chacun d'eux sont réécrits par le périphérique IP dépistant pour l'adresse IP spécifique.

L'ACL de Par-utilisateur a pu être vérifié avec l'**epm de débogage toute la** commande :

```
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
```

Et également par l'intermédiaire de la commande de **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
```

Que diriez-vous de l'IP : attribut d'outacl ? Il est complètement omis dans la version 15.x. L'attribut a été reçu, mais le commutateur ne fait pas s'appliquer/processus qui attribuent.

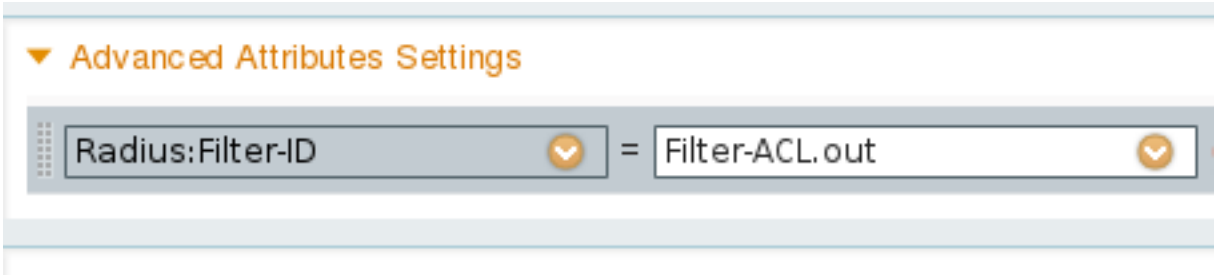
Différence une fois comparé au DACL

Comme observé dans l'ID de bogue Cisco CSCut25702, l'ACL de Par-utilisateur se comporte différemment que DACL. DACL avec juste une entrée (« IP tout quel d'autorisation ») et un suppliant connecté à un port peut fonctionner correctement sans cheminement de périphérique IP activé. Le « aucun » argument ne sera substitué et tout le trafic sera permis. Cependant, parce que l'ACL de Par-utilisateur il est obligatoire pour faire activer le cheminement de périphérique IP. S'il est désactivé et a juste le « IP d'autorisation n'importe quelle n'importe quelle » entrée et un suppliant, alors tout le trafic sera bloqué.

Périphérique IP dépistant avec le 802.1x et l'ACL de Filtre-ID pour la version 15.x

En outre, le filtre-id [11] d'attribut IETF peut être utilisé. Le serveur d'AAA renvoie le nom d'ACL, qui devrait être défini localement sur le commutateur. Le profil ISE a pu ressembler à ceci :

Notez que vous avez besoin specifiy de la direction (dans ou). Pour cela il est nécessaire d'ajouter l'attribut manuellement :



Puis les expositions de débogage :

```
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
```

Cet ACL sera également affiché pour la session authentifiée :

```
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
```

Et, comme ACL binded à l'interface :

```
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
```

Notez que cet ACL peut être fusionné avec d'autres types d'ACLs sur la même interface. Par exemple, ayant sur le même port de commutateur un autre suppliant qui obtient DACL d'ISE : « IP tout quel d'autorisation » que vous pourriez voir :

```
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
```

Notez que le cheminement de périphérique IP réécrit le source ip pour chaque source (suppliant).

Ce qui au sujet du « » filtrez la liste ? De nouveau (comme ACL de Par-utilisateur), il ne sera pas utilisé par le commutateur.

Cheminement de périphérique IP - Par défaut et pratiques recommandées

Pour des releases plus tôt que 15.2(1)E, avant que n'importe quelle caractéristique puisse utiliser IPDT il doit être activé globalement d'abord avec cette commande CLI :

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

Pour des versions 15.2(1)E et ultérieures, la commande de **cheminement de périphérique d'IP** n'est pas nécessaire plus. IPDT est activé seulement si une caractéristique qui se fonde sur lui l'active. Si aucune caractéristique n'active IPDT, IPDT est désactivé. La « aucune commande de cheminement de périphérique d'IP » n'a aucun effet. La caractéristique spécifique a le contrôle pour activer/IPDT.

Quand vous activez IPDT, vous devez se souvenir au sujet de la question de « adresse IP en double » en fonction. Voyez pour dépanner le pour en savoir plus de messages d'erreur « de 0.0.0.0 d'adresse IP en double ».

Il est recommandé pour désactiver IPDT sur un port de joncteur réseau :

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

Sur le Cisco IOS plus défunt, c'est une commande différente :

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

Il est recommandé pour permettre à IPDT sur les sondes de port d'accès et d'ARP de retard afin d'éviter la question de « adresse IP en double » :

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

Réécriture d'ACL d'interface pour la version 15.x

Pour l'ACL d'interface, cela fonctionne avant l'authentification :

```
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
```

Cependant, après l'authentification réussit il est réécrit (dépassement) par l'ACL retourné du serveur d'AAA (il n'importe pas si c'est DACL, IP : inacl, ou filterid).

Cet ACL (test1) peut bloquer le trafic (qui serait normalement permis sur le mode ouvert), mais après l'authentification n'importe plus. Même lorsqu'aucun ACL n'est retourné du serveur d'AAA, l'ACL d'interface est remplacé et l'accès complet est fourni. C'est un bit trompant puisque la mémoire associative ternaire (TCAM) indique que l'ACL binded encore au niveau d'interface. Voici un exemple de version 15.2.2 sur 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
```

Ces informations sont valides seulement pour le niveau d'interface, pas pour le niveau de session. Encore plus d'informations (présente un ACL composé) peuvent être déduites de :

```
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
```

La première entrée est créée en tant que « IP d'autorisation que n'importe quel n'importe quel » DACL est retourné pour l'authentification réussie (et « » est remplacé par une entrée du périphérique dépistant la table). La deuxième entrée est le résultat de l'ACL d'interface et est appliquée pour toutes les nouvelles authentifications (avant l'autorisation).

Malheureusement, (de nouveau personne à charge de plate-forme) les deux ACLs sont concaténés. Cela se produit sur la version 15.2.2 sur 3750X. Cela signifie cela pour la session autorisée, chacun d'eux sont appliqué. D'abord le DACL et deuxième l'ACL d'interface. C'est pourquoi quand vous ajoutez explicite « refusez l'IP tout », le DACL ne prendra pas en compte l'ACL d'interface. Habituellement il n'y a pas explicite refusent dans le DACL et alors l'ACL d'interface est appliqué ensuite que.

Le comportement pour la version 15.0.2 sur 3750X est identique, mais la commande d'interface SH d'ip access-list n'affiche plus l'ACL d'interface (mais lui sera encore concaténé avec l'ACL d'interface à moins qu'explicite refusent dans le DACL existe).

ACL par défaut utilisé pour le 802.1x

Il y a deux types d'ACLs par défaut :

- Authentique-par défaut-ACL-OUVERT - utilisé pour le mode ouvert
- Authentique-par défaut-ACL - utilisé pour l'accès fermé

L'authentique-par défaut-ACL et authentique-par défaut-ACL-OUVERTS sont utilisés quand le port est dans l'état non autorisé. Par défaut, l'accès fermé est utilisé. Cela signifie qu'avant que l'authentification tout le trafic soit abandonnée excepté celui a autorisé par l'authentique-par défaut-ACL. On permet ce trafic DHCP de manière avant l'autorisation réussie. L'adresse IP est allouée et le DACL téléchargé peut être correctement appliqué. Que l'ACL est créé automatiquement et ne peut pas être trouvé dans la configuration.

```
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
```

Il est créé dynamiquement pour la première authentification (entre l'authentification et la phase d'autorisation) et retiré après que la dernière session soit retirée.

L'Authentique-Par défaut-ACL permet seulement le trafic DHCP. Après l'authentification réussit et le nouveau DACL est téléchargé, il est appliqué à cette session. Quand le mode est changé pour ouvrir authentique-par défaut-ACL-OUVERT apparaît et cela est utilisé et fonctionne de la même manière comme Authentique-Par défaut-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
```

Les deux ACLs peut être personnalisé, mais ils ne seront jamais vus dans la configuration.

```
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#
```

Ouvrez le mode

La section précédente a décrit le comportement pour ACLs (qui inclut celui utilisé par défaut pour le mode ouvert). Le comportement pour le mode ouvert est :

- il tient compte de tout le trafic (selon le par défaut authentique-par défaut-ACL-OUVERT) quand la session est dans un état non autorisé.
- la session est dans un état non autorisé pendant l'authentification/autorisation (bonnes pour

des scénarios de démarrage du modèle E (PXE) d'appareils) de cryptage ou ensuite ce processus échoue (bon pour des scénarios appelés le « bas mode d'incidence »).
- quand la session se déplace à l'état autorisé pour des plates-formes multiples, ACLs sont concaténés et le premier DACL est utilisé, puis l'ACL d'interface.
- pour multi-auth ou le multi-domaine il pourrait y avoir des plusieurs sessions en même temps dans différents états (alors le type différent d'ACL s'appliquera pour chaque session).

Quand l'ACL d'interface est obligatoire

Pour le multiple 6500/4500 Plateformes, l'ACL d'interface est obligatoire afin d'appliquer le DACL correctement.

Voici un exemple avec 4500 sup2 12.2.53SG6, aucun ACL d'interface :

```
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
```

Alors après que l'hôte soit authentifié, le DACL est téléchargé. Il ne sera pas appliqué et l'autorisation échoue.

```
*Apr 25 04:38:05.239: RADIUS: Received from id 1645/19 10.48.66.74:1645,Access-Accept,
len 209
*Apr 25 04:38:05.239: RADIUS:  authenticator 35 8E 59 E4 D5 CF 8F 9A -
EE 1C FC 5A 9F 67 99 B2
*Apr 25 04:38:05.239: RADIUS:  User-Name           [1]   41
 "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1"
*Apr 25 04:38:05.239: RADIUS:  State               [24]  40
*Apr 25 04:38:05.239: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 61
 [ReauthSession:0a]
*Apr 25 04:38:05.239: RADIUS:   33 30 34 32 34 61 30 30 30 45 46 35 30 46 35 33
 [30424a000EF50F53]
*Apr 25 04:38:05.239: RADIUS:   35 41 36 36 39 33            [ 5A6693]
*Apr 25 04:38:05.239: RADIUS:  Class               [25]  54
*Apr 25 04:38:05.239: RADIUS:   43 41 43 53 3A 30 61 33 30 34 32 34 61 30 30 30
 [CACS:0a30424a000]
*Apr 25 04:38:05.239: RADIUS:   45 46 35 30 46 35 33 35 41 36 36 39 33 3A 69 73
 [EF50F535A6693:is]
*Apr 25 04:38:05.239: RADIUS:   65 32 2F 31 38 30 32 36 39 35 33 38 2F 31 32 38
 [e2/180269538/128]
*Apr 25 04:38:05.239: RADIUS:   36 35 35 33              [ 6553]
*Apr 25 04:38:05.239: RADIUS:  Message-Authenticato[80]  18
*Apr 25 04:38:05.239: RADIUS:   AF 47 E2 20 65 2F 59 39 72 9A 61 5C C5 8B ED F5
        [ G e/Y9ra\]
*Apr 25 04:38:05.239: RADIUS:  Vendor, Cisco       [26]  36
*Apr 25 04:38:05.239: RADIUS:   Cisco AVpair       [1]   30
 "ip:inacl#1=permit ip any any"
*Apr 25 04:38:05.239: RADIUS(00000000): Received from id 1645/19
*Apr 25 04:38:05.247: EPM_SESS_ERR:Failed to apply ACL to interface
*Apr 25 04:38:05.247: EPM_API:In function epm_send_message_to_client
*Apr 25 04:38:05.247: EPM_SESS_EVENT:Sending response message to process
```

```
AUTH POLICY Framework
*Apr 25 04:38:05.247: EPM_SESS_EVENT:Returning feature config
*Apr 25 04:38:05.247: EPM_API:In function epm_acl_feature_free
*Apr 25 04:38:05.247: EPM_API:In function epm_policy_aaa_response
*Apr 25 04:38:05.247: EPM_FSM_EVENT:Event epm_ip_wait_event state changed from
policy-apply to ip-wait
*Apr 25 04:38:05.247: EPM_API:In function epm_session_action_ip_wait
*Apr 25 04:38:05.247: EPM_API:In function epm_send_ipwait_message_to_client
*Apr 25 04:38:05.247: EPM_SESS_ERR:NULL feature list for client ctx 1B2694B0
for type DOT1X
*Apr 25 04:38:05.247: %AUTHMGR-5-FAIL: Authorization failed for client
(0007.5032.6941) on Interface Gi2/3
AuditSessionID 0A304345000000060012C050

brisk#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE    Authz Failed   0A304345000000060012C050
```

Après interface l'ACL est ajouté :

```
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'authentification et l'autorisation réussiront et le DACL sera appliqué correctement :

```
brisk#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE    Authz Success  0A304345000000008001A2CE4
```

Le comportement ne dépend pas de la « authentication open ». Afin de recevoir le DACL, vous avez besoin de l'ACL d'interface pour des les deux ouvrez/avez clôturé le mode.

DACL sur 4500/6500

Sur le 4500/6500, le DACL est appliqué avec l'acl_snoop DACLs. Un exemple avec 4500 sup2 12.2.53SG6 (téléphone + PC) est affiché ici. Il y a un ACL distinct pour la Voix (10) et les données (100) VLAN :

```
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 sont spécifique parce qu'IPDT a les entrées correctes :

```
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
```

Les sessions authentifiées confirment les adresses :

```
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
```

Àce stade le PC et le téléphone répond à l'écho d'ICMP, mais aux présents d'ACL d'interface seulement :

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

Pourquoi ? Puisque le DACL a été poussé seulement le téléphone (192.168.10.12). Pour le PC, l'ACL d'interface avec le mode ouvert est utilisé :

```
interface GigabitEthernet2/3
 ip access-group all in
 authentication open

brisk#show ip access-lists all
Extended IP access list all
   10 permit ip any any (73 matches)
```

En résumé, l'acl_snoop sera créé pour le PC et le téléphone, mais le DACL est retourné juste pour le téléphone. C'est pourquoi cet ACL est vu comme binded à l'interface.

État d'adresse MAC pour le 802.1x

Quand des débuts d'authentification de 802.1x, l'adresse MAC est encore vus en tant que DYNAMIQUE mais l'action pour ce paquet est BAISSE :

```
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
```

Après que réussi l'authentification l'adresse MAC devient charge statique et le numéro de port est fourni :

```
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
```

C'est vrai pour toute la session mab/dot1x pour les deux domaines (VOICE/DATA).

Dépannez

Souvenez-vous pour lire le guide de configuration de 802.1x pour votre version de logiciel et plate-forme spécifiques.

Si vous ouvrez une valise TAC, fournissez la sortie de ces commandes :

- affichez le tech
- détail de <xx> d'interface de session de show authentication
- <xx> de show mac address-table interface

Il est également bon de collecter une capture de paquet de port SPAN et ceux-ci met au point :

- debug radius bavard
- mettez au point l'epm tout
- debug authentication tout
- debug dot1x tout
- <yy> tout de caractéristique de debug authentication
- **debug aaa authentication**
- **debug aaa authorization**

Informations connexes

- guide de configuration de services d'authentification de 802.1X, release 3SE (Commutateurs de Cisco IOS XE de Catalyst 3850)
- Le Catalyst 3750-X et le Catalyst 3560-X commutent le guide de configuration du logiciel, Cisco IOS version 15.2(1)E
- Catalyst 3750-X et guide de configuration du logiciel 3560-X, release 15.0(1)SE
- Guide de configuration du logiciel de Catalyst 3560, release 12.2(52)SE
- Support et documentation techniques - Cisco Systems