DACL 802.1x, ACL для каждого пользователя, Filter-Id и поведение отслеживания устройства

Содержание

Введение

Этот документ описывает, как характеристика отслеживания IP - устройства работает, который включает то, что триггеры должны добавить и удалить хост. Кроме того, влияние отслеживания устройства на Загружаемом списке контроля доступа (DACL) 802.1x объяснено. Поведение изменяется между версиями и платформами.

Вторая часть документа фокусируется на Списке контроля доступа (ACL), возвращенном аутентификацией, авторизацией и учетом (AAA) и примененном к сеанс 802.1x. Сравнение между DACL, ACL Для каждого пользователя и ACL Filter-Id представлено. Кроме того, обсуждены некоторые предупреждения в отношении перезаписи ACL и списка доступа по умолчанию.

Теория отслеживания устройства

Отслеживание устройства добавляет запись когда:

- это изучает новую запись через отслеживание DHCP.
- это учится, новая запись через Запрос протокола переопределения адресов (ARP) (читает MAC-адрес отправителя и IP-адрес отправителя от пакета ARP). Ту функциональность иногда называют проверкой ARP, но это не то же как Динамическая проверка ARP (DAI). Та опция активирована по умолчанию и не может быть отключена. Это также называют отслеживанием ARP, но отладки не покажут его после того, как "будет включено отслеживание debug arp". Отслеживание ARP включено по умолчанию и не может отключаться или управляться.

Когда нет никакого ответа для запроса ARP (передача зонда для каждого хоста в таблице отслеживания устройства, по умолчанию каждые 30 секунд), отслеживание устройства удаляет запись.

Конфигурация отслеживания устройства

```
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
```

Тесты отслеживания устройства

```
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
```

Отладки от версии 12.2.33, отслеживание IP - устройства, обновленное отслеживанием DHCP

Отслеживание DHCP заполняет таблицу привязки:

```
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
```

После того, как привязка DHCP добавлена к базе данных, она инициирует уведомление для отслеживания устройства:

```
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
```

Зонды ARP передаются по умолчанию каждые 30 секунд:

```
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

После того, как запись удалена из таблицы отслеживания устройства, соответствующий DHCP, который обязательная запись все еще там:

```
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
```

Существует проблема, когда у вас есть ответ ARP, но запись отслеживания устройства удалена так или иначе. Тот дефект, кажется, находится в Версии 12.2.33 и не появился в программном обеспечении Версии 12.2.55 или 15.x.

Также существуют некоторые различия при обработке через порт L2 (порт доступа) и порт L3 (никакой switchport).

Зонд и отслеживание ARP

Отслеживание устройства с ARP, snooping функция:

```
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
```

Отслеживание IP - устройства для версии 12.2.55 - команда hidden

Для Версии 12.2 могла бы быть потребность использовать команду hidden для активации его:

```
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
```

Отслеживание IP - устройства для версии 12.2.55 - статический ip пример

В данном примере ПК был настроен со статическим IP - адресом. Отладки показывают, что после того, как вы получаете ответ ARP (MSG=2), обновлена запись отслеживания устройства.

```
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
```

Таким образом, каждый запрос ARP от ПК обновляет таблицу отслеживания устройства (MAC-адрес отправителя и IP-адрес отправителя от пакета ARP).

Отслеживание IP - устройства для версии 15. x

Важно помнить, что некоторые функции, такие как DACL для 802.1x не поддерживаются в LAN Облегченная версия (остерегайтесь - Cisco Feature Navigator не всегда показывает корректную информацию).

Команда hidden от Версии 12.2 может быть выполнена, но не будет иметь никакого эффекта. В Версии программного обеспечения 15.x IP - устройство, отслеживающий (IPDT) по умолчанию, только включен для интерфейсов, которым включили 802.1x:

```
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
```

После удаления конфигурации 802.1x от порта IPDT будет также удален из того порта. Состояние порта могло бы не работать, таким образом, необходимо иметь "switchport mode access" и "authenticaion управление портами, автоматическое" для активирования IP - устройства, отслеживающего на том порту. Максимальный предел интерфейсного устройства установлен к 10:

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

Отслеживание IP - устройства для Cisco IOS-XE®

Снова, поведение на Cisco IOS XE 3.3 изменилось когда по сравнению с версией Cisco IOS 15. x. Команда hidden от Версии 12.2 является устаревшей, но теперь будет возвращена эта ошибка:

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

В Cisco IOS XE отслеживание устройства активировано для всех интерфейсов (даже те, которым не настроили 802.1x):

```
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)
```

Кроме того, нет никаких пределов для максимальных записей на порт (0 отключенных средств).

Отслеживание IP - устройства с 802.1x и DACL для версии 12.2.55

Если 802.1x настроен с DACL, запись отслеживания устройства используется для заполнения IP-адреса устройства. Данный пример показывает отслеживание устройства, работающее для статически настроенного IP:

```
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
```

Это - сеанс 802.1x, созданный с "icmp разрешения любой любой" 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
```

Это показывает прикладной 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)
```

Кроме того, ACL на интерфейсе fa0/1 является тем же:

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

Даже при том, что по умолчанию является ACL dot1x:

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

Это, как могли бы ожидать, для ACL будет использовать "любого" в качестве 192.168.0.244. Это работает как это для подлинного прокси, но для src DACL 802.1x "любой" не изменен на обнаруженного IP ПК.

Для подлинного прокси один исходный ACL от ACS кэшируется и показывается с командой show ip access-list и определенным (Для каждого пользователя с определенным IP), ACL применен на интерфейс с интерфейсом show ip access-list fa0/1 команда. Однако auth-proxy не использует отслеживание IP устройства.

Что, если IP-адрес не обнаружен правильно? После того, как отслеживание устройства отключено:

```
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
```

Таким образом, no ip address подключен тогда, но все еще применен DACL:

```
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
```

В этом сценарии не требуется отслеживание устройства для 802.1x. Единственная разница - то, что знание IP-адреса искреннего клиента может использоваться для access-request RADIUS. После того, как атрибут 8 подключен:

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

Это будет существовать в Access-Request, и на ACS будет возможно создать большие гранулированные правила авторизации:

```
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
```

Следует иметь в виду, что TrustSec также нужно отслеживание IP - устройства для IP к связываниям SGT.

Отслеживание IP - устройства с 802.1x и DACL для версии 15. x

Каково различие между Версией 15.x и Версией 12.2.55 в DACL? В программном обеспечении Version15.x это работает то же что касается auth-proxy. ACL общего назначения может быть замечен, когда **команда show ip access-list** введена (кэшируемый ответ от AAA), но после **интерфейса show ip access-list fa0/1** команда, src "любой" заменен IP - адресом источника хоста (известный через отслеживание IP - устройства).

Это - пример для телефона и ПК на одном порту (g1/0/1), версии программного обеспечения 15.0.2SE2 на 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: C0A800010000001012B680D23
     Acct Session ID: 0x0000017B
              Handle: 0x99000102

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

---------------------------------------
           Interface: GigabitEthernet1/0/1
         MAC Address: 0050.5699.4ea1
          IP Address: 192.168.2.200
           User-Name: cisco
              Status: Authz Success
              Domain: DATA
     Security Policy: Should Secure
     Security Status: Unsecure
      Oper host mode: multi-auth
    Oper control dir: both
       Authorized By: Authentication Server
         Vlan Policy: 20
             ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
     Session timeout: N/A
        Idle timeout: N/A
   Common Session ID: C0A80001000001BD336EC4D6
     Acct Session ID: 0x000002F9
              Handle: 0xF80001BE


Runnable methods list:
      Method  State
      dot1x   Authc Success
      mab     Not run
```

В то время как ПК использует dot1x, телефон аутентифицируется через Обход проверки подлинности MAC (MAB). И телефон и ПК используют тот же 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
```

Однако, когда проверено на уровне интерфейса источник был заменен IP-адресом устройства. Триггеры отслеживания IP - устройства, которые изменяются и это может произойти в любое время (намного позже, чем сеанс аутентификации и загрузка 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
```

Оба MAC-адреса должны быть отмечены как статичные:

```
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
```

Определенная запись ACL

Когда источник - "кто-либо" в DACL, замененном адресом IP - адреса хоста? Только, когда существует по крайней мере два сеанса на том же порте (два соискателя).

Когда существует только один сеанс, нет никакой потребности заменить источник "любой". Проблемы могли бы появиться, когда существуют несколька сеансов, и для не все они, какое отслеживание IP - устройства знает IP-адрес хоста. В том сценарии это все еще будет "любой" для некоторых записей.

То поведение является другим на некоторых платформах. Например, на 2960X с Версией 15.0 (2) EX ACL всегда будет определенным, даже когда существует всего один сеанс аутентификации на порт. Однако для 3560X и 3750X SE Версии 15.0 (2), у вас должно быть по крайней мере два сеанса для создания того ACL определенным.

Направление контроля

По умолчанию направление контроля является типом оба:

```
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
```

Это означает, что, прежде чем соискатель аутентифицируется, трафик не может быть передан или от порта. Поскольку "в" режиме, трафик, возможно, был передан от порта до соискателя, но не от соискателя к порту (могло быть полезно для WAKE на функции LAN).

Однако, коммутатор применяет ACL только на "в" направлении. Это не имеет значения, какой режим используется.

```
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
```

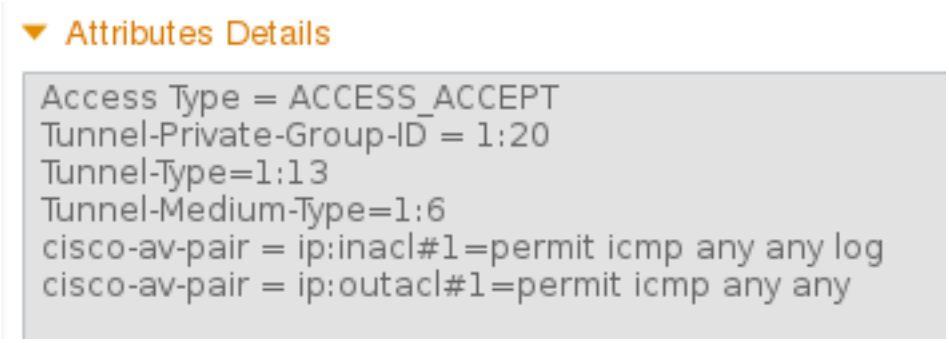
Это в основном означает, что после аутентификации ACL применен для трафика к порту (в направлении), и весь трафик разрешен от порта (направление).

Отслеживание IP - устройства с 802.1x и ACL для каждого пользователя для версии 15. x

Также возможно использовать ACL Для каждого пользователя, который передают в Cisco-

av-pair "ip:inacl" и "ip:outacl".

Конфигурация данного примера подобна предыдущей конфигурации, но на этот раз телефонный DACL использования и ПК используют ACL Для каждого пользователя. Профиль ISE для ПК:



Телефону все еще применили DACL:

```
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
```

Однако ПК на том же порте использует ACL Для каждого пользователя:

```
   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: C0A8000100000005674311400B
     Acct Session ID: 0x000006D1
              Handle: 0x9D000568
```

Чтобы проверить, как это объединено на gig1/0/1 порту:

```
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
```

Первая запись была взята от ACL Для каждого пользователя (заметьте регистрационное ключевое слово), и вторая запись взята от DACL. Они оба переписаны отслеживанием IP - устройства для определенного IP-адреса.

ACL для каждого пользователя мог быть проверен с **отладкой epm вся** команда:

```
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
```

И также через **команду 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
```

Что относительно атрибута ip:outacl? Это полностью опущено в Версии 15. x. Атрибут был получен, но коммутатор не применяется/обрабатывает тот атрибут.

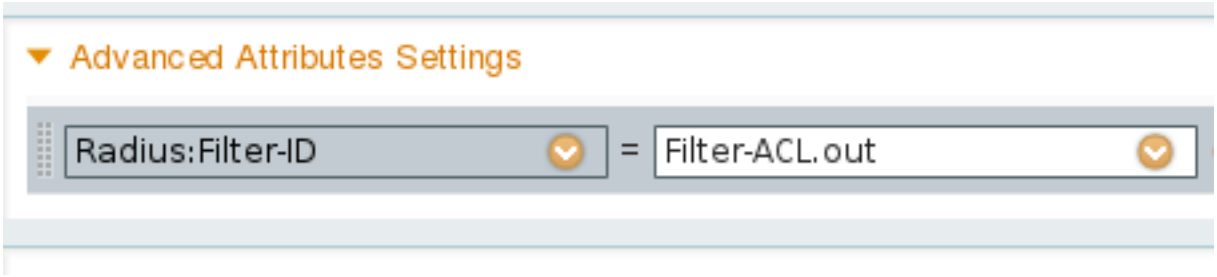
Различие, когда По сравнению с DACL

Как обращено внимание в идентификаторе ошибки Cisco CSCut25702, ACL Для каждого пользователя ведет себя по-другому, чем DACL. DACL со всего одной записью ("permit ip any any") и один соискатель, связанный с портом, может работать правильно без включенного отслеживания IP - устройства. "Любым" аргументом не заменят, и весь трафик будет разрешен. Однако для ACL Для каждого пользователя это является обязательным для включения IP - устройства, отслеживающего. Если это будет отключено и будет иметь просто запись "permit ip any any" и одного соискателя, то весь трафик будет заблокирован.

Отслеживание IP - устройства с 802.1x и ACL Filter-Id для версии 15. x

Кроме того, идентификатор фильтра атрибута IETF [11] может использоваться. AAA-сервер возвращает название ACL, которое должно быть определено локально на коммутаторе. Профиль ISE мог быть похожим на это:

Обратите внимание на то, что вам нужно к specifiy направление (в или). Для этого необходимо добавить атрибут вручную:



Затем отладка показывает:

```
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
```

Тот ACL также покажут для аутентифицируемого сеанса:

```
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
```

И, поскольку ACL связан к интерфейсу:

```
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
```

Обратите внимание на то, что этот ACL может быть объединен с другими типами ACL на том же интерфейсе. Например, имея на том же порте коммутатора другого соискателя, который получает DACL от ISE: "permit ip any any" вы видели:

```
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
```

Обратите внимание на то, что отслеживание IP - устройства переписывает source IP для каждого источника (соискатель).

Что относительно списка фильтров? Снова (как ACL Для каждого пользователя), это не будет использоваться коммутатором.

Отслеживание IP - устройства - настройки по умолчанию и оптимальные методы

Для версий ранее, чем 15.2 (1) E, прежде чем любая функция может использовать IPDT, который это должно быть включено глобально сначала с этой командой CLI:

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

Для версий 15.2 (1) E и позже, **IP** команда **отслеживания устройства** больше не необходима. IPDT включен, только если функция, которая полагается на него, включает его. Если никакая функция не включает IPDT, IPDT отключен. "Никакая IP команда" отслеживания устройства не имеет никакого эффекта. Определенная функция имеет контроль к позволить/запретить IPDT.

При включении IPDT необходимо помнить о проблеме "Дублирования IP-адреса" на. Посмотрите Устранение неполадок "Дублирование IP-адреса 0.0.0.0" Сообщения об ошибках для получения дополнительной информации.

Рекомендуется отключить IPDT на магистральном порте:

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

На более поздней Cisco IOS это - другая команда:

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

Рекомендуется включить IPDT на порте доступа и зондах ARP задержки во избежание проблемы "Дублирования IP-адреса":

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

Интерфейсная перезапись ACL для версии 15. x

Для интерфейсного ACL это работает перед аутентификацией:

```
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
```

Однако после того, как аутентификация успешно выполняется, она переписана (отвергают) ACL, возвращенным из AAA-сервера (не имеет значения, если это - DACL, ip:inacl, или фильтруемый).

Тот ACL (test1) может заблокировать трафик (который обычно разрешался бы на открытом режиме), но после того, как аутентификация больше не имеет значения. Даже когда никакой ACL не возвращен из AAA-сервера, интерфейсный ACL перезаписан, и полный доступ предоставлен. Это является немного вводящим в заблуждение, так как Ternary Content Addressable Memory (TCAM) указывает, что ACL все еще связан на уровне интерфейса. Вот пример от Версии 15.2.2 на 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
```

Та информация допустима только для уровня интерфейса, не для сеансового уровня. Некоторые дополнительные сведения (представляет составленный ACL) могут быть выведены из:

```
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
```

Первая запись создана, когда DACL "permit ip any any" возвращен для успешной аутентификации (и "любой" заменен записью от таблицы отслеживания устройства). Вторая запись является результатом интерфейсного ACL и применена для всех новых аутентификаций (перед авторизацией).

К сожалению, (снова зависимость от платформы) оба ACL связаны. Это происходит на Версии 15.2.2 на 3750X. Это означает, что для санкционированного сеанса, они оба применены. Сначала DACL и второй интерфейсный ACL. Именно поэтому, когда вы добавляете явный, "deny ip any any", DACL не учтет интерфейсный ACL. Обычно там является не явным, запрещают в DACL, и затем интерфейсный ACL применен после этого.

Поведение для Версии 15.0.2 на 3750X является тем же, но **sh** команда **интерфейса ip access-list** больше не показывает интерфейсный ACL (но это будет все еще связано с

интерфейсным ACL, пока не явный запрещают в DACL, существует).

Список доступа по умолчанию, используемый для 802.1x

Существует два типа списков доступа по умолчанию:

- auth-default-ACL-OPEN - используемый для открытого режима
- подлинный список доступа по умолчанию - используемый для закрытого доступа

Когда порт находится в неавторизованном состоянии, и подлинный список доступа по умолчанию и auth-default-ACL-OPEN используются. По умолчанию закрытый доступ используется. Это означает, что перед аутентификацией весь трафик отброшен кроме того, разрешенного подлинным списком доступа по умолчанию. Таким образом, трафик DHCP разрешен перед успешной авторизацией. IP-адрес выделен, и загруженный DACL может быть правильно применен. Тот ACL создан автоматически и не может быть найден в конфигурации.

```
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
```

Это создано динамично для первой аутентификации (между фазой проверки подлинности и авторизация) и удалено после того, как последний сеанс удален.

Подлинный список доступа по умолчанию разрешает только трафик DHCP. После того, как аутентификация успешно выполняется, и новый DACL загружен, это применено к тому сеансу. Когда режим изменен для открытия, auth-default-ACL-OPEN появляется, и это используется и работает точно таким же образом как Подлинный список доступа по умолчанию:

```
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
```

Оба ACL могут быть настроены, но они никогда не будут замечаться в конфигурации.

```
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#
```

Открытый режим

Предыдущий раздел описал поведение для ACL (который включает тот, используемый по умолчанию для открытого режима). Поведение для открытого режима:

- это обеспечивает весь трафик (согласно по умолчанию auth-default-ACL-OPEN), когда сеанс находится в неавторизованном состоянии.
- сеанс находится в неавторизованном состоянии во время аутентификации/авторизации (хороший для Модели E Устройства шифрования (PXE), загрузочные сценарии) или после того процесса сбои (хороший для сценариев, вызванных "низко, влияют на режим").
- когда сеанс переходит в санкционированное состояние для нескольк платформ, ACL связаны, и первый DACL используется, тогда интерфейсный ACL.
- для мультиаутентификации или мультидоменный могли бы быть несколька сеансов в то же время в других состояниях (тогда, другой тип ACL будет просить каждый сеанс).

Когда Интерфейсный ACL является Обязательным

Для множественных 6500/4500 платформ интерфейсный ACL является обязательным для применения DACL правильно.

Вот пример с 4500 sup2 12.2.53SG6, никаким интерфейсным ACL:

```
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
```

Затем после того, как хост аутентифицируется, DACL загружен. Это не будет применено и сбои авторизации.

```
*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
```

После того, как интерфейсный ACL добавлен:

```
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
```

Проверка подлинности и авторизация успешно выполнится, и DACL будет применен правильно:

```
brisk#show authentication sessions

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

Поведение не зависит от "authentication open". Для принятия DACL вам нужен интерфейсный ACL для обоих, открываются/закрывают режим.

DACL на 4500/6500

На 4500/6500 DACL применен с acl_snoop DACLs. Пример с 4500 sup2 12.2.53SG6 (телефон + ПК) показывают здесь. Существует отдельный ACL для голоса (10) и данные (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
```

ACL являются определенными, потому что IPDT имеет корректные записи:

```
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
```

Аутентифицируемые сеансы подтверждают адреса:

```
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
```

На данном этапе и ПК и телефон отвечают на эхо - запрос ICMP, но интерфейсный ACL представляет только:

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

В чем причина? Поскольку DACL был выдвинут только для телефона (192.168.10.12). Для ПК используется интерфейсный ACL с открытым режимом:

```
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)
```

Таким образом, acl_snoop будет создан и для ПК и для телефона, но DACL возвращен только для телефона. Именно поэтому тот ACL замечен как связанный к интерфейсу.

Статус MAC-адреса для 802.1x

Когда аутентификация 802.1x запускается, MAC-адрес все еще замечен как ДИНАМИЧНЫЙ, но действие для того пакета является ОТБРАСЫВАНИЕМ:

```
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
```

После успешной аутентификации MAC-адрес становится статичным, и номер порта предоставлен:

```
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
```

Это истинно для всего сеанса mab/dot1x для обоих доменов (VOICE/ДАННЫЕ).

Устранение неполадок

Не забудьте читать руководство по конфигурации 802.1x для своей определенной версии программного обеспечения и платформы.

При открытии кэйса TAC (Центра технической поддержки) предоставьте выходные данные от этих команд:

- show tech
- интерфейс сеанса show authentication <xx> подробность
- show mac address-table interface <xx>

Также хорошо собрать захват пакета Порта SPAN и эти отладки:

- многословный debug radius
- отладьте epm все
- debug authentication все
- debug dot1x все
- функция debug authentication <yy> все
- debug aaa authentication
- debug aaa authorization

Дополнительные сведения

- Руководство по конфигурации сервисов проверки подлинности 802.1X, выпуск 3SE Cisco IOS XE (коммутаторы Catalyst 3850)
- 3750-X Catalyst и Catalyst 3560-X руководство по конфигурации программного обеспечения коммутатора, Cisco IOS Release 15.2 (1) E
- Catalyst 3750-X и 3560-X руководство по конфигурации программного обеспечения, SE выпуска 15.0 (1)
- Руководство по конфигурации программного обеспечения Catalyst 3560, релиз 12.2 (52) SE
- Cisco Systems – техническая поддержка и документация