Adatkapcsolati protokollok – II.
Konzisztencia és hozzáférés kontroll

második rész

2016. december 19.

Smart Vision Solutions

taking you one step ahead

Hol tartottunk?

- **Hozzáférés kontroll**, ezen belül
  - Eszköz hozzárférés
  - AAA

    Ezt megbeszéltük, itt tartottunk.

  - Hálózat hozzáférés, ezen belül:
  - Nem végponti hozzáférés-kontroll
    - DHCP snooping
    - Dynamic ARP Inspection (DAI)

  - Végponti hozzáférés-kontroll
    - IP Source guard
    - Port security
    - VMPS
    - 802.1x

Problémák, amikre készülni kell

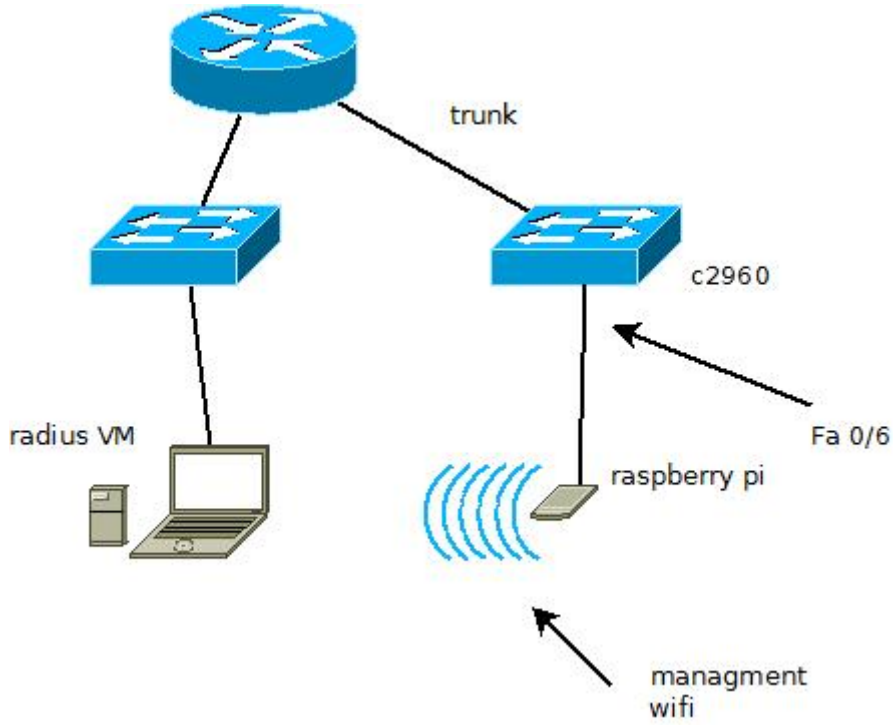
- Erőforrásokkal kapcsolatos problémák
  - Fizikai védelem
  - Végtelen ciklusok, hurkok
  - Túl nagy forgalom
  - Túl gyakori forgalom
- Tiltott eszközök a hálózaton
  - Idegen DHCP szerver
  - Idegen wireless AP
- Hozzáféréssel kapcsolatos problémák
  - Időbeli korlátozás megszegése
  - IP cím lopás
  - Nem engedélyezett VLAN-hoz hozzáférés
  - MAC address hamisítás
  - BYOD

Honnan indulunk ma?

- A múltkori állapotból lépünk tovább
- Központosított autentikáció, netadmin / sysadmin felhasználókkal
- A két felhasználó eltérő jogokkal rendelkezik
- A radius szerver most nem MS IAS, hanem freeradius, mert ma erre lesz szükség

- Van hostnevünk, beállítottuk a pontos időt

- Van egy raspberry pi, két interfésszel
- Egy vezetékes hagyományos 10/100 ethernet, ez lesz a kliens, aki hozzáfér a hálózathoz
- Van benne egy USB wireless adapter, második interfész
- Ezen át férünk hozzá távolról, hogy lássuk, mi történik a kliensen, ha nincs hálózata



A mai alkalommal a következőket tanuljuk meg:

- ✔ Hogyan védekezz az **idegen hálózati eszközök** ellen
- ✔ Mit tegyél, ha unod a **vlan – port konfigurálás**okat de szükségesek
- ✔ Hogyan akadályozd meg a **MAC cím átírást** / klónozást (vagy legalább azt, hogy értelme legyen)
- ✔ Miként nem okoz problémát, ha **idegen DHCP** szervert raknak a hálózatodra
- ✔ Miképp védekezz az ellen, hogy az emberek **statikus IP**-t állítsanak be maguknak

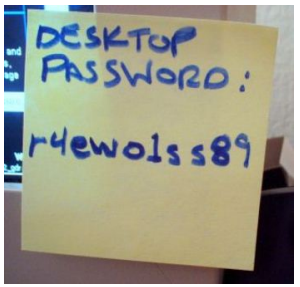
Védelmi rétegek

A példa kedvéért egy weboldalt képzelj el, amin át bizalmas információkat lehet elérni. Ezt vannak akik elérhetik, mások viszont nem. Mi a tennedőd?

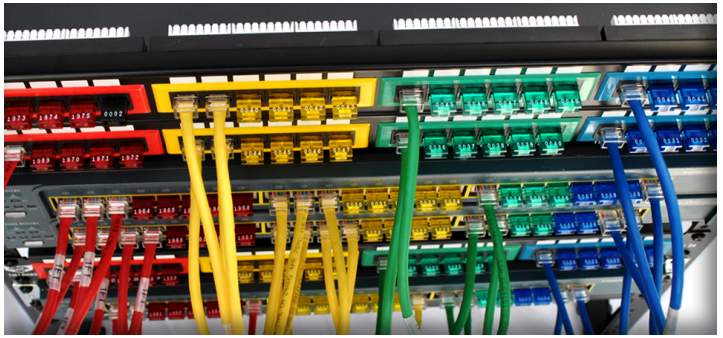
Megoldás

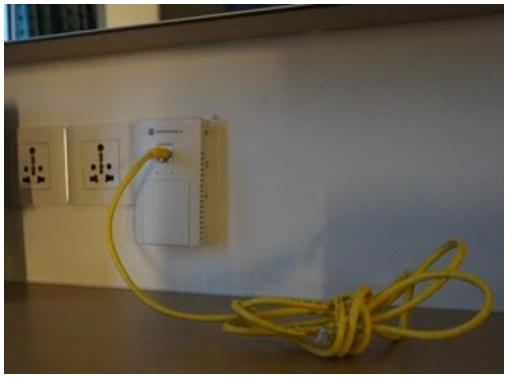
Probléma
a megoldással

1. Szint: jelszóvédelem



2. Szint: IP címre korlátozás





3. Szint: a hálózat védelme

Smart Vision Solutions
taking you one step ahead

Idegen eszközök, védett portok

- Idegen eszközök a hálózaton, általában hálózati eszközök (idegen switch, access point)
- Gyakran veszélyes, tiltott, mert a hálózat ellenőrizetlen kiterjesztését valósítják meg
  - Lehet nagyon biztonságos a hálózatod, de csak addig, amíg valaki rá nem köt egy **jelszavazatlan** wifi AP-t
  - Lehet letűzfallal ellenőrzött kijárat a hálózatodból, de valaki ráköt egy 4G-s modemet akkor simán megkerüli a tűzfalan, sőt, bárki más is ezt simán megteheti ugyanazon a hálózaton

- Védett portoknak most itt azokat nevezzük, amelyekre kijelölt végpontokat és csak azokat engedünk
  - Portok, amelyekre egy-egy kitüntetett gépet várunk (szerver, kijelölt PC stb)
  - Ezeken a portokon lehetnek olyan beállítások, amelyek több jogosultságot biztosítanak
  - Mivel a jogosultságok a portokhoz tartoznak, nem a végponthoz, más ebbe kötve magát örökli ezeket

- A fenti problémák egyszerű megoldása arra épít, hogy a MAC címek nem babráltak
- Az egyszerű megoldás neve: port security

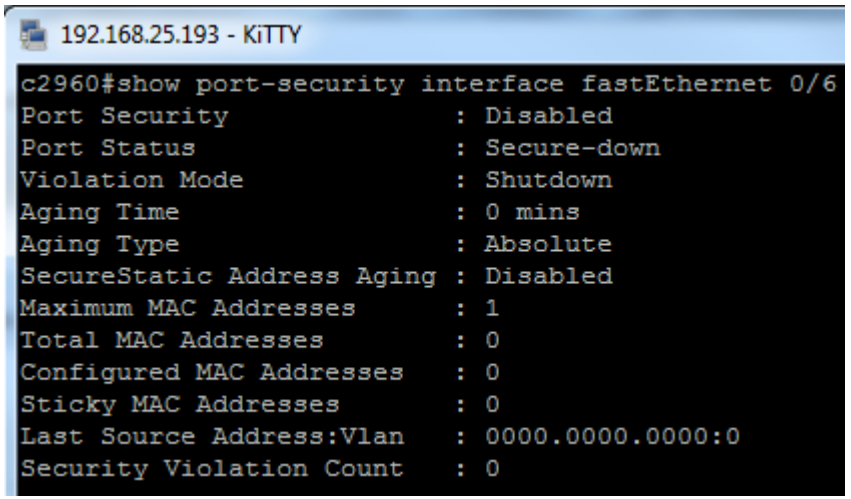
- Adott darabszámú, előírt MAC címek csatlakozhatnak csak egy switchportra
- Amennyiben nem azok a MAC címek, vagy több, a port
  - naplózhatja, hogy mi történt
  - eldobhatja a forgalmat, ami tiltott
  - lekapcsolhatja a portot, megszűntetve minden forgalmat

- Ezt fogjuk bekonfigurálni és tanulmányozni

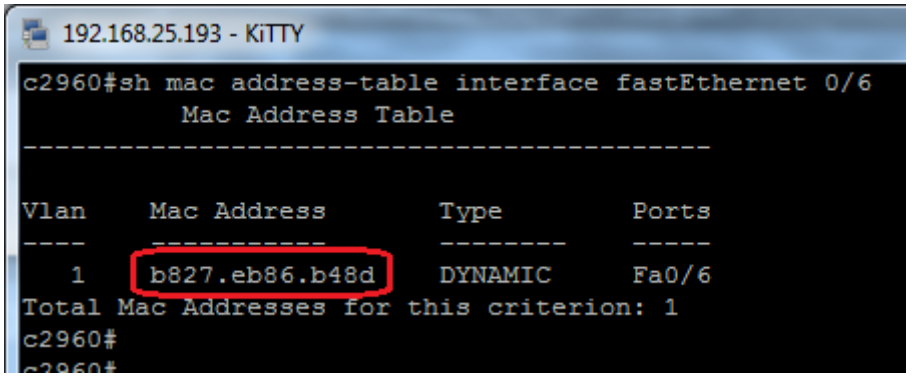
Port security példa

- Szükség lesz a Pi MAC címére
- Lehetséges opciók: shutdown, restrict, protect
  - shutdown: lekapcsolja a teljes portot
  - restrict: a “jó” MAC címek forgalmazhatnak, a “rossz” címek nem
  - protect: ugyanaz, mint a restrict, de értesítést is kapunk (log, snmp)
- A demóhoz nekünk most shutdown kell, hogy lássuk, hogyan működik
- Csak access módban működik

Kiindulási állapot



Port security kikapcsolva



Egy MAC cím a porton

Port security (2)

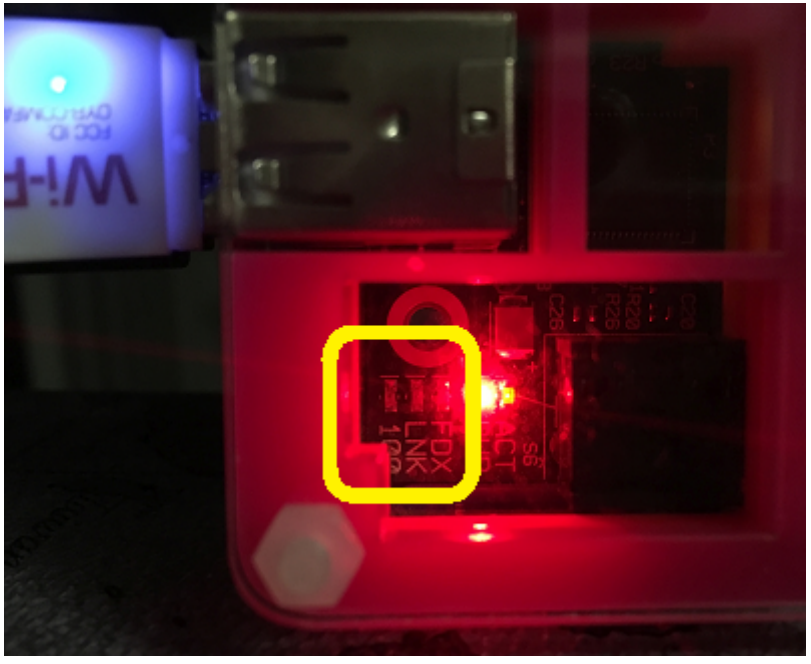
```
File  Edit  Setup  Control  Window  Help
Dec 11 22:34:28.737: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/6, putting Fa0/6 in err-disable st
ate
c2960#
Dec 11 22:34:28.745: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address b827.e
b86.b48d on port FastEthernet0/6.
c2960#
Dec 11 22:34:29.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down
c2960#
Dec 11 22:34:30.741: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to down
c2960#
```

- A port ún error-disabled állapotba került
- Ebből az állapotból beállítás függvénye, hogy automatikusan vissza tud-e térni működő állapotba, és ha igen, mennyi idő után
- A port úgy látszik, mintha nem lenne kábel bekötve

```
c2960#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
link-flap                    Disabled
mac-limit                    Disabled
loopback                     Disabled
pagp-flap                    Disabled
port-mode-failure            Disabled
pppoe-ia-rate-limit          Disabled
psecure-violation            Disabled
security-violation           Disabled
sfp-config-mismatch          Disabled
small-frame                  Disabled
```

```
c2960#show interfaces status

Port      Name               Status       Vlan
Fa0/1                        notconnect   1
Fa0/2                        notconnect   1
Fa0/3                        notconnect   1
Fa0/4                        notconnect   1
Fa0/5                        notconnect   1
Fa0/6     [rpi]              err-disabled 1
Fa0/7                        notconnect   1
Fa0/8     [uplink]           connected    trunk
Gi0/1                        notconnect   1
c2960#
```

Port security (3)



```
pi@raspberrypi: ~
pi@raspberrypi:~ $ /sbin/ethtool eth0
Settings for eth0:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Advertised pause frame use: Symmetric Receive-only
        Advertised auto-negotiation: Yes
        Speed: 10Mb/s
        Duplex: Half
        Port: MII
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
Cannot get wake-on-lan settings: Operation not permitted
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: no
pi@raspberrypi:~ $
```

- A végpont szempontjából nincs link, nincs fizikai kapcsolat
- Ha több gép volt csatlakoztatva switchen át, mind csak a kalóz switchig fog látni, tovább nem
- A MAC címet kézzel kellet beírni. Sok végpontnál ez nem praktikus, se nem skálázható
- Minket nem érdekel, ha egy porton valami megoldható, sok ezer, tízezer portra akarjuk megoldani
- Áthidaló megoldás a sticky kulcsszó, ami azonban kevésbé biztonságos (ellenőrzött)

```
192.168.25.193 - KiTTY
c2960#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
c2960(config)#int fa 0/6
c2960(config-if)#shutdown
c2960(config-if)#$rt port-security mac-address b827.eb86.b48a vlan access
c2960(config-if)#switchport port-security mac-address b827.eb86.b48d
c2960(config-if)#no shutdown
c2960(config-if)#end
c2960#
```

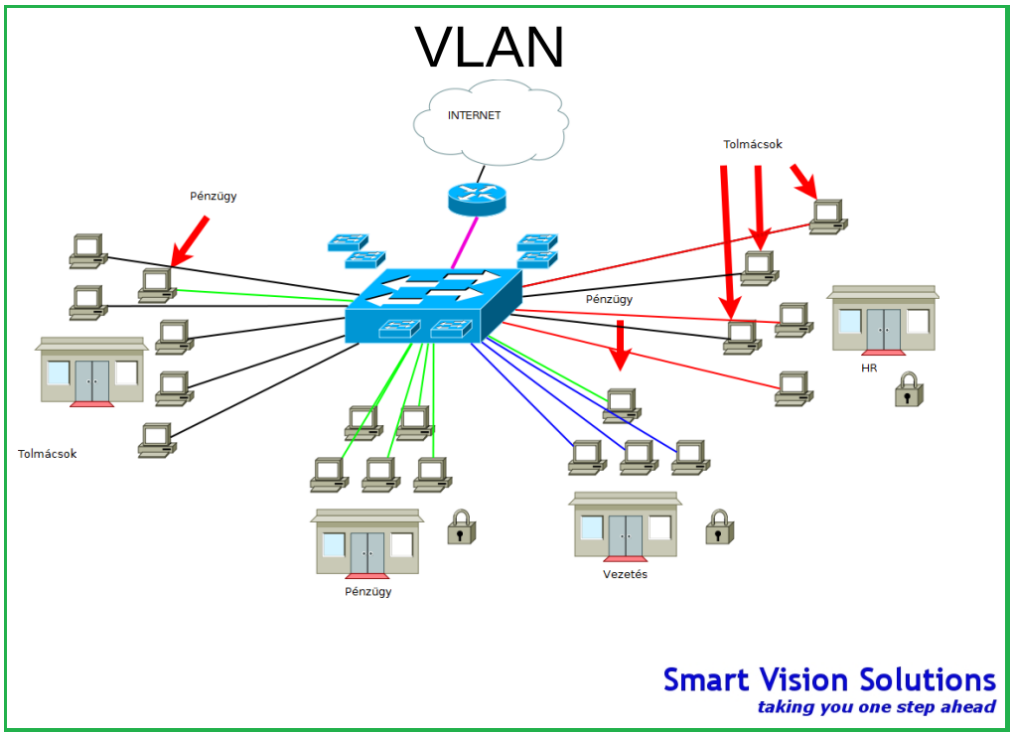
Smart Vision Solutions
taking you one step ahead

VLANok portokhoz rendelése

- A korábbi előadásokon kitárgyaltuk a VLANokat, valamint azt, hogy portokat VLANokba lehet rendelni
- Sőt, rögtön a VLANok felvezetésénél elhangzott, hogy egy switch, több virtuális hálózat, a fizikai portok más – más hálózatba lehetnek kötve és mindez szoftveresen konfigurálható
- Az akkor példa a tolmácsoké volt, ahol a különböző munkakörök emberei eltérő hálózatokhoz férhettek hozzá

Akkor azt mondtam, hogy a konfiguráció statikus és be is mutattam ezt

A parancs: **switchport access vlan X** ahol X a VLAN sorszáma. A hálózati rendszergazda feladata tehát, hogy a portokat kiossza és megfelelően bekábelezze.



Mi történik, ha egy-egy végpont néha átköltözik?

Mi történik, ha hetente egy tucat végpont átköltözik?

Mi történik, a végpontok százai naponta vándorolnak?

VMPS

- Vlan Membership Policy Server
- Cisco protokoll
- Funkciója, hogy MAC címek alapján automatikusan legyen VLANokba sorolva a switchport
- A működéshez szükség van egy VMPS szerverre
- VMPS szerverként lehet Cisco switcheket használni (pl. CatOS-t futtató 6500 tud ilyet)
- VMPS kliens maga a switch (hasonlóan a RADIUShoz, ahol a kliens nem a végfelhasználó)
- A switch a MAC címet elküldi a szervernek, az válaszol egy VLAN sorszámmal
- Hasonló a RADIUShoz, a döntést a szerver hozza, a switch vakon követi
- Cisco switchen kívül a freeradius tud VMPS szerver lenni
- A port security és a VMPS **kizárja egymást**: vagy egyik, vagy másik van a switchporton
- A VMPS szerver kritikus fontosságú: ha leáll vagy elérhetetlen lesz, a VMPS portok nem fognak semelyik VLANba sem tartozni --> senkinek nem lesz hálózata
- Hiba esetén érdemes figyelni a sárga port állapotra, ami normál esetben zöld

192.168.25.193 - KiTTY

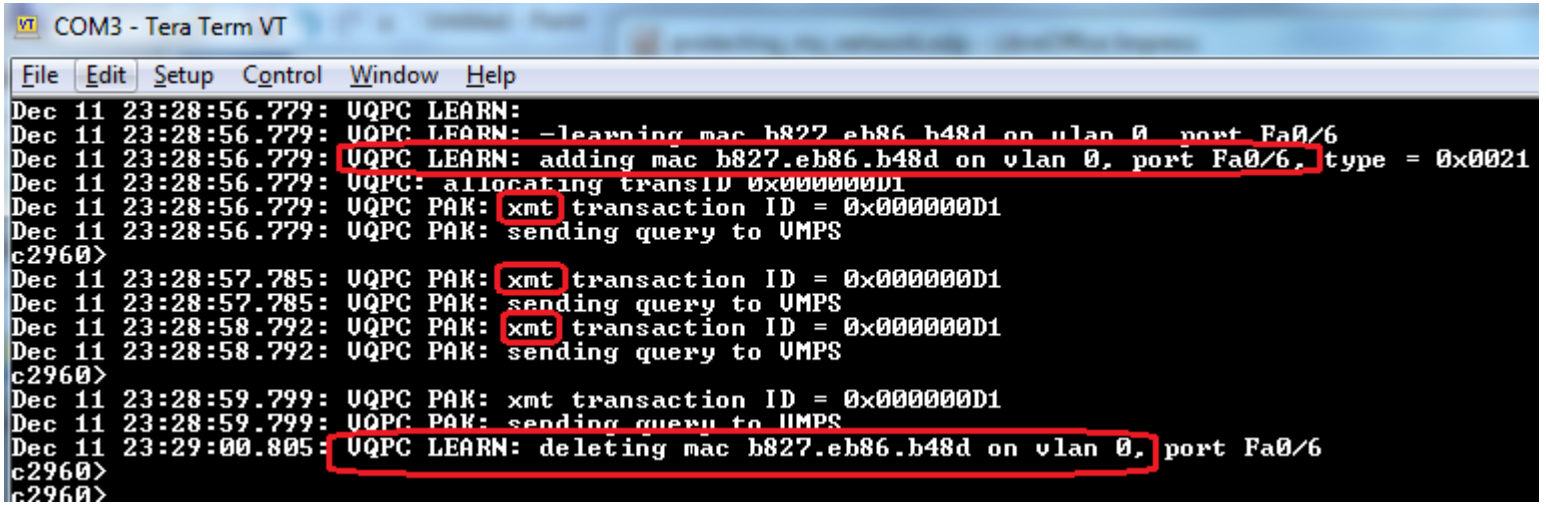
```
c2960(config)#vmps server 192.168.25.195 primary
c2960(config)#int fa 0/6
c2960(config-if)#switchport access vlan dynamic
c2960(config-if)#end
c2960#
```

```
c2960#sh int status

Port      Name               Status       Vlan       Duplex
Fa0/1                        notconnect   1            auto
Fa0/2                        notconnect   1            auto
Fa0/3                        notconnect   1            auto
Fa0/4                        notconnect   1            auto
Fa0/5                        notconnect   1            auto
Fa0/6     [rpi]              connected    unassigned a-full
Fa0/7                        notconnect   1            auto
```

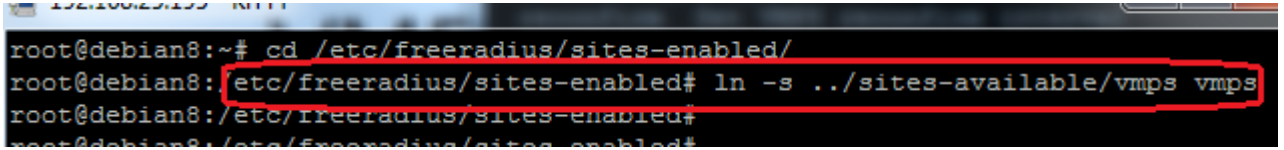
Smart Vision Solutions
taking you one step ahead

VMPS (2)

- Látható, hogy a VMPS bekapcsolásra került, de nem sikerült a portot egyátalán VLANba tenni. Miért?

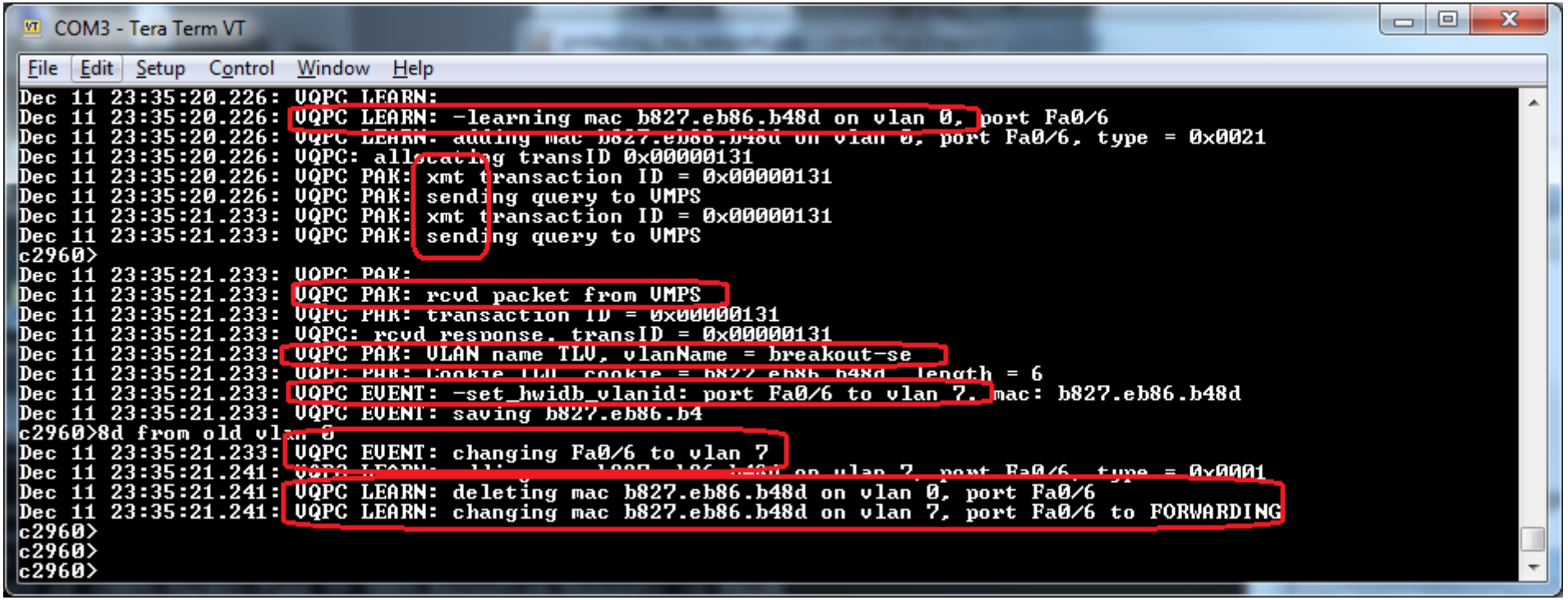


- A MAC címet felismeri, megtanulja és VLAN 0-ba helyezi
- A VLAN 0 érvénytelen, nem létezik (csak **1-4096** közötti VLANok léteznek, **emlékezz a tanultakra!**)
- Folyamatosan küldi a kéréseket a VMPS szervernek, de nem kap választ
- A kretén debian-stílus: a VMPS konfig ott van, el van készítve, de nincs “bekapcsolva”

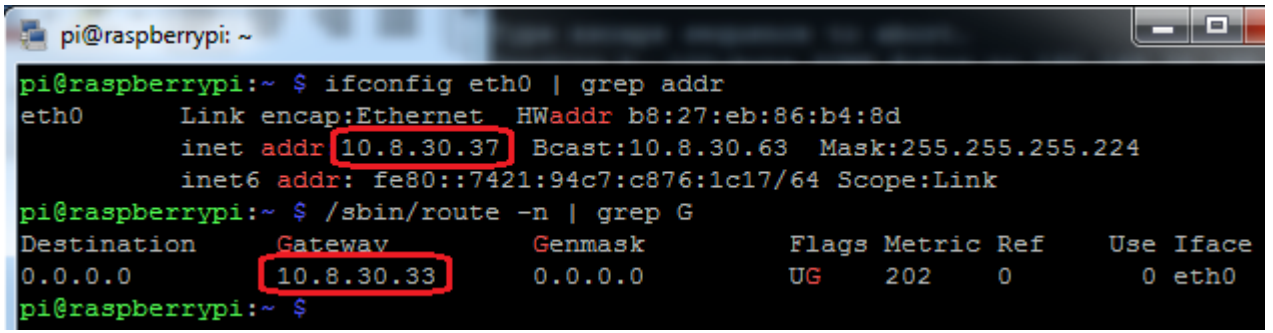


Smart Vision Solutions
taking you one step ahead

VMPS (3)



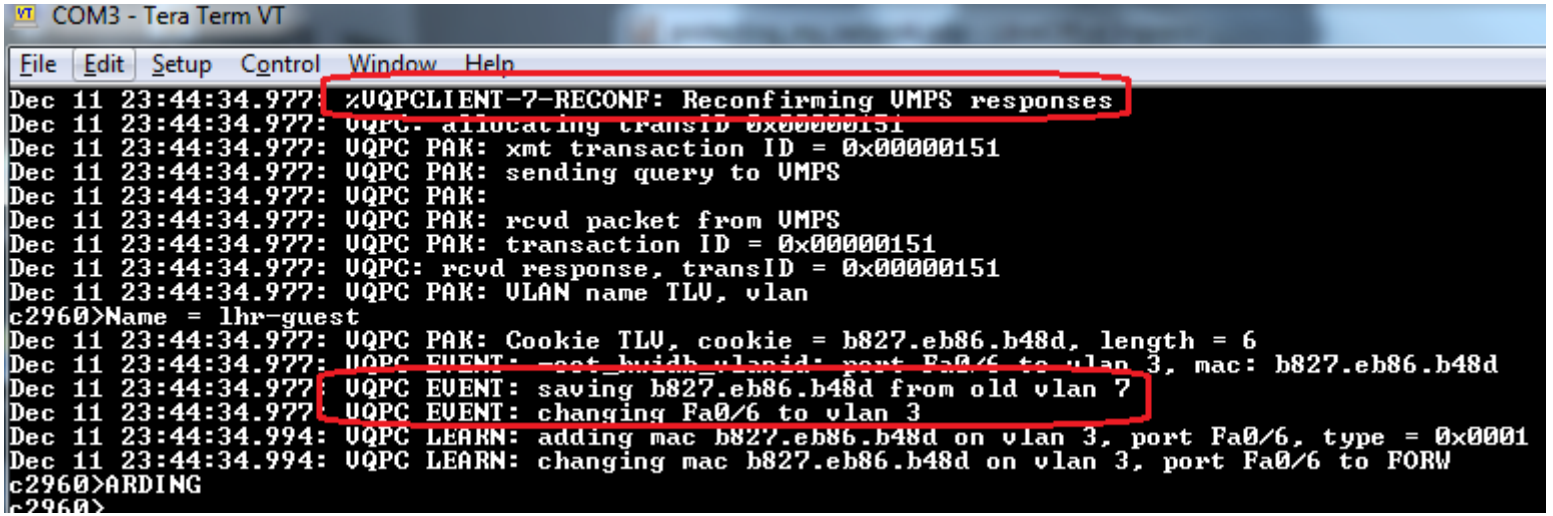
- VLAN nevet kaptunk a VMPS szervertől
- A VMPS nem felelős a VLAN konfigurációért a switchen, csak az allokációért
- Amennyiben a VLAN név létezik és stimmel, a switchportot berakja a switch a megfelelőbe
- A végfelhasználó innentől tudja használni a portot, számára ez a folyamat **transzparens**



Smart Vision Solutions
taking you one step ahead

VMPS (4)

- Mi történik, ha a MAC cím nincs az adatbázisban? Fallback VLAN
- Ez a freeradius szerveren a konfigurációban állítható (mi a default)
- A VLAN hozzárendelés a switchporthoz menet közben dinamikusan változhat
- A switch periodikusan lekérdezi a VMPS szervertől a MAC – VLAN összerendelést
- Kézzel is indítható: **vmps reconfirm** parancs
- A VMPS a végpont számára teljesen transzparens
- Tehát a VLAN megváltozásáról sem fog tudni
- Ha nincs DHCP, nem is fog soha tudni arról, milyen új IP címet kellene kapnia
- Ha van DHCP, a kliens előbb-utóbb kér IP címet, a jó VLAN-ból fog kapni
- Gyorsítható rövid lease time beállításával a DHCP szerveren
- Gyorsítható az interfész kézzel billentésével (shut / no shut, vagy kábel kihúzás – visszadugás)
- Az **átlag szemlélőnek** ez csak úgy tűnik, **mintha egy újraindítás megjavítana egy hálózati hibát**
- De most már tudod, hogy mi van a háttérben és azt, hogy ez egyátalán nem hibás működés



VMPS (5)

- Mire használható?

- MAC címek nyomonkövetése, naplózása
  - A VMPS mellékhatása, hogy minden MAC címről naplózásra kerül, merre járt
  - Lopott eszközök hol voltak utoljára használva?
  - Laptopot merre felejtettem?

- Gyakran vándorló végpontok
  - Bárhova mozog egy laptop, emberi beavatkozás nélkül mindig a jó VLAN-ba kerül
  - Nem kell várni a rendszergazdára, hogy újrakonfigurálja a hálózatot
  - Nem kell a rendszergazdának időt tölteni ilyen apróságokkal

- Szabad, bárki által elérhető végpontok (irodák, közös helységek)
  - A switchport “kaméleon” módban üzemel
  - Egy megbízható MAC cím észlelésekor egy normál VLANba kerül
  - Egy idegen MAC címre korlátozott VLANba kerül
  - Nem kell aggódni, ki mit dug be a szabadon lógó kábelekbe

- Guest VLAN: bárhol
  - Minden ismert MAC címet felvenni egy SQL-be, a megfelelő VLAN névvel
  - A nem ismertek pedig a guest VLAN-ba kerülnek, mindegy, hova mennek

A problémák

- Mint minden protokoll vagy funkció, miközben megoldást kínál valamire, újabb problémát vet fel
- Egyébként ezek felismerése, súlyozása, értelmezése különbözteti meg a kóklert a profitól
- Mind a port security, mind a VMPS a MAC címre épít
- A MAC cím nem állandó, módosítható
- Illetve ez a megoldás nem a végfelhasználót azonosítja, hanem a gépet, amit használ

- Olyan problémára tehát már tudunk megoldást, hogy egy gép mindenhol azonos jogokat kapjon
- Olyanra viszont még nem, hogy ugyanaz a felhasználó kapjon azonos jogokat, mindegy mit haszál
- Ehhez a végpont azonosításától el kell mozdulnunk a felhasználó azonosítása felé

- Egy lehetséges megoldás a végpontokon futtatott szoftver
- Ez azonban gyártófüggő, egyedi megoldás, valamint megkerülhető

- Új protokoll után kell nézni, amit az eddigi előadások alapján még nem ismerünk

802.1x

A bevezetéshez az alábbiakat tesszük:

- Bekonfiguráljuk a switchen, hogy használjon RADIUS szervert a végpontok hálózatba engedéséhez (eddig az eszköz hozzáféréshez használtuk, mostantól a hálózat hozzáféréshez is)
- Bekonfiguráljuk a switchen, hogy egy konkrét végponton használjon 802.1x protokollt
- Vetünk egy pillantást a RADIUS konfigurációra

Honnan indulunk?

```
c2960#sh run int fa 0/6
Building configuration...

Current configuration : 102 bytes
!
interface FastEthernet0/6
 description [rpi]
 switchport access vlan 7
 spanning-tree portfast
end
```

```
root@raspberrypi:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.8.30.33      0.0.0.0         UG    202    0        0 eth0
10.8.30.32      0.0.0.0         255.255.255.224 U     202    0        0 eth0
192.168.25.192  0.0.0.0         255.255.255.224 U     303    0        0 wlan0
```

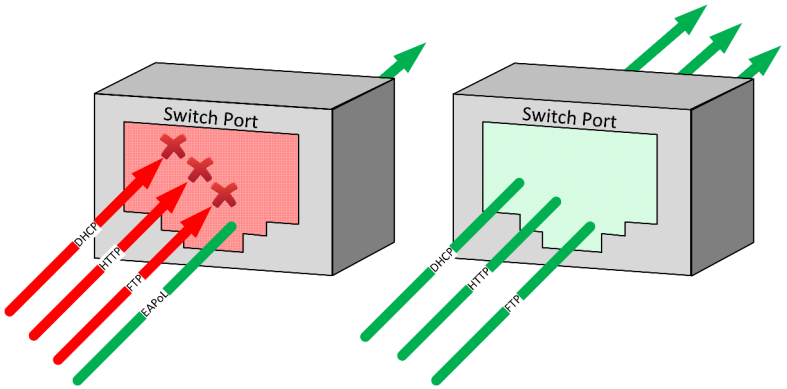
```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.8.30.33  0.821 ms  0.757 ms  0.733 ms
 2  178.73.210.225  41.655 ms  42.224 ms  43.573 ms
 3  178.73.210.1  46.078 ms  46.402 ms  47.874 ms
 4  80.67.4.192  49.353 ms  51.415 ms  49.639 ms
 5  192.121.80.47  51.293 ms  52.883 ms  53.138 ms
 6  216.239.54.181  55.063 ms  53.808 ms  54.926 ms
 7  209.85.245.61  56.068 ms 72.14.234.83  40.931 ms 72.14.234.87  42.199 ms
 8  8.8.8.8  42.438 ms  41.486 ms  40.905 ms
```

```
root@raspberrypi:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=40.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=40.3 ms
```

802.1x (2)

- Már konfiguráltunk az AAA-ból AA -t, azaz: Authentication, Authorization megvolt
- Eddig ezt a switchen konfiguráltuk ahhoz, hogy RADIUS alapú azonosítással és megfelelő jogokkal érjük el
- Már a múltkor is azt mondtam: **ha hálózatos karriert tervezel, akkor köss barátságot az AAA-val!**
- Most is ugyanazt konfiguráljuk, az első A-t a háromból, de most a hálózati hozzáférésre
- A switch EAPoL kereteket vár (Extensive Authentication Protocol over LAN) minden mást eldob

  - Amíg az azonosítás nem történik meg, a switch jelzi is, hogy autentikációt vár
  - Ezek a speciális keretek azok, ahonnan a kliens felismeri, hogy mit kell tennie (ha van szoftvere hozzá!)
  - Innen tudja a windows, hogy fel kell dobnia egy buborékot, amiben közli, hogy azonosítanod kell magad
  - Mi itt ma raspberry pi klienst használunk, ez nem dobál semmilyen buborékot sehova



Switch oldalon innen indulunk:

```
c2960#show run | i aaa
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius
aaa session-id common
```

A már a múltkor bekonfigurált AAA kiegészítése a mostani feladathoz:

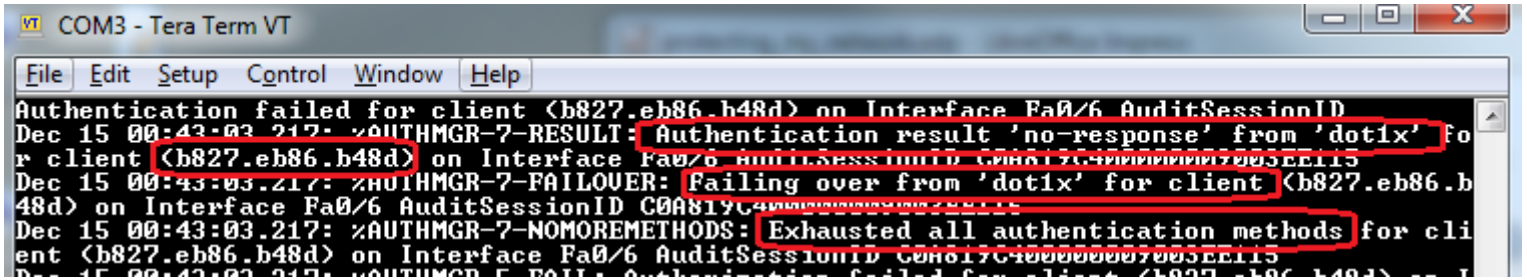
aaa authentication dot1x default group radius
dot1x system-auth-control

interface fastethernet 0/6
  dot1x port-control auto

802.1x (3)

Mit látunk ezen a ponton?

- A switch már beállítva 802.1x-re
- A radius szerver készen áll
- A kliens pedig forgalmazni próbál – de nem megy neki. Ez az a pont, ahol “nem megy a hálózat”
- Hibakeresés során pedig a switchen az látszik, hogy a kliens minden forgalmára válaszként EAPoL megy ki, de a kliens nem válaszol ezekre a keretekre
- Innen nyilvánvaló, hogy vagy nem történik azonosítás, vagy a kliens nem támogatja
- Látható, hogy nem állítottunk be fallback-et sem! Csak radius van, ha az nem ment, ennyi volt.




```
root@raspberrypi:~# dhclient -d -v eth0
Internet Systems Consortium DHCP Client 4.3.1
Copyright 2004-2014 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/b8:27:eb:86:b4:8d
Sending on   LPF/eth0/b8:27:eb:86:b4:8d
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
```

Mindeközben a kliensen...

... a felhasználó szerint nincs internet, levelet ír a levlistára, ahol azt mondják neki indítsa újra, húzza ki a kábelt, majd dugja vissza, esetleg kérjen újra IP címet... ami persze nem fog működni, hiába van link a kábelen, ha nem történt meg az azonosítás...

802.1x (4)

```
root@raspberrypi:~# cat /etc/wpa_supplicant/wpa_supplicant.conf
country=GB
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1

#802.1x
eapol_version=2

#802.1x
network={
        key_mgmt=IEEE8021X
        eap=TTLS MD5
        identity="sysadmin"
        anonymous_identity="sysadmin"
        password="titok"
        phase1="auth=MD5"
        phase2="auth=PAP password=titok"
        eapol_flags=0
}

# wifi
network={
```

Már tehát csak a kliens van hátra a teljes sikerhez. Kliens oldalon a linux alapból nem támogatja a 802.1x -et, szükséges hozzá egy külön szoftver. Ez ugyanaz, mint ami a WiFi hálózatoknál ismert azonosításhoz is használható, hiszen most is ugyanaz fog történni, csak épp vezetéken át.

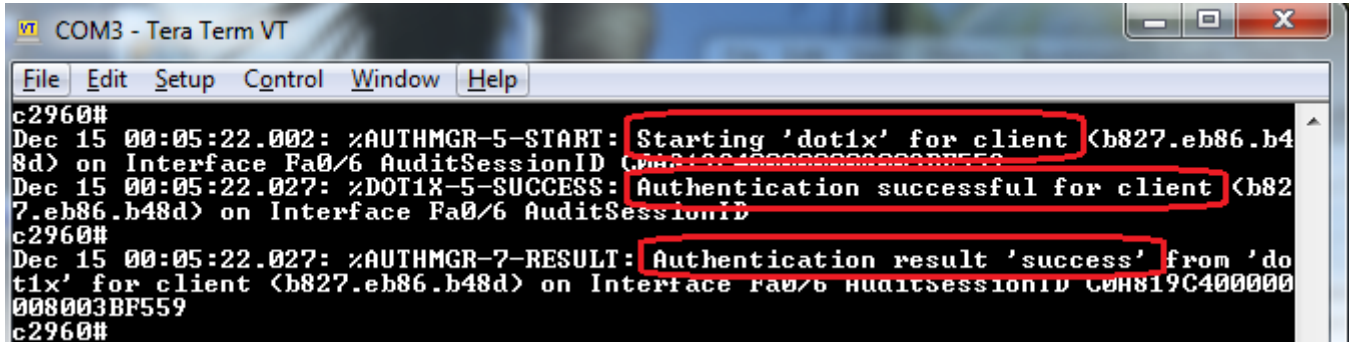
Windows / Mac, de még egy GUI-val rendelkező linux esetén is egyszerűen felbukkan egy ablak ami bekéri az adatokat.

```
root@raspberrypi:~#
root@raspberrypi:~# wpa_supplicant -c /etc/wpa_supplicant/wpa_supplicant.conf -D
 wired -i eth0
Successfully initialized wpa_supplicant
eth0: Associated with 01:80:c2:00:00:03
eth0: CTRL-EVENT-EAP-STARTED EAP authentication started
eth0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=4
eth0: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 4 (MD5) selected
eth0: CTRL-EVENT-EAP-FAILURE EAP authentication failed
eth0: CTRL-EVENT-EAP-STARTED EAP authentication started
eth0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=4
eth0: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 4 (MD5) selected
eth0: CTRL-EVENT-EAP-FAILURE EAP authentication failed
eth0: CTRL-EVENT-EAP-STARTED EAP authentication started
eth0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=4
eth0: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 4 (MD5) selected
eth0: CTRL-EVENT-EAP-FAILURE EAP authentication failed
eth0: CTRL-EVENT-EAP-STARTED EAP authentication started
eth0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=4
eth0: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 4 (MD5) selected
eth0: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
eth0: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 completed [id=0 id_
str=]
```

Sikeres azonosítás esetén a kliens is megmondja, hogy minden rendben, hiszen kapott a switchtől információt az azonosítás sikerességéről, EAPoL keretekben.

Ez az a pont, ahonnan részesei vagyunk a hálózatnak, kérhetünk IP címet, forgalmazhatunk és a switch nem fogja eldobni azt.

802.1x (5)



A sikeres azonosítás a switch oldaláról – látható hol, milyen MAC cím jutott be a hálózatba és az is, hogy miért.

```
c2960#show dot1x all details
[...]
Dot1x Authenticator Client List
-------------------------------
Supplicant                  = b827.eb86.b48d
Session ID                  = C0A819C40000000200131CA7
    Auth SM State           = AUTHENTICATED
    Auth BEND SM State      = IDLE
Port Status                 = AUTHORIZED
```

Az egyes portok állapota külön paranccsal is lekérdezhető, a kimenetben látható, milyen MAC cím azonosította magát, valamint a port aktuális állapota.

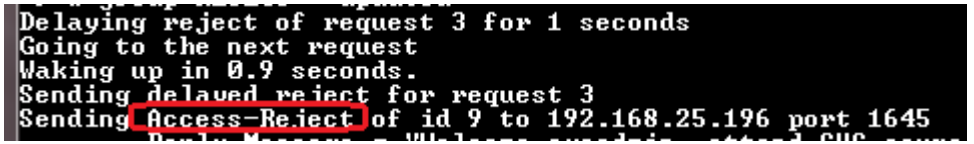
```
root@raspberrypi:~# dhclient -v -d eth0
Internet Systems Consortium DHCP Client 4.3.1
Copyright 2004-2014 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/b8:27:eb:86:b4:8d
Sending on   LPF/eth0/b8:27:eb:86:b4:8d
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPOFFER from 10.8.30.33
DHCPACK from 10.8.30.33
bound to 10.8.30.39 -- renewal in 1517 seconds.
```

Ez után a kliens természetesen azonnal kérhet és kaphat is címet DHCP-vel, mert most már része a hálózatnak, beengedtük.

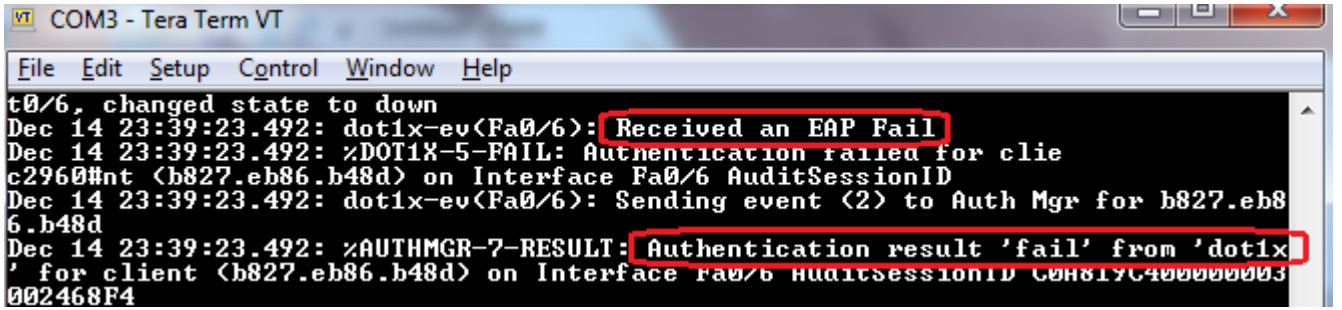
802.1x (6)

Mi történik, amikor
- elrontja a jelszót a végfelhasználó?
- vagy nem jogosult a hálózat használatára?
- vagy nem akkor, amikor próbálja?

Ezeket a döntéseket, mint korábban is, a RADIUS szerver hozza meg, a switch csak “betartja”. Ha úgy tetszik, a RADIUS a törvényhozó politikus, a switch pedig a rendőr és a bíró egyszerre.



A RADIUS szerver szerint nem netezhet ez a felhasználó



A switch meg kézbesíti az “ítéletet”: EAP Fail.

Milyen okok miatt lehet sikertelen az azonosítás?
- Szimplán helytelen név / jelszó / letiltott felhasználó
- Már be van lépve ugyanez a felhasználó máshonnan, egyszerre csak egy belépés lehetséges
- Időkorlát van, pl. tanulók éjfél után, vagy tanítási időben nem netezhetnek
- Földrajzi korlát van: bizonyos gépekről bizonyos felhasználók nem netezhetnek
- Esetleg: egy tanuló egy nap csak adott mennyiséget forgalmazhat (pl. napi 200 MB) és elérte a limitet
- Vagy ezek tetszőleges kombinációja (tanuló gépteremből csak 100 MB-t tölthet le, mindegy melyik gépet vagy gépeket használja ehhez)

802.1x (7)

Dőlj hátra. Lazíts. Ha kezdő vagy a hálózatok világában, akkor az előző slide megértése után valószínűleg pörög az agyad. **Egy egész világ tárult ki előtted.** Lázasan gondokodsz: mennyi mindent fogsz tudni ezután beállítani, amire eddig nem is gondoltál!

Ezentúl a publikusan hozzáférhető gépekre amikor a felhasználó belép, attól függően **lesz, vagy nem lesz** hálózati hozzáférés az adott gépen, hogy az **illetőnek szabad-e vagy sem** azt használnia. Ráadásul ez a tulajdonság **követi** a felhasználót: **bármely gépre** lép is be a saját azonosítójával, **mindegyiken ugyanezt** tapasztalja majd.

Fokozzuk az eufóriát, emeljük a tétet.

Az, hogy egy gépnek vagy abszolút **van**, vagy abszolút **nincs** hálózata a **felhasználótól függően**, nem elég. Ez túl bináris. Mi lenne, ha **mindenképp lenne** hálózata, de **attól függően** érne vagy nem érne el erőforrásokat, **hogy szabad-e neki?** Például: diákok éjfél után nem netezhetnek, **de a belső hálózatot elérhetik**. Vagy elérhetnek **bizonyos oldalakat** az interneten. Vagy **tudhatnak levelezni**, de **nem tudhatnak chatelni**.

Mindez rendkívül egyszerűen megvalósítható, ha már az eddigiek amúgy is megvannak. Lehet bonyolultabban és egyszerűbben. Bonyolultabban: miután a **felhasználó azonosította magát**, egyedi, **rá jellemző tűzfal szabályok**at lehet leküldeni a switchnek a RADIUS szerverből. Egyszerűbben: ha nem akarunk tűzfal szabályokkal vacakolni, egyszerűen **attól függően** soroljuk a **switchportot VLANba**, hogy **ki lépett be** a gépre!

Egy pillanatra csak gondolkozz el: ha vannak gépek a tanári irodában, a tanárok számára kialakított alhálózatban:

- mekkora **biztonsági rés**, ha ezekhez a gépekhez valaki illetéktelen fizikailag hozzáfér – hozzáfér a védett hálózathoz is
- mekkora **amatőr** rendszergazdára utal, ha **egy tanárnak a tanáriba kell mennie**, hogy **elérjen bizonyos dolgokat** a hálózaton, mert **az** az alhálózat csak ott van jelen
- méginkább **amatőr** rendszergazdára utal, ha a védett, tanári alhálózat **csak úgy elérhető valahol**, egy nem biztonságos helyen
- és végül gondolkozz el azon, **ha valahol máshol dolgoznál**, ahol komoly feltételeknek kell megfelelni hálózatbiztonság terén, akkor **hogyan oldanád meg**?

802.1x (8)

```
c2960(config)#do sh run | i aaa
aaa new-model
aaa authentication login default group radius local
aaa authentication dot1x default group radius
aaa authorization exec default group radius
aaa session-id common
```

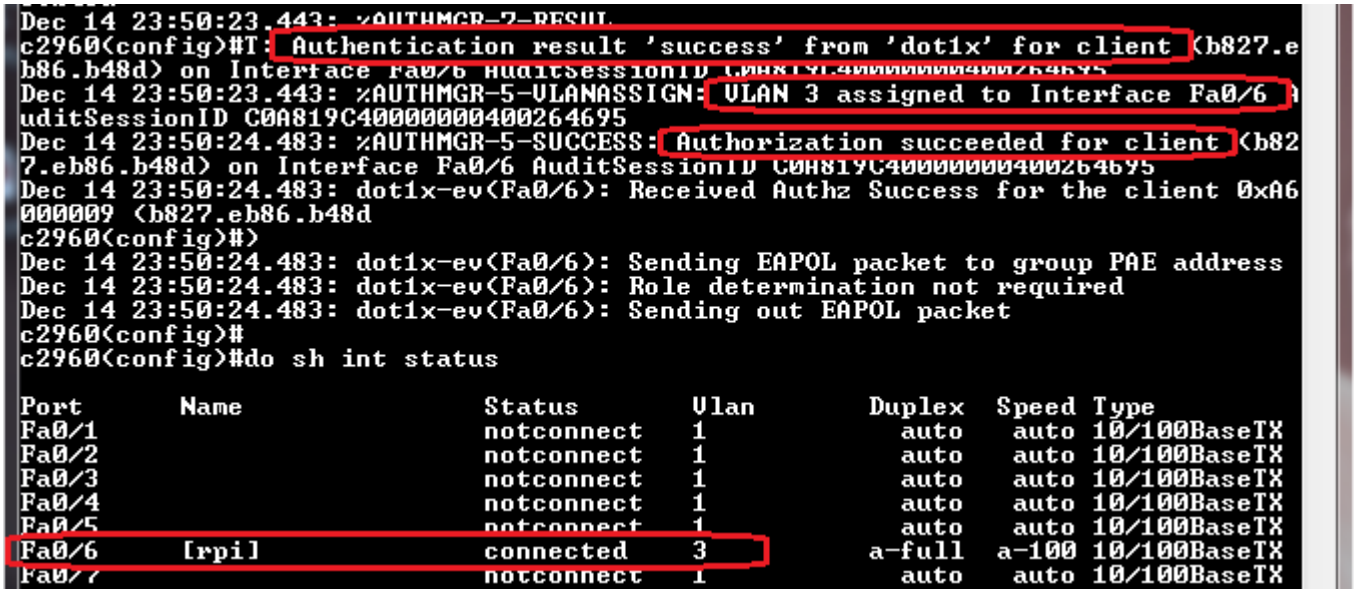
Eddig itt tartunk

```
aaa authorization network default group radius
```

Egyetlen parancsra van szükségünk a switchen

```
sysadmin        Cleartext-Password := "titok"
                Service-Type = NAS-Prompt-User,
                Tunnel-Type = "VLAN",
                Tunnel-Medium-Type = "IEEE-802",
                Tunnel-Private-Group-Id = "lhr-guest"
```

Apró kiegészítés a RADIUS szerveren: emlékezz az AVP-kre (Attribute Value Pair) amiket visszaküldünk: újabbakat ismerünk meg (eddig csak a Reply-Message volt).



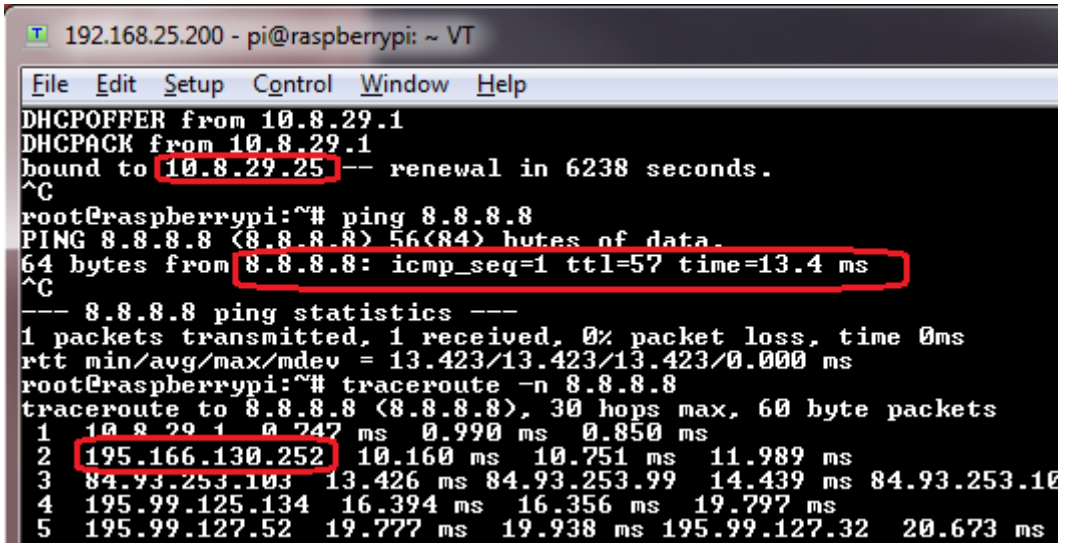
A kliens a következő azonosításkor már **abba a VLANba kerül, amit a RADIUS szerver jelölt ki neki**. Másik VLAN, másik hálózati tartomány, másik IP tartomány, más tűzfal szabályok... tehát **más hozzáférési szint**, **függetlenül** attól, a felhasználó **melyik gépen, hol lépett be**!

802.1x (9)

Az eredeti traceroute, még az előző azonosítás után

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.8.30.33  0.821 ms  0.757 ms  0.733 ms
 2  178.73.210.225  41.655 ms  42.224 ms  43.573 ms
 3  178.73.210.1  46.078 ms  46.402 ms  47.874 ms
 4  80.67.4.192  49.353 ms  51.415 ms  49.639 ms
 5  192.121.80.47  51.293 ms  52.883 ms  53.138 ms
 6  216.239.54.181  55.063 ms  53.808 ms  54.926 ms
 7  209.85.245.61  56.068 ms 72.14.234.83  40.931 ms 72.14.234.87  42.199 ms
 8  8.8.8.8  42.438 ms  41.486 ms  40.905 ms
```

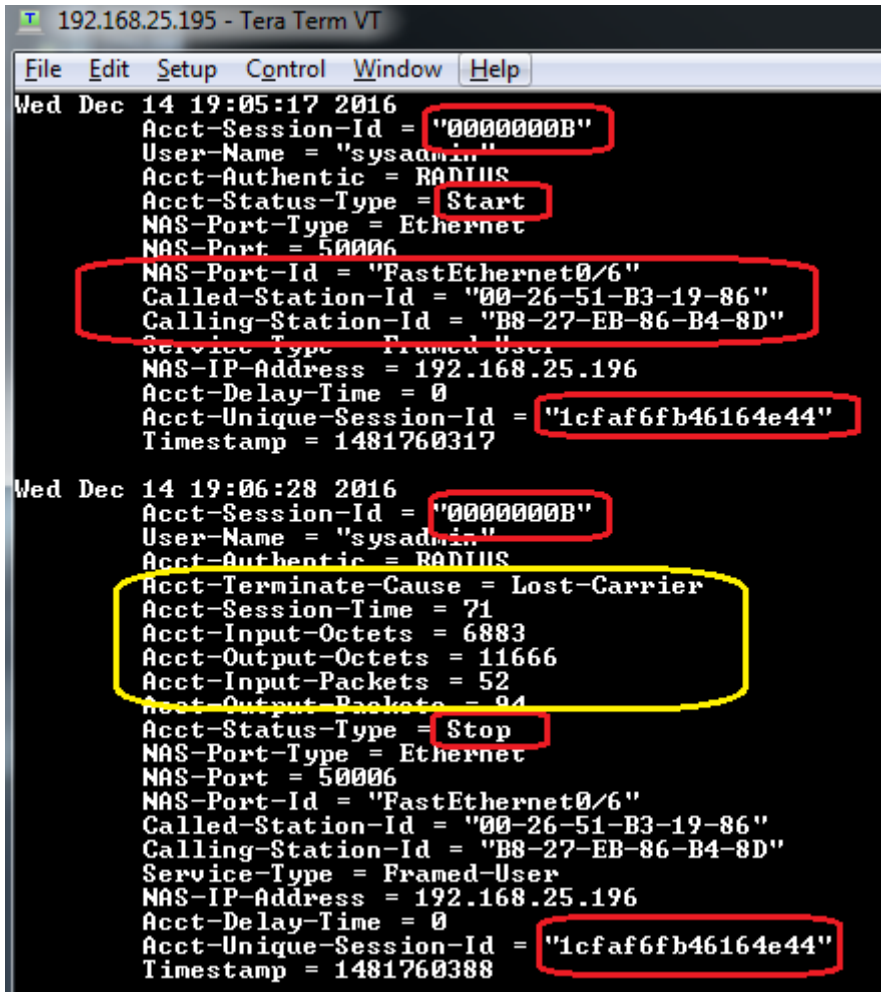
Új azonosítás után új hálózatból kapott IP cím után más útvonal ugyanahhoz a célhoz, más tűzfalon át, más szabályok mentén.



802.1x (10)

Fokozzuk tovább a hangulatot! Eddig a három A-ból (AAA) következetesen csak kettőt használtunk. Itt az ideje használni a harmadikat is. Accounting. Végre van mit számlázni.

Gondolom meg sem lepődsz, ha mindösszesen egy parancs kell ehhez – hiszen már minden eddig megírt és működő konfigurációra építünk.




```
aaa accounting dot1x default start-stop group radius
```

Mostantól minden egyes azonosítás után képződik egy START, a folyamat végén pedig egy STOP rekord. A RADIUS szerver maga nem tudja ezeket az adatokat, a switch küldi el neki, utána a RADIUS csak nyilvántartja.

Mikor keletkezik STOP rekord, mi volt az ok az itt látható esetben? Lost-Carrier: kihúztam a kábelt.

Mi történik, ha a STOP előtt a switch újraindul? Az utolsó UPDATE rekord adatai vehetőek alapul.

Mit lehet kezdeni a számokkal? Ezek a byte- és csomagszámlálók, irányonként bontva. Ezeket SQL-be teheted és a RADIUS azonosításkor felhasználhatja (ugyanezen az alapon működik a telco szolgáltatók forgalomkorlátos vagy percdíjas csomagja is).

Szusszanjunk

Amíg kipihened az izgalmakat, lapozzunk vissza egy kicsit a gondolataink között!

- Novemberben elindultunk az alapoktól. Nyaggattalak a protokollokkal, az ISO rétegekkel. Miért?
- Mert megtanultad a rétegződés folyamatát, annak az értelmét, hogy a rétegek belső szerkezete rejtve maradhat a többi réteg elől, amíg a kapcsolódási pont szabványosított.
- Miután megvoltak a rétegek, beszéltünk a konzolról, távoli hozzáférésről
  - Feltűnt, hogy mindenhez szükséges a konzol, vagy a távoli konzol? Különösen ha nem egy eszközt konfigurálsz.
- Miután megvolt a konzol, beszéltünk az alapvető konfigurációs módokról
  - Feltűnt, hogy a későbbiekben ez előkerült megint? A RADIUS vezérelte eszköz jogosultságoknál építettünk erre a tudásra.
- Felépítettünk egy mini labort, beállítottunk rajta sok protokollt: feszítőfát, stb.
  - Miközben ezt megépítettük, legalább fél tucat trunk és/vagy access portot konfiguráltunk be, rutinosan.
- Miután ez megvolt, jöttek a VLANok
  - Ahhoz, hogy megértsd a problémákat, kellett tudnod a korábbiak alapján, mi a feszítőfa, mi történik a háttérben vele.
- A VLANok után következtek az egyéb, alacsony szintű protokollok
  - Ahhoz, hogy megértsd, mi történik amikor két switchet összekötsz, kellett a DTP, ahhoz kellettek a VLAN ismeretek
  - Ahhoz, hogy megértsd a VTP előnyeit, a veszélyeit, építettünk a korábban megtanult trunk portokra és arra, hogy mi a VLAN
- Megismerkedtél a centralizált felhasználókezeléssel, valamint az AAA alapjaival
  - Feltűnt, hogy mindeközben újra átvettük a korábban már megismert lokális jelszókezelést, felhasználókezelést?
- Most pedig a hálózatod védelme kapcsán megismerkedtél a 802.1x protokollal
  - Feltűnt, hogy teljes egészében az előző előadás során megismert AAA alapokra építkeztünk?
- Valamint megismerted a port security lehetőségeit
  - Feltűnt, hogy most kapott értelmet a MAC cím, valamint az, hogy mindeddig az adatkapcsolati réteggel foglalkoztunk?
- Megismerted a VMPS lehetőségeit
  - És az feltűnt-e, hogy éppen most kombináltuk a MAC cím és a VLAN ismereteket együtt, egy közös protokollban?

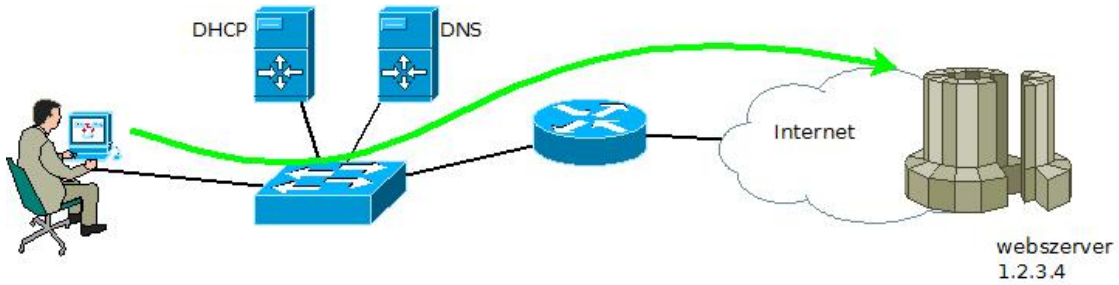
Mostanra gondolom nyilvánvaló, hogy a hálózatok világa nem izolált témakörök egyvelege. Minden összefügg mindennel. Ha jó rendszergazda akarsz lenni aki ért a hálózatokhoz, mindent összefüggésében nézz, keresd a kapcsolatot a már megtanult dolgokkal!

MitM támadási formák

Normális működés

1. Végpont: Itt a MAC címem, kérek IP címet és a hálózati adatokat
2. DHCP szerver: tessék az IP címed, a DNS szerverek címei, az átjáró címe
3. Végpont: DNS szerver, mi a webszerver címe?
4. DNS szerver: 1.2.3.4
5. Végpont: Átjáró, el akarok jutni 1.2.3.4-hez
6. Átjáró: Rajta
7. Végpont: Webszerver, kérem a weboldalt
8. Webszerver: tessék

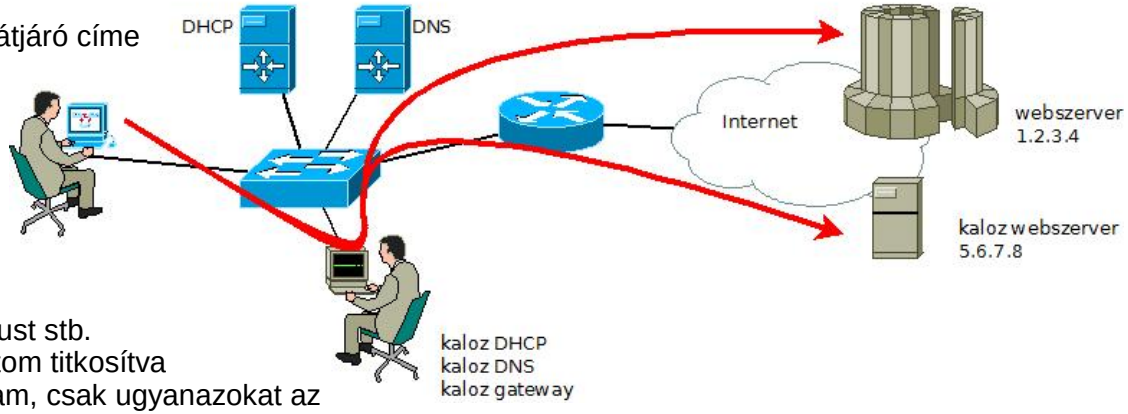
Happy end.



Kalóz működés

1. Végpont: Itt a MAC címem, kérek IP címet és a hálózati adatokat
2. Kalóz DHCP szerver: tessék, itt van mind, én vagyok a DNS és az átjáró is
3. Végpont: köszi
4. Igazi DHCP szerver: tessék az IP címed, a DNS szerverek címei, az átjáró címe
5. Végpont: hmm, már van mindenem, ezeket eldobom
6. Végpont: DNS szerver, mi a webszerver címe?
7. Kalóz DNS szerver: 5.6.7.8
8. Végpont: Átjáró, el akarok jutni 5.6.7.8-hoz
9. Kalóz átjáró: Erre, csak tessék, csak tessék
10. Végpont: Webszerver, kérem a weboldalt
11. Kalóz átjáró némán naplóz mindent, esetleg belenyúl a forgalomba
12. Webszerver: tessék
13. Kalóz átjáró esetleg javascriptet illeszt az oldalba, esetleg trójait, vírust stb.
14. Végpont: milyen érdekes üzenet, vajon mit jelent, hogy minden adatom titkosítva

és 20 bitcoint kell fizetnem értük? Pedig semmi szokatlant nem csináltam, csak ugyanazokat az oldalakat látogattam meg, mint eddig.



Eredmény?

Senki nem érti mi történt, a felhasználó esküszik, hogy semmire nem kattintott, mint amire máskor ne tette volna. A rendszergazda sem érti mi történt és a felhasználót hibáztatja, mindenki hülyének néz mindenkit.

DHCP Snooping

A vázolt támadást számtalan formában lehet kivitelezni, akár titkosított kapcsolatokat is be lehet vele csapni, ha a felhasználó elég gyanútlan. A rendszergazda tehetetlen. A hálózatos pedig, mint mindig, megjavít mindent. Lássuk, hogyan?

A probléma gyökere, hogy:
- megjelent egy idegen DHCP szerver a hálózaton
- senki nem ellenőrzi, hogy milyen paramétereket osztogat
- aki tőle kap paramétereket, gondolkodás nélkül elfogadja azokat

Mit tesz egy rendszergazda?
- ha ügyes a támadó, semmit, mert tudomást sem vesz róla
- ha nem ügyes a támadó, rájön, hogy van egy idegen DHCP szerver
- elkezd kábeleket lehúzgálni, megpróbálni behatárolni, hol van (listán többször javasolták!)
- feltesz egy arpwatch-ot, amivel most már “élő közvetítésben” nézheti a kliensek vergődését

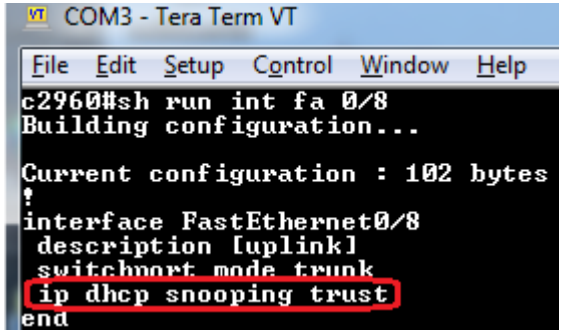
Mit tesz a hálózat üzemeltető?
- bekapcsolja DHCP snooping funkciót a hálózati eszközökön
- elmegy sörözni

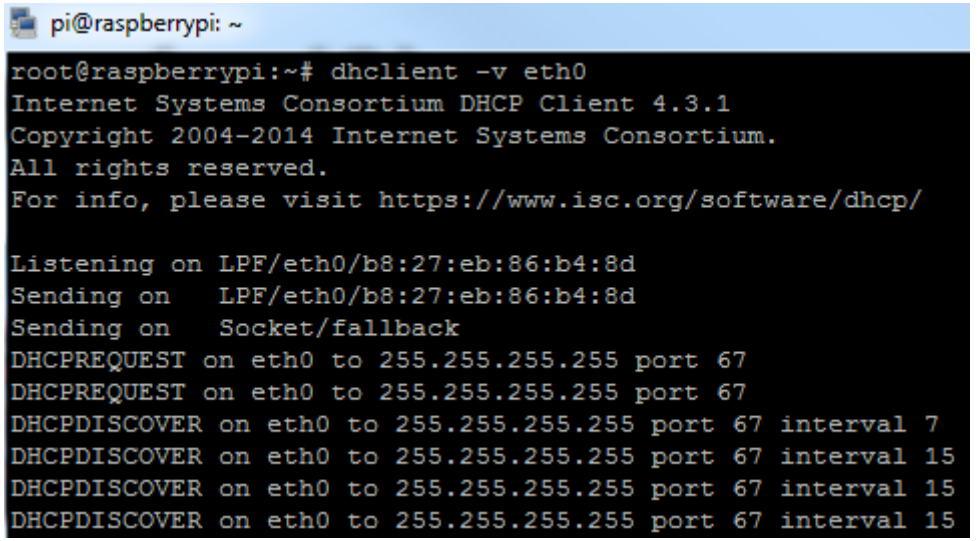
Mi a DHCP snooping?
- Layer 2 technológia arra, hogy csak **a megbízható DHCP szerverek** üzemelhessenek a hálózaton, a nem megbízhatóak pedig nem. A switch a DHCP kéréseket **nem továbbítja**, csak a megbízhatóak felé.
- Eldobják továbbá a DHCP release és decline üzeneteket is, ha ezek a válaszok **nem ugyanarról** a switchportról érkeznek, mint az eredeti kérés
- Ha nem továbbítjuk a kereteket a nem megbízható DHCP szerver felé, valamint a hamisított release/decline üzeneteket eldobjuk, a problémát kiküszöböltük

Hogyan működik?

- A funkciót be kell kapcsolni 1) globálisan, 2) vlanokra egyesével
- Ezek után a switch fenntart egy táblázatot, amelyben minden DHCP információt feljegyez, amit a forgalomból meg tud figyelni:
  - forrás MAC
  - melyik interfészről érkezett
  - milyen címet kapott
  - melyik VLAN
  - meddig érvényes
- A táblázatot folyamatosan karbantartja, hogy tudja milyen DHCP forgalmat kell szűrni
- Sok kliens esetén a táblázat meglehetősen nagyra nőhet – a flash és a memória korlátos
- Ilyen esetekben a táblázatot lehetőség van a swtichen kívül tárolni: tftp szerveren, http/https szerveren, stb.
- Mi történik ha a switch újraindul? A DB agent újraindulás után betölti kívülről a korábbi állapotot
- Tulajdonképpen tekinthető egy Layer 2 tűzfalnak, DHCP-re kihegyezve

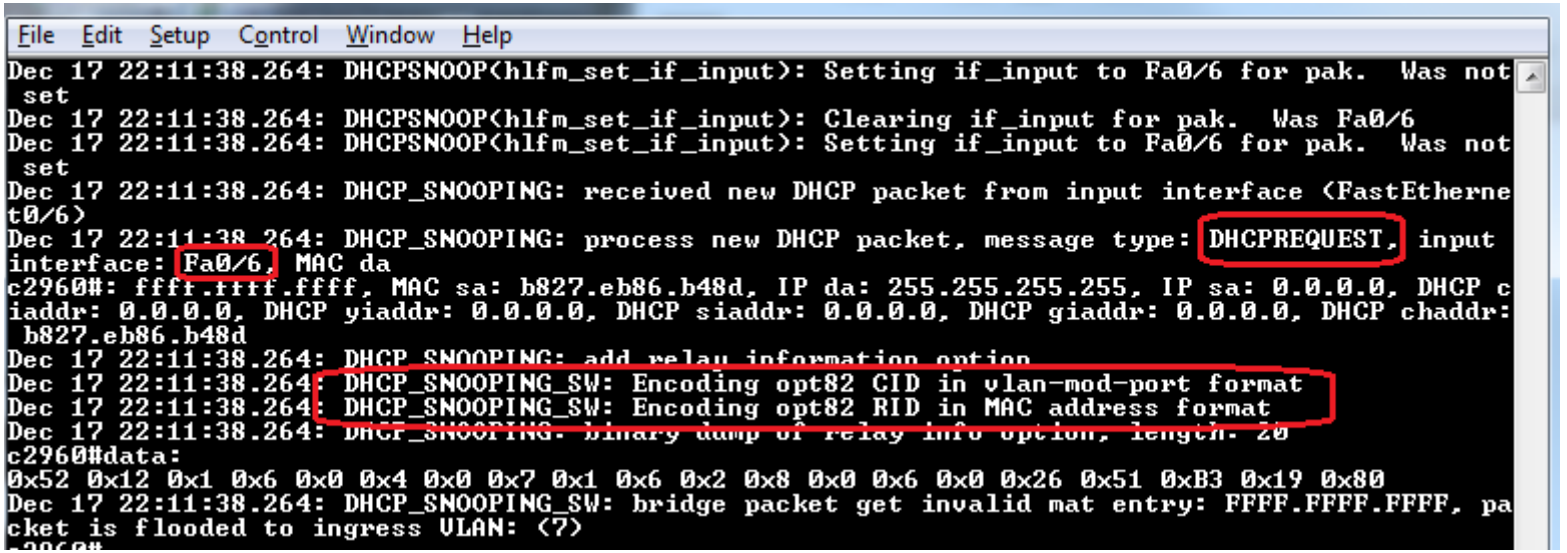
```
ip dhcp snooping
ip dhcp snooping vlan 7
```

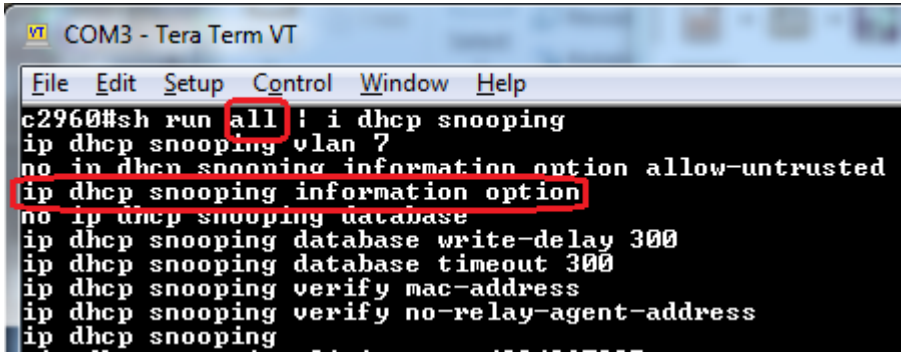




Hibakeresés

```
debug ip dhcp snooping event
debug ip dhcp snooping packet
```

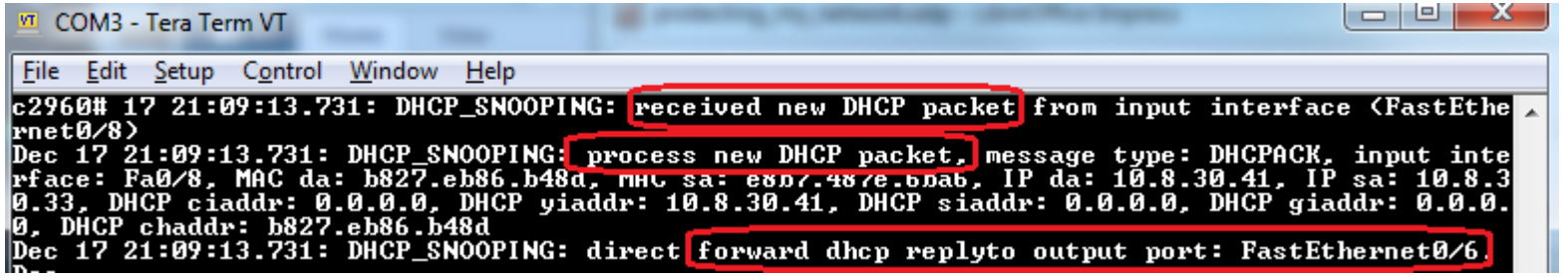


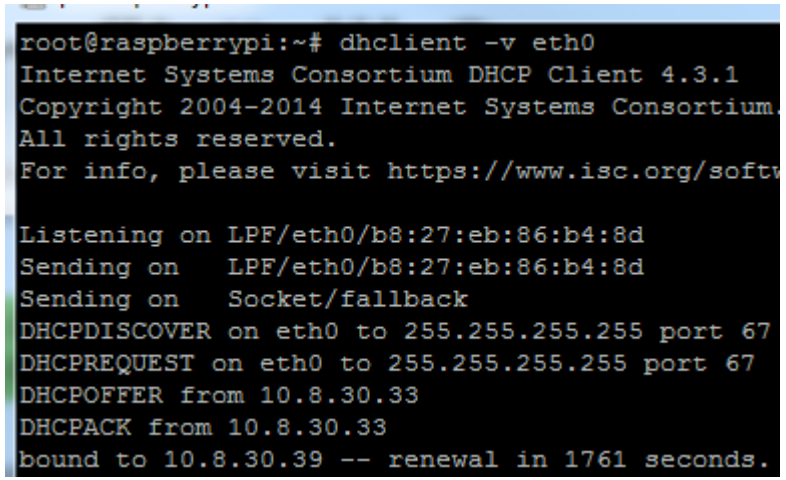


Hibakeresés során látható, hogy a DHCP kérés továbbításra kerül, de válasz nincs. Vannak viszont fura option 82-re utaló üzenetek. Tudjuk, hogy egy Cisco router a DHCP szerver és azt, hogy alapértelmezetten nem kezeli az option 82-t. Érdemes megnézni, alapbeállításban a switch használja-e?

Az ellenőrzés alapján igen! Ki kell kapcsolni tehát.

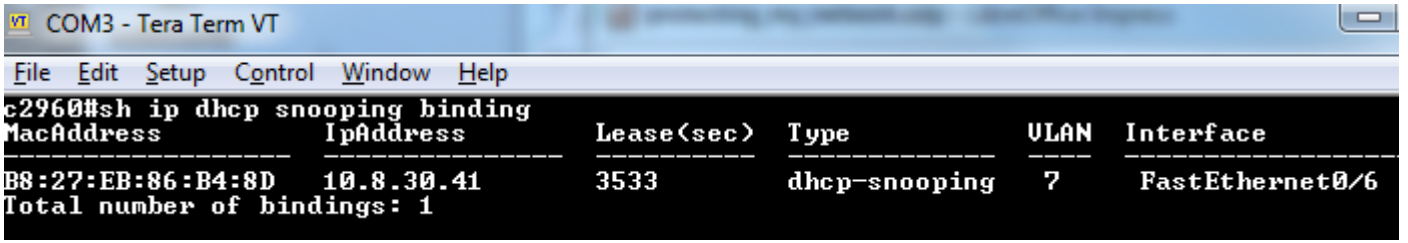
Hibakeresés (2)





Az option 82-re nekünk most nincs szükségünk, kikapcsolás után máris látható, hogy a kérésre megérkezik a válasz, a tartalom bekerül a helyi táblázatba, majd a switch továbbítja a végpontnak.

Fun fact! Néha előfordul, hogy DHCP mellett szeretnénk fix IP címeket kiosztani. Ezzel semmi gond nincs. Gond akkor van, ha a fix IP címet helyszínhez akarjuk kötni és nem végponthoz. Normális esetben az IP címet MAC címhez foglalja az ember. De például azt akarod, hogy egy teremben egy végponton mindegy mi van, de mindig ugyanazt az IP címet kapja? Ha egy gép elromlik és kicseréled, de nem akarsz bajlódni az IP cím foglalással. A Cisco eszközökben van erre megoldás, a neve **DHCP Port-Based Allocation**. Ilyenkor a switch gondoskodik arról, hogy a DHCP szerver mindig ugyanazt az azonosítót lássa, amihez egyszer IP lett rendelve, ez pedig a switchport lesz.



Smart Vision Solutions
taking you one step ahead

DAI – Dynamic ARP Inspection

Megnéztük, hogyan kell a végponton egy biztonságos határvonalat kiépíteni, mint egy képzeletbeli kerítést egy határon.

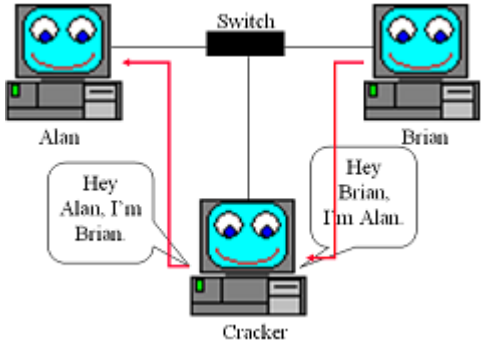
Hmm, kísértetiesen hasonlít a mi határvédelmünk a 2016 nyarán zajlott eseményekre... csak mi a hálózatokban ezt nem néhány évente és nem néhány százezer ember ellen építjük, hanem naponta néhány millió kéretlen látogató ellen védekezünk. Ráadásul, ellentétben a valósággal, a mi kéretlen látogatóink kártékony szándékkal akarnak behatolni a védvonalon belülre.

A port security, a VMPS, a 802.1x és a DHCP snooping teljesen jó akkor, ha határvédelmet építünk.

De mi a teendőnk akkor, ha eleve bent lévő gonosz emberek akarnak zavart okozni a hálózatunkban, például MitM (Man-in-the-Middle) támadásokkal? A DHCP snooping bevezetésénél láttuk, miért akar valaki DHCP szerver lenni. Mi van akkor, ha valaki nem DHCP szerver akar lenni, csak szimplán elterelni a forgalmat azzal, hogy megszemélyesít más gépeket a hálózaton?

A megoldás a DAI.

DAI (2)



Az ARP Spoofing Attack lényege, hogy az ARP (IP-MAC összerendelést támogató protokoll) működésében az azonosítás hiányát használjuk ki. Amikor “A” beszélni akar “B”-vel, de nem tudja a MAC címét, megkérdezi. Mindenkitől. Ha “C” úgy dönt, hogy válaszol “B” helyett, akkor “A” azt fogja hinni, hogy “B”-vel beszélget. A DAI erre kínál megoldást.

- A DAI csak LAN Base licensz mellett használható, LAN Lite nem támogatja
- A 2960-as switch itt mellettem csak Lan Lite, így egy másik switchre térünk most át: Cisco 3560
- A 3560-as swich elő lett konfigurálva, ott tartunk rajta, ahova eddig eljutottunk

- A Dynamic ARP Inspection a DHCP Snooping funkcióra épül, használja a már megismert snoop binding táblázatot
- A switch minden beérkező **válasz**keretet megvizsgál: a feladó MAC/IP pár az-e, mint aminek lennie kell
- Minek kell lennie? Annak, amit az adott végpont a DHCP szervertől kapott
- Amennyiben a beérkező keret más MAC / IP párral bír, a switch a forgalmat eldobja
- Ezen túlmenően a switch limitálni fogja, hogy mennyi ARP forgalom érkezhet egy portról. Ez amolyan 2for1 dolog.

- Implementáljuk akkor ezt: a DHCP Snooping már megvolt
- Jelöljük ki a megbízható portokat, ahol nem kell semmit eldobni (uplink)

192.168.25.196 - PuTTY

```
c3560#show ip arp inspection interfaces

 Interface        Trust State     Rate (pps)     Burst Interval
 ---------------  -----------     ----------     --------------
 Fa0/1            Untrusted               15                  1
 Fa0/2            Untrusted               15                  1
 Fa0/3            Untrusted               15                  1
 Fa0/4            Untrusted               15                  1
 Fa0/5            Untrusted               15                  1
 Fa0/6            Untrusted               15                  1
 Fa0/7            Untrusted               15                  1
 Fa0/8            Trusted                 None              N/A
 Gi0/1            Untrusted               15                  1
```

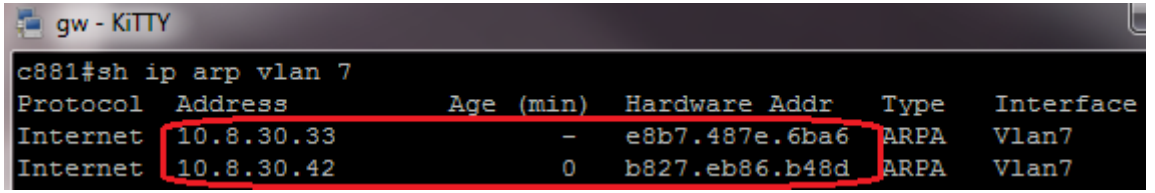
192.168.25.196 - PuTTY

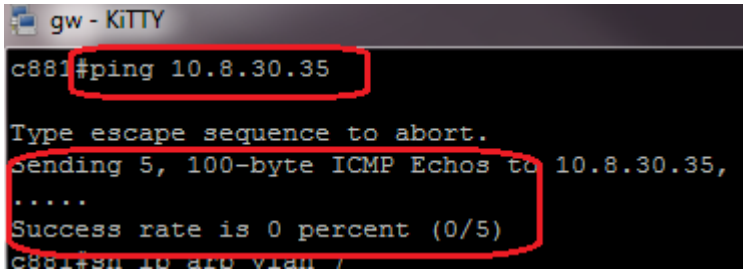
```
c3560#conf t
Enter configuration commands, one per line.
c3560(config)#interface fastethernet 0/8
c3560(config-if)#ip arp inspection trust
c3560(config-if)#exit
c3560(config)#ip arp inspection vlan 7
c3560(config)#end
c3560#
```

Smart Vision Solutions
taking you one step ahead

DAI (3)

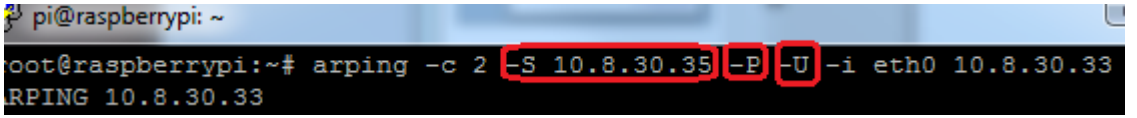
Nézzük meg, DAI nélkül hogyan lehet becsapni mindenkit a hálózaton. Kezdetben egy másik host a subneten csak két élő IP címet lát: magát (33) és a pi-t (42). Mindkettőhöz van MAC cím is.

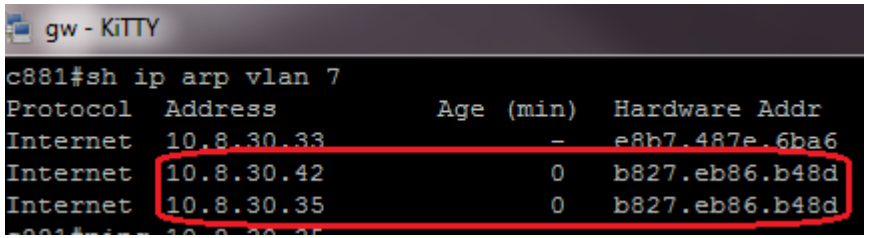




Egy véletlenül választott cím (35) nem elérhető, senkié, az ARP kérések (milyen MAC címé a 35-ös IP?) megválaszolatlan marad.

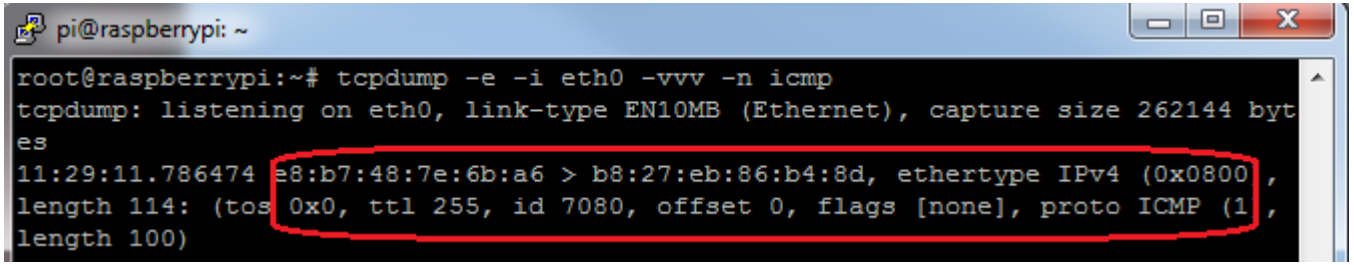
Küldjünk egy hamisított ARP választ, amiben meghirdetjük a saját MAC címünk mellé a keresett IP címet.





Voilá, mások ARP táblája szerint az IP cím már a miénk, innentől ha erre a címre forgalmat küldenek, nálunk landol majd, az eredeti címzett helyett.

A másik gép hamis információval megfertőzött ARP cache miatt nekünk küldi az információt.



DAI (4)

```
c3560#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
c3560(config)#int fastethernet 0/8
c3560(config-if)#ip arp inspection trust
c3560(config-if)#exi
c3560(config)#ip arp inspection vlan 7
c3560(config)#end
c3560#
```

Kapcsoljuk be a DAI-t és nézzük meg, mi történik!

Látható, hogy az áldozat ARP cache-e nem módosul, nem kapja meg a támadó ARP kereteit. A switch pedig jelzi, hogy melyik VLAN, melyik port és melyik MAC cím támad.

192.168.25.200 - KiTTY

```
root@raspberrypi:~# arping -c 2 -P -U 10.8.30.33 -i eth0
ARPING 10.8.30.33
Timeout
Timeout

--- 10.8.30.33 statistics ---
2 packets transmitted, 0 packets received, 100% unanswered
```

gw - KiTTY

```
c881#sh ip arp vlan 7
Protocol  Address          Age (min)  Hardware Addr
Internet  10.8.30.33             -   e8b7.487e.6ba6
Internet  10.8.30.42             0   b827.eb86.b48d
c881#sh ip arp vlan 7
Protocol  Address          Age (min)  Hardware Addr
Internet  10.8.30.33             -   e8b7.487e.6ba6
Internet  10.8.30.42             0   b827.eb86.b48d
c881#
```

192.168.25.217 - PuTTY

```
c3560#show ip arp inspection stat vlan 7

 Vlan      Forwarded        Dropped      DHC
 ----      ---------        -------      ---
    7             15              2

 Vlan   DHCP Permits    ACL Permits  Probe
 ----   ------------    -----------  -----
    7              7              0
```

192.168.25.217 - PuTTY

```
Dec 18 11:34:11.839: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/6
, vlan 7.([b827.eb86.b48d/10.8.30.35/ffff.ffff.ffff/10.8.30.33/11:34:11 GMT Sun
Dec 18 2016])
Dec 18 11:34:12.845: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/6
, vlan 7.([b827.eb86.b48d/10.8.30.35/ffff.ffff.ffff/10.8.30.33/11:34:12 GMT Sun
Dec 18 2016])
```

Majdnem jók vagyunk

- Van egy remek határvédelmünk
  - Be tudjuk engedni csak a megbízható MAC címeket
  - Hozzá tudjuk rendelni az idegen MAC címeket egy vendég hálózathoz
  - Sőt, mindezt emberekre is meg tudjuk csinálni, nem csak gépekre
  - Ki tudjuk szűrni az idegen DHCP szervereket, hogy ne okozzanak zavart

- Van védelmünk azok ellen, akik már bent vannak és ARP spoofing attack-ot próbálnak végrehajtani
- Egy dolog hiányzik: nem tudjuk az embereket kötelezni arra, hogy ne használjanak statikusan beállított IP címet, csak a DHCP által kiosztottat.

Miért akarnánk, hogy mindenki DHCP-t használjon?

- Láttuk, hogy korábbi protokollok esetén a végpontot VLANok között dobáljuk, ilyenkor ha nem használ DHCP-t, hiába minden
- Bár az ARP támadásokat már ki tudjuk védeni, de szeretnénk ugyanezt IP rétegben is megtenni
- A DAI csak az ARP válaszokat szűri ki. Ha nincs ARP válasz, csak beállítok magamnak egy statikus IP címet, attól még küldhetek csomagokat és azok célba fognak érkezni
- Válasz ugyan nem lesz, de küldeni tudni fog a támadó gép.

Miért baj, ha tud küldeni a gép, ha fogadni úgysem tud? A baj ezzel az, hogy **nem csak úgy** lehet zavart okozni a hálózatban, **hogy közben neki működjön** a hálózata. Zavart lehet okozni csak azzal is, hogy elárasztom a hálózatot hamisított IP címekről érkező forgalommal (Denial of Service, DoS). Sőt, ilyen esetekben a támadónak külön **hasznos** is, hogy **semmi forgalmat nem fog visszakapni**. Ha visszajutna hozzá a válasz, **saját magát** DoS támadná!

IP Source Guard

- Az IPSG feladata, hogy minden olyan forgalmat eldobjon, amely olyan MAC – IP cím párról indult, amely nem szerepel a DHCP snooping táblázatban
- Ha tehát az IP címet DHCP-n keresztül kaptad, minden oké, de ha csak beállítottál egyet, a switch eldobálja a forgalmad, amíg az IP címed nem DHCP-n keresztül szerzed meg
- Az IPSG demonstrálásához a raspberry pi fog statikus IP címet választani magának, DHCP után
- IPSG nélkül látható, hogy simán adhatok bármilyen statikus IP-t magamnak és működik a ping

```
c3560#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type
------------------  ---------------  ----------  -------------
----------
B8:27:EB:86:B4:8D   10.8.30.39       2975        dhcp-snooping
net0/6
Total number of bindings: 1
```

```
root@raspberrypi:~# dhclient -d eth0
Internet Systems Consortium DHCP Client 4.3.1
Copyright 2004-2014 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/b8:27:eb:86:b4:8d
Sending on   LPF/eth0/b8:27:eb:86:b4:8d
Sending on   Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 10.8.30.33
bound to 10.8.30.39 -- renewal in 1658 seconds.
^C
root@raspberrypi:~# ping -q -c 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 40.755/40.755/40.755/0.000 ms
root@raspberrypi:~# ip addr del 10.8.30.39/27 dev eth0
root@raspberrypi:~# ifconfig eth0 10.8.30.38 netmask 255.255.
root@raspberrypi:~# route add default gw 10.8.30.33 dev eth0
root@raspberrypi:~# ping -q -c 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 40.545/40.545/40.545/0.000 ms
```

Ha lenne még DAI beállítva, a ping kérésekre **nem érkezne válasz**, de maguk **a kérések eljutnának** a címzetthez. Ha nem egyet küldenék, hanem **egymilliót** és nem egy hamis címről, hanem **százról**, hiába nem kapok választ, a hálózatot és a címzettet **leterhelném**. Nem az számít tehát, hogy **kapok-e választ**, a támadót ez nem értekli. Sőt, neki **jobb is, hogy nem kap választ**, mert így **nem kell feldolgoznia** százszor egymillió ICMP választ!

IP Source Guard (2)

- A beállítás egyetlen parancs, majd elkezdünk pingelni a pi-ről
- Nem működik
- Visszaállítjuk statikusan az eredeti, DHCP-től kapott címet
- A ping azonnal működik
- Mi történik a switchen? Hogyan diagnosztizáljuk a problémát, ha valaki szerint “nem megy az internet”?
- Nincs egyértelmű parancs rá, csak következtetni lehet

Történik egyátalán csomagvesztés a switchen folyamatos pingelés mellett?

```
c3560#show interfaces fastEthernet 0/6 | i put rate
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
c3560#
```

E szerint a forgalom nem is jön a végpontról. De valóban nem?

```
c3560#show interfaces counters | i Port|0/6
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Fa0/6             176606           1476            123             11
Port           OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
Fa0/6             137756            100           1636              1
c3560#show interfaces counters | i Port|0/6
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Fa0/6             176912           1479            123             11
Port           OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
Fa0/6             137884            100           1638              1
```

Rendben, dobáljuk a forgalmat... de vajon ez hiba?

```
c3560#show interfaces fastEthernet 0/6 | i error
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 output errors, 0 collisions, 1 interface resets
```

Foglaljuk össze:
- Látunk forgalmat bejönni
- A switch interfész dobja el
- De nem hiba miatt

192.168.25.196 - PuTTY

```
c3560#conf t
Enter configuration commands, one per line.  En
c3560(config)#int fa 0/6
c3560(config-if)#ip verify source
c3560(config-if)#end
c3560#debug ip verify source packet
Ip source guard debug packet debugging is on
c3560#
```

192.168.25.200 - KiTTY

```
root@raspberrypi:~# ping -c 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, t

root@raspberrypi:~# ip addr del 10.8.30.38/27 dev eth0
root@raspberrypi:~# ifconfig eth0 10.8.30.39 netmask 2
root@raspberrypi:~# route add default gw 10.8.30.33 de
root@raspberrypi:~# ping -q -c 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, tim
rtt min/avg/max/mdev = 41.314/41.314/41.314/0.000 ms
```

Ezek alapján már alapos ok van feltételezni, hogy nem hiba ami történik, hanem normális működés. De vajon minek a normális működése?

Smart Vision Solutions
taking you one step ahead

IP Source Guard (3)

```
c3560#show interfaces fastEthernet 0/6 | i put rate
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
c3560#

c3560#show interfaces counters | i Port|0/6
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Fa0/6             176606           1476            123             11
Port           OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
Fa0/6             137756            100           1636              1
c3560#show interfaces counters | i Port|0/6
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Fa0/6             176912           1479            123             11
Port           OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
Fa0/6             137884            100           1638              1
```

Megfigyeltük a befelé érkező forgalom számlálóit. Ez volt a sárgával jelölt számérték. Időzzünk még el egy kicsit ennél a táblázatnál, értsük meg teljesen az adatokat!

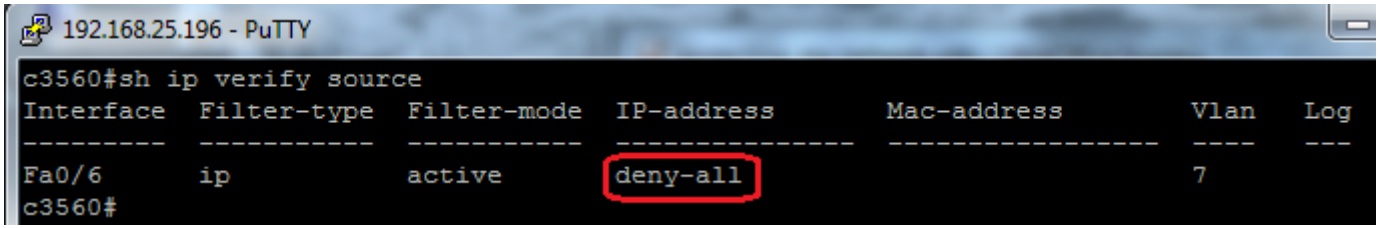
Miért nő a kifele byte, de a kifele packet nem?
A pirossal jelzett számoknál a byte számláló nő, mert a switch folyamatosan feszítőfa-protokoll kereteket küld ki minden porton, ezen is (BPDU). Ez alkalmanként kb. 43 byte. Ez viszont nem Unicast, hanem Multicast. Onnan tudni, hogy semmi más nem működik, hogy a byte out forgalom nő, a multicast out counter nő (kék), de az unicast out stagnál. Ez egyértelmű jel arra, hogy a porton semmilyen “értelmes” forgalom nem zajlik, csak háttérzaj: STP.

Mire jutottunk akkor? Rakjuk össze az információmorzsákat:

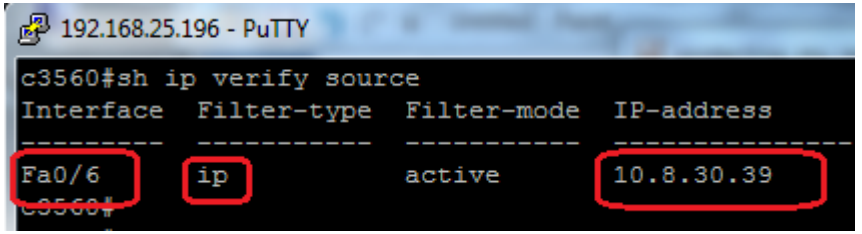
- Kaptunk tehát egy hibajelzést, hogy nem működik egy végponton a hálózat
- Miközben folyamatosan generáltattunk forgalmat (pl. ping -t gateway) látszik, hogy **a switch dobja** el a forgalmat
- De azt is tudjuk, hogy a dobálás **nem hiba miatt** történik
- Sőt, az is látszik, hogy kifele **normálisan küld a switch STP** kereteket
- És azt is tudjuk, hogy **csak STP megy ki**, semmi más, tehát a végpont nem kap semmi igazi forgalmat
- Ezekből a lehetséges “gyanúsítottakat” le lehet szűkíteni pusztán egy pár jelöltre
- például: ACL (filter), IP Source Guard, rossz VLAN beállítás stb.

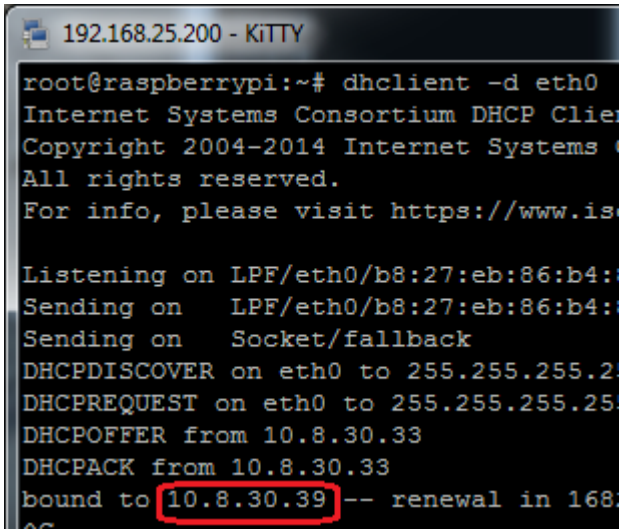
IP Source Guard (4)

Ha már az IP Source Guard a jelöltek egyike, nézzük meg, mit gondol erről a switch:



Hogyan kellene ennek kinéznie, ha az illető nem statikus IP címet használna?





Ez az a pont, ahol a végfelhasználó által adott IP, MAC adatokat összevetjük a DHCP snooping táblázattal és látjuk, hogy teljesen más van neki kiosztva. Innen pedig már egyértelmű, hogy nem hiba van.

Tanulság? Ahogy egyre bonyolultabb protokollok felé haladunk, egyre kevésbé lesz első ránézésre egyértelmű, hogy melyik irányba kell folytatni a hibakeresést. **Megfordul a helyzet a korábbi hibakeresésekhez képest.** Nincs egy show, vagy debug parancs, ami megmondja mi történik. Neked magadnak kell **elméleteket felállítanod**, tudván, hogy mi történhet a háttérben. Ezeknek a folyamatoknak a **nyomait kell kutatnod** és a talált **adatokból következtetned** valamire. Magadtól kell tudnod, hogy ha befele jön forgalom és kifele csak feszítőfa BPDU megy, az mit jelent és egyébként hogyan tudod megnézni, hogy **tényleg ez-e a helyzet**?

Örülök, hogy eljöttél meghallgatni. Kérdések?

Az oktatások tartalma, általános információk:
http://svs.cx

Piaci alapokon működünk, de törekszünk arra, hogy ingyen, vagy legalább igen nagy kedvezménnyel tartsunk további online előadásokat magyar rendszergazdáknak. A kedvezményeket biztosító kódokat a hírlevelekben fogjuk közzétenni.

Megköszönjük, ha véleményezed a munkánkat.

Ha nem tetszik ahogy csináljuk, kérlek mondd el nekünk.
Ha tetszik ahogy csináljuk, kérlek mondd el másoknak!

facebook.com/svsltduk