

# Adatkapcsolati protokollok – II.

## Konzisztencia és hozzáférés kontroll

*első rész*

2016. december 8.

# Eddigi ismereteink

- Megismertünk adatkapcsolati protokollokat:
  - VLAN
  - CDP
  - STP
  - Etherchannel
- Folytassuk olyan protokollokkal, amik a mindennapi életben is hasznosak
- Amik válaszokat adnak a fentiek megtanulása közben felmerült kérdésekre
- Konfiguráljuk is be rögtön ezeket és értsük meg, hogyan működnek
- Ma két témát járunk körbe:

- **VLAN kezelések, konzisztencia fenntartása a switchek között**
  - DTP
  - VTP

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

És amúgy ma eddig fogunk eljutni

- **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

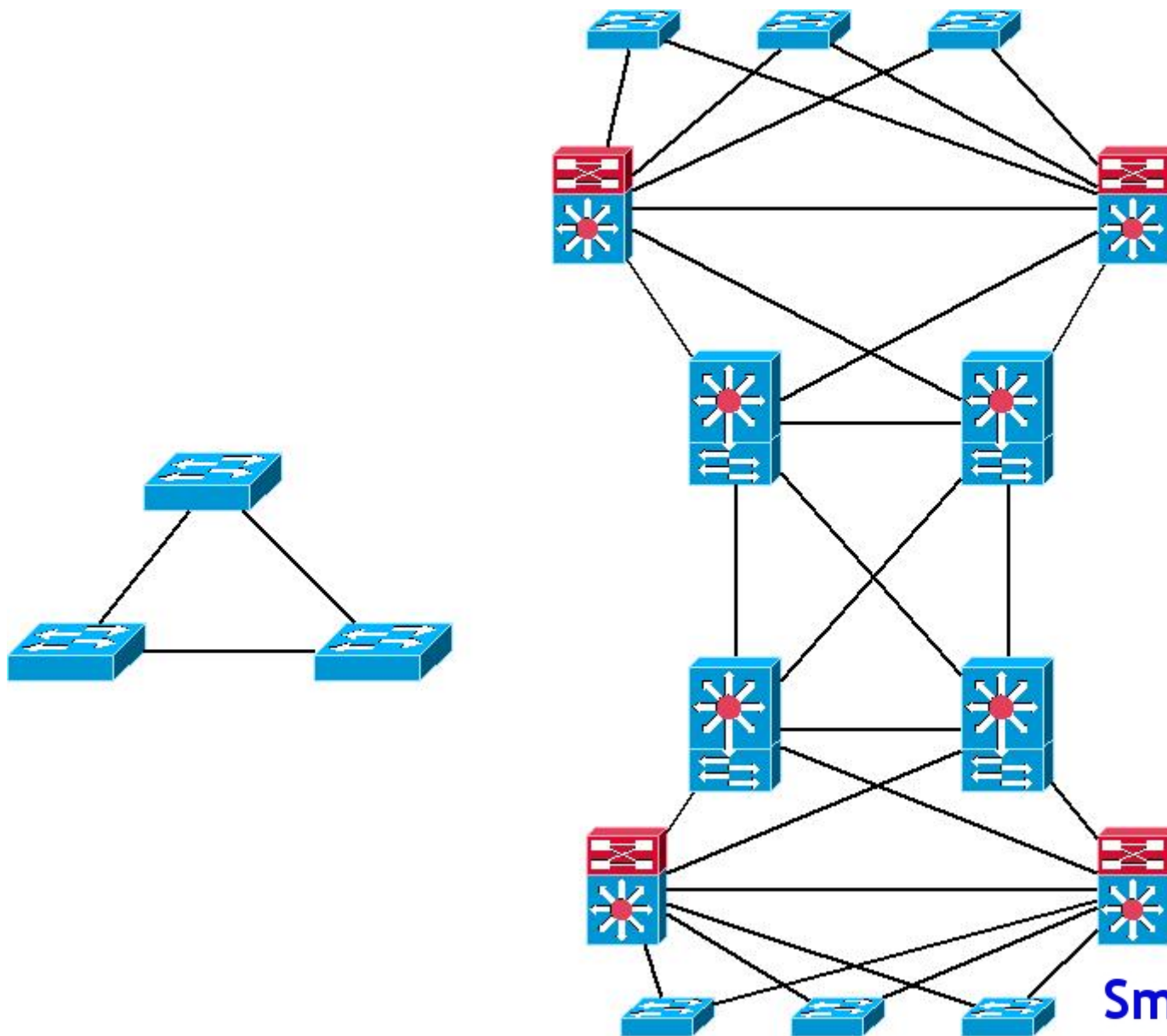
# VLAN konfigurálás, a konzisztencia fenntartása

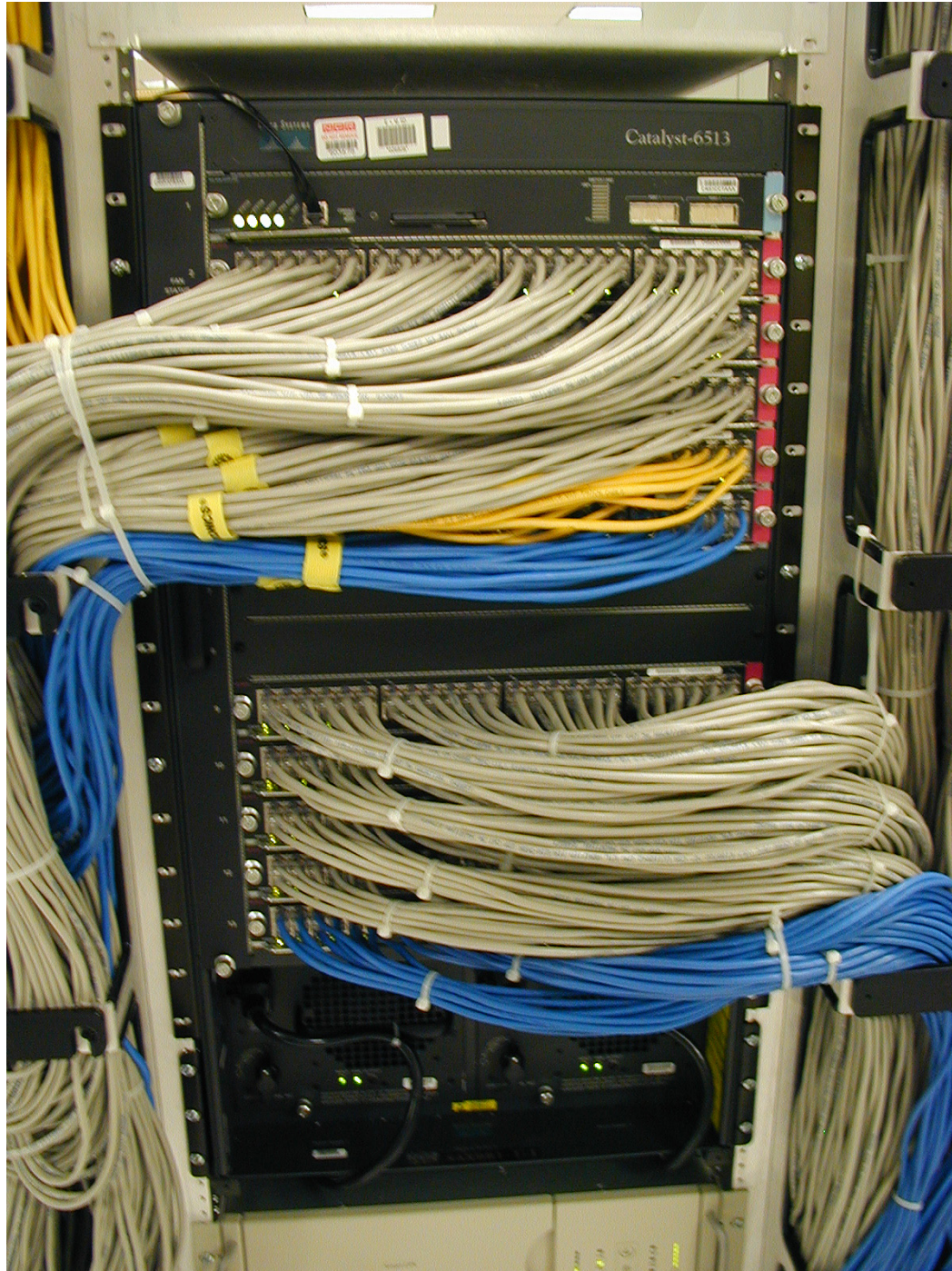
- VLAN (Emlékeztető)
  - Azonos fizikai eszközben több, logikailag elválasztott hálózat (switchport)
  - Az elválasztás adatkapcsolati rétegben történik meg
  - Switchport – vlan hozzárendelés: eddigi ismereteink szerint manuális
  - Access port – egy vlan, Trunk port: több vlan
  - Trunk port: 802.1q (vagy ISL), 4 byte TAG a keret fejlécben
  - Trunk port: taggeletlen forgalom: natív vlan
- Milyen problémáink vannak?
- VLANok konfigurálása:
  - **HE** - Minden eszközben kézzel konzisztensen kell tartani a létező vlanokat
  - **HE** - Minden trunk porton engedélyezni kell, kivéve ahol nincs értelme (pruning)
  - **SR** - Feszítőfát kell nyilvántartani, kezelni, számolni, frissíteni
  - **HE** - Trunk portokat szinkronban tartani

HE – Human Error    SR – System Resources

- Ne három, vagy öt switchben gondolkozzunk – a probléma a skálázhatóság
- Átlag Bélánál van 150 végpont és hat switch – fejben tartja
- Egy hálózati mérnöknek több tízezer végpontja, néhány ezer eszközön
- Néha nem, hogy több épületben, de több kontinensen is elszórva

# VLAN konfigurálási problémák

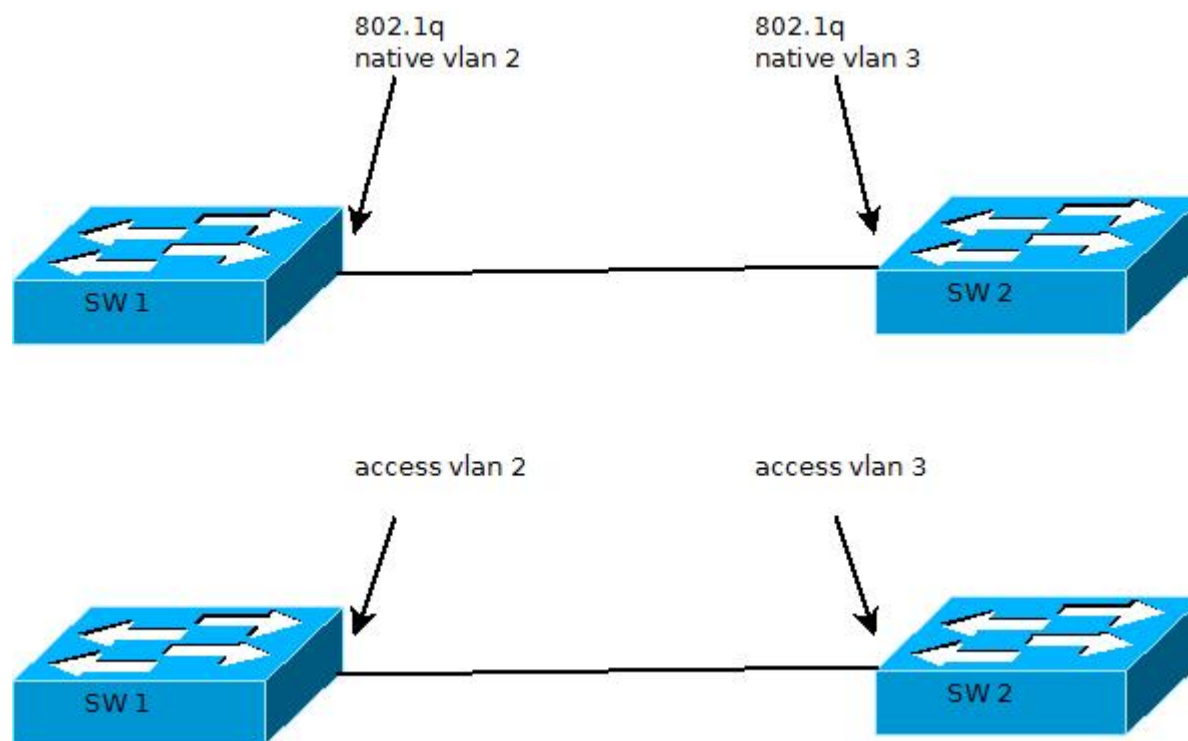




**Smart Vision Solutions**  
*taking you one step ahead*

# VLANok kezelése

- A VLANok sorszámozása ún. locally significant (csak helyben érdekes)
- Ugyanakkor a natív vlan hibás beállítása folyamatos log üzeneteket generál
- Lehet így is VLANok között kereteket mozgatni, de ez ritkán indokolt
- Vegyük észre, hogy az egyik esetben a hibát egy protokoll jelzi - DTP



# DTP – Dynamic Trunking Protocol

- Leegyszerűsítendő az életet, a Cisco switchek **általában** alapértelmezetten minden portján ún. dynamic auto beállításban vannak. Verziófüggő!
- Azaz ha azon a porton valaki trunk portot akar szemközt, akkor hadd legyen
- Ez biztonsági kockázat, valamint addicionális pár tized másodperc, mielőtt a port rendesen üzemelhetne (fel kell ismerni, a túloldal mit akarhat)
- Ez a protokoll a DTP: layer 2 kereteket küldözget és vár, hogy eldönthesse: kell-e trunk a portra?

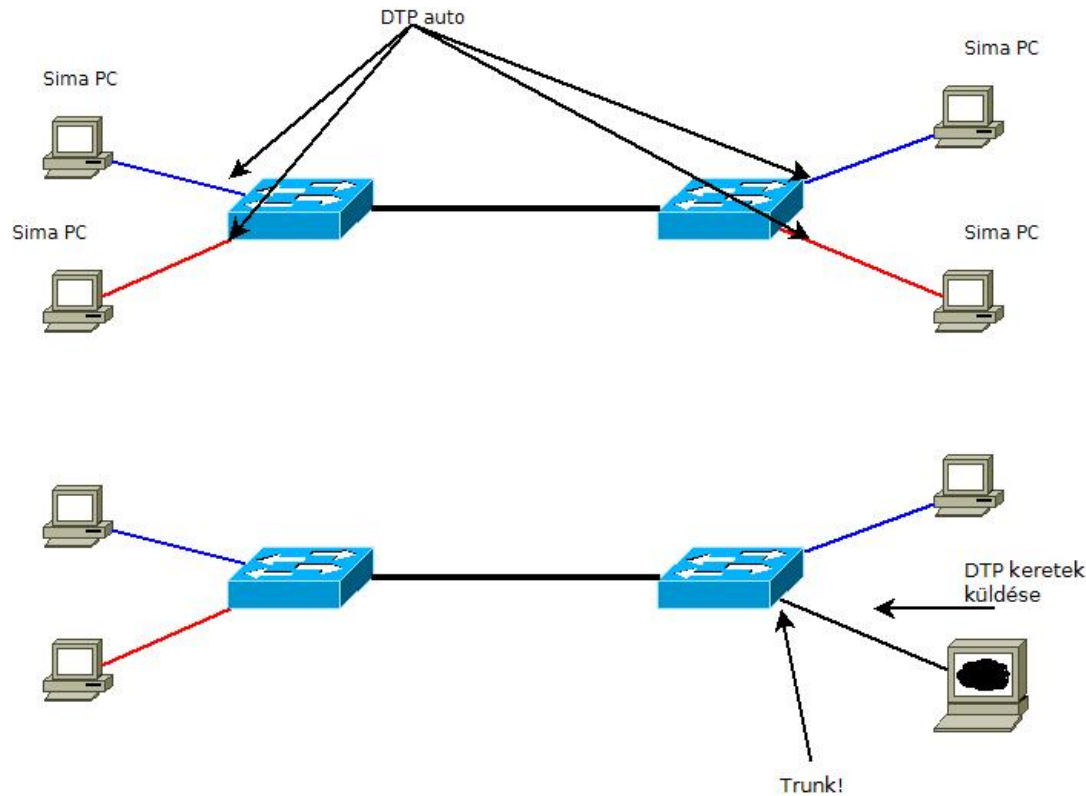
## Miért biztonsági kockázat?

Mert egy támadó a saját gépéről megfelelő DTP kereteket küldhet ki, amivel a switchet ráveheti, hogy a portot trunk módba kapcsolja.

Ezzel pedig máris hozzáfér minden VLAN forgalmához, mivel alapértelmezetten minden VLAN engedélyezett egy trunk porton.

On	Mindig trunk port lesz és folyamatosan DTP-t küld ki
Off	Soha nem lesz trunk és DTP-t küld ki erről
Desirable	Aktívan, DTP-t küldve megpróbál trunk lenni
Auto	Passzívan lehet trunk: nem hirdeti magáról, de az lesz, ha DTP-t hall
Nonegotiate	DTP lekapcsolása (de ettől még lehet trunk port is, access is)

# A DTP, mint biztonsági rés



Amíg egy port access port, csak egy vlan forgalma mehet rajta

Megkülönböztetünk statikus és dinamikus access portokat, de ettől még csak egy vlan megy rajta.

Amint trunk port lesz, több is, konfiguráció szabályozza, mely vlanok.

A PC, amelyik DTP-t küld, ezetül megkaphatja bármelyik, switchen engedélyezett vlan forgalmát.

A két vlan között akár átjáróként is működhet.



# A DTP jeletősége

Amennyiben egy switchport lehet trunk, akkor erről többnyire egyezkedni is tud. Miről kell egyezkedni?

- Egyáltalán legyen-e trunk vagy sem
- Ha legyen, akkor milyen protokoll szerint (802.1q, ISL, egyéb)

Mit könnyít meg? Switch – switch kapcsolatok beállítását:

- hibamentesen (konzisztencia)
- gyorsan (nem kell konfigurálni, csak bedugod)
- egyszerűen (ugyancsak)

Mit nem tud? Nincs benne autentikáció ==> bárki, egy PC is küldhet DTP kereteket

Megoldás: switchport nonegotiate minden trunk portra, ami pedig nem kell trunk legyen, ne legyen az.

Minta: egy 2940 és 2960, konfigurálatlan switch szembekötve:

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Switch#sh int status | i 0/2
Fa0/2 connected trunk
Switch#sh interface fast 0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

```
192.168.25.217 - KITTY
Switch#sh int status | i 0/2
Fa0/2 connected trunk
Switch#sh int fas 0/2 sw
Switch#sh int fas 0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

# VTP – VLAN Trunking Protocol

- Sokkal mókásabb protokoll, mivel sokkal nagyobb hibákat lehet vele okozni
- Egyenesen katasztrófálisakat is, rendkívül egyszerűen
- A VTP Cisco eszközökben alapértelmezetten bekapcsolt – kell a VLANokhoz
- Eredetileg a konzisztens VLAN menedzsmentre találták ki
- A VTP Cisco-specifikus protokoll
- Feladata, hogy automatikusan elterjessze a VLAN konfigurációt a hálózati eszközökben anélkül, hogy azt mindenhol be kellene konfigurálni

## A VTP létjogosultsága:

100 VLAN konfigurálása 100 eszközben, ha egy VLAN konfigurálása tíz másodpercig tart, akkor  $100 \text{ vlan} \times 100 \text{ eszköz} \times 10 \text{ mp} = 100\,000 \text{ mp} = 27 \text{ óra} = \mathbf{3.5 \text{ munkanap}}$  valakinek

VTP esetén egy helyen konfigurálunk, azaz  $100 \text{ vlan} \times 10 \text{ mp} \times 1 = \mathbf{17 \text{ perc}}$  alatt megvagyunk

Client	Lokális konfiguráció nincs, VTP domainen belül szervertől tanul
Server	Lokális konfiguráció, az eredményt a kliensek tanulják domainben
Transparent	Lokális konfiguráció, VTP kereteket átpasszolja magán

# VTP

- Gyári, üres konfigurációból indulunk, hogy megfigyeljük az alapértelmezett beállításokat is
- A VTP működéséhez szükséges, hogy működő trunk portok legyenek az eszközök között
- Az alapértelmezett beállításokhoz újra is indítjuk mindkét switchet, a vlan adatbázis nélkül

```
192.168.25.217 - PuTTY
c2940#sh vtp status
VTP Version           : 2
Configuration Revision : 0
Maximum VLANs supported locally : 16
Number of existing VLANs : 5
VTP Operating Mode    : Server
VTP Domain Name      :
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MD5 digest           : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960#show vtp status
VTP Version capable   : 1 to 3
VTP version running   : 1
VTP Domain Name      :
VTP pruning mode     : Disabled
VTP Traps Generation : Disabled
Device ID            : 0026.51b3.1980
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 192.168.25.197 on interface V11 (lowest numbered VLAN interface found)

Feature VLAN:
VTP Operating Mode    : Server
Maximum VLANs supported locally : 64
Number of existing VLANs : 5
Configuration Revision : 0
MD5 digest           : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                    : 0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC
```

# VTP (2)

Látható, hogy kliens módban nem lehet VLANokat konfigurálni

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960(config)#vlan 99
VTP VLAN configuration not allowed when device is in CLIENT mode.
c2960(config)#
```

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960#debu sw-vlan vtp events
vtp events debugging is on
c2960#
*Mar 1 09:35:04.231: UTP LOG RUNTIME: Summary packet received, domain = svslab,
rev = 4, followers = 1, length 80, trunk Fa0/2
*Mar 1 09:35:04.231: UTP LOG RUNTIME: Validate TLVs : #tlvs 1, max blk size 4
*Mar 1 09:35:04.231: UTP LOG RUNTIME: Validate TLVs : #00, val 6, len 4
*Mar 1 09:35:04.231: UTP LOG RUNTIME: Summary packet rev 4 greater than domain
svslab rev 3
*Mar 1 09:35:04.231: UTP LOG RUNTIME: Domain svslab currently not in updating s
tate
*Mar 1 09:35:04.231: UTP LOG RUNTIME: pdu len 80, #tlvs 1
*Mar 1 09:35:04.231: UTP LOG RUNTIME: Subset packet received, domain = svslab,
rev = 4, seq = 1, length = 260
*Mar 1 09:35:04.256: UTP LOG RUNTIME: Transmit vtp summary, domain svslab, rev
4, followers 1, tlv blk size 8 (inc #tlv field),
MD5 digest calculated = 1C 24 51 DE 84 05 63 B8 23 89 52 31 A8 BB 8B 30
*Mar 1 09:35:04.256: UTP LOG RUNTIME: Transmit vtp summary, domain svslab, rev
4, followers 1, tlv blk size 8 (inc #tlv field),
MD5 digest calculated = 1C 24 51 DE 84 05 63 B8 23 89 52 31 A8 BB 8B 30
*Mar 1 09:35:04.256: UTP LOG RUNTIME: Summary packet received, domain = svslab,
rev = 4, followers = 1, length 80, trunk Fa0/3
*Mar 1 09:35:04.256: UTP LOG RUNTIME: Validate TLVs : #tlvs 1, max blk size 4
*Mar 1 09:35:04.256: UTP LOG RUNTIME: Validate TLVs : #00, val 6, len 4
*Mar 1 09:35:04.256: UTP LOG RUNTIME: Summary packet rev 4 equal to domain svsl
ab rev 4
*Mar 1 09:35:04.256: UTP LOG RUNTIME: Subset packet received, domain = svslab,
rev = 4, seq = 1, length = 260
```

Fa 0/2 -n érkezik a VTP információ, a négyes verziójú konfiguráció újabb, mint a hármas, elfogadjuk

A Fa 0/3 -mon is érkezik VTP, de eddigre a négyes verziójú konfigurációval már rendelkezünk. Vegyük észre, hogy a 0/3 egy STP blokkolt port és mégis érkezik üzenet!

# VTP – a megoldás problémája

Látható, hogy a switchek egymástól mindent szépen megtanulnak, az összes VLAN-t. Ezek szerint egyetlen VTP szerver switchen bármit beállítok, azonnal megtanulja a többi szerver és kliens is. **Jó ez nekünk?**

Korábbi példa: 100 switch, egyenként 100 VLAN beállítása: ha a gépelési sebességgel egy VLAN egy eszközben 10 mp, akkor szumma 3.5 napnyi munka.

**Ez jó.**

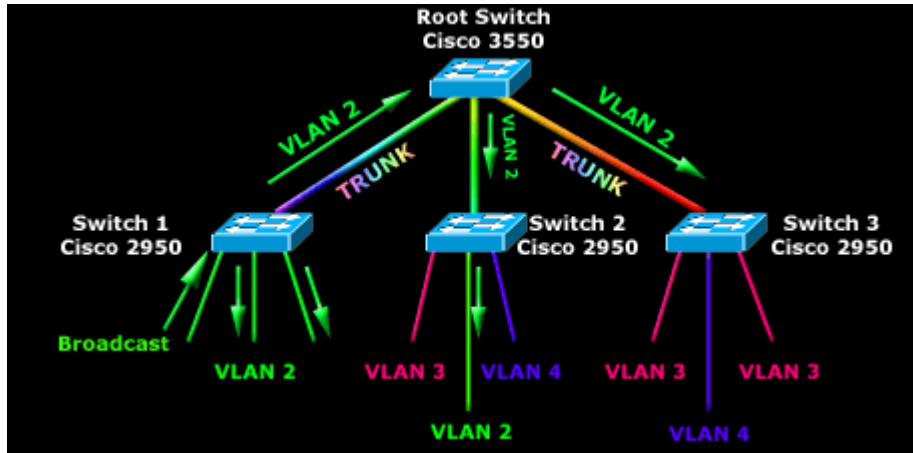
Viszont, ha nincs minden munkaállomás mindenhol jelen, azaz nincs minden VLANra minden switchben szükség, akkor minden switch 100 darab feszítőfát számol, 100 darab ARP táblát, 100 darab CAM táblát tart nyilván, interfész billenéskor legrosszabb esetben 100 VLANban egyszerre számol újra feszítőfát. Ez rendkívül erőforrás-igényes. Ráadásul, 100 VLAN-ban kiküldött 1-1 csomag minden switchen át fog menni, folyamatosan, akkor is, ha semmi értelme, mert nincs ott olyan access port, ahova ki lehetne küldeni.

**Ez rossz.**

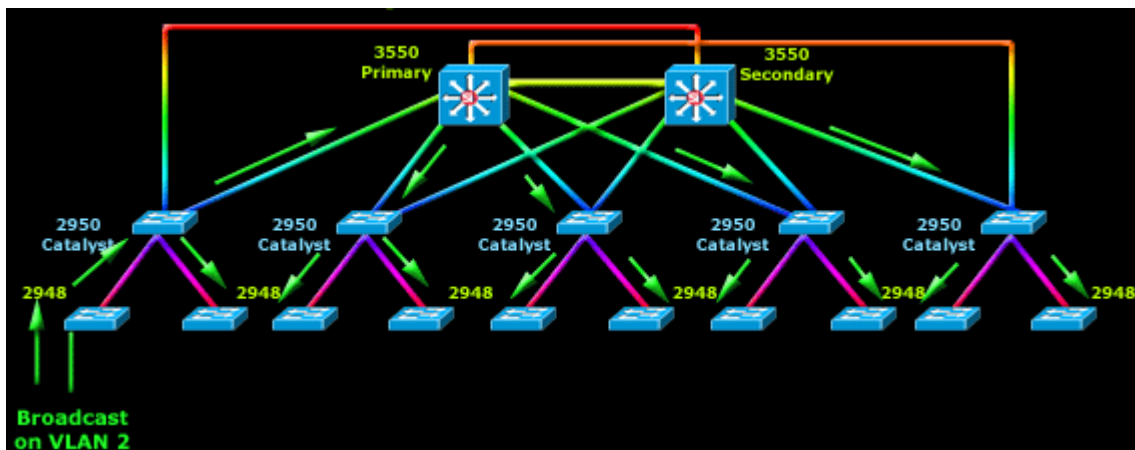
A csodálatos VTP protokoll, bár megoldja a konfiguráció konzisztencia problémáját, bevezet két problémát: egy **erőforrás** problémát és egy **kapacitás** problémát.

Ha ez zavar (pl. a switchek túlterheltek, csomagvesztés van), akkor viszont le kell mondjak a VTP-ről, ezzel megoldom ezeket. Cserébe egy rémálom lesz a VLAN konfiguráció karbantartása.

# VTP – a probléma szemléltetése



Kis hálózatokban legyintünk, nem jelentős a probléma, mondhatni csupán elvi hibás hálózatunk van, de minden működik (“belefér”).



Nagyobb, vagy egyenesen nagy hálózatokban viszont olyan jelentős túlterhelést okozhat a meggondolatlan VTP használat, ami már hasznos sávszélességet vesz el a felhasználótól.

# VTP pruning

A dolgot kézzel is lehetne kezelni, de akkor megint manuálisan kéne konfigurálni a dolgokat, a VTP-nek semmi értelme nem lenne.

- Második előadás, VLAN trunking, **switchport trunk allowed vlan** parancs!

A VTP maga is el tudja ezt intézni, hogy egy VLAN csak akkor menjen ki egy trunk porton, ha arra a túloldalon szükség van. Ez a vlan pruning.

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960#sh vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : svslab
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 0026.51b3.1980
Configuration last modified by 0.0.0.0 at 3-1-93
```

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960#show interfaces fa 0/2 switchport | i VLANs
Administrative private-vlan trunk normal VLANs: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture VLANs Allowed: ALL
c2960#
c2960#
c2960#
c2960#
```

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960#show interfaces fa0/2 trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/2     auto     802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/2     1-4094

Port      Vlans allowed and active in management domain
Fa0/2     1,13-15

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/2     1,13-15
c2960#
c2960#
c2960#
c2960#
```

A pruning lehetősége alapértelmezetten adott, de kikapcsolt

# VTP pruning (2)

Engedélyezzük a funkciót és nézzük meg, mi történik.

- A VTP elterjeszti a pruning bekapcsolását is, automatikusan beállítja a VTP kliens is
- A trunk portról lekerül minden olyan VLAN, aminek nem kell ott lennie (1-en kívül mind lekerül)

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960#show interfaces fastEthernet 0/2 trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/2     auto      802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/2     1-4094

Port      Vlans allowed and active in management domain
Fa0/2     1,13-15

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/2     1
c2960#
c2960#
c2960#
```

```
192.168.25.217 - PuTTY
c2940#show interfaces fastEthernet 0/2 trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/2     desirable 802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/2     1-4094

Port      Vlans allowed and active in management domain
Fa0/2     1,13-15

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/2     1
c2940#
c2940#
```

Egyetlen helyen, a szerveren beállítva elterjed a pruning beállítás és mostantól a switchek lebeszélnek egymással, melyik VLAN-t hova kell és hova nem kell továbbítani.

Amint megjelenik egy valós érv arra, hogy a VLAN mégis kell, meg fog jelenni. Ez az érv lehet:

- egy végpont access porton, ami up
- egy SVI valamelyik switchen, ami up



# VTP pruning (3)

```
192.168.25.217 - PuTTY
VTP PRUNING DEBUG: trunk Fa0/2 rx Join, len=166 (domain svslab)
VTP PRUNING DEBUG: trunk Fa0/3 rx Join, len=166 (domain svslab)
VTP PRUNING DEBUG: trunk Fa0/2 rx Join, len=166 (domain svslab)
VTP PRUNING INFO: T Fa0/2,V13: st Pruned ,event RxJ1=>new st Joined
VTP PRUNING INFO: trunk Fa0/3 vlan 13: J0->1 (trig Join)
VTP PRUNING INFO: trunk Fa0/3 - send trig Join
VTP PRUNING DEBUG: trunk Fa0/3 stop trig Join
VTP PRUNING DEBUG: trunk Fa0/2 rx Join, len=166 (domain svslab)
VTP PRUNING DEBUG: trunk Fa0/2 timeout
```

A debug üzenetek mutatják, hogy a szomszéd switchben van valaki a 13-mas VLANban, így mostantól küldeni kell a forgalmat a trunkon.

```
192.168.25.217 - PuTTY
c2940#sh interfaces fastEthernet 0/2 trunk | begi 13-15
Fa0/2      1,13-15
Port       Vlans in spanning tree forwarding state and not pruned
Fa0/2      1,13
c2940#
```

És valóban, látható, hogy a 2960-as switch felé már küldünk 13-mas VLANt, mert van ott valaki, akinek kell a forgalom.

```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960#show interfaces fastEthernet 0/2 trunk
Port      Mode      Encapsulation  Status      Native vla
Fa0/2     auto     802.1q         trunking    1
Port      Vlans allowed on trunk
Fa0/2     1-4094
Port      Vlans allowed and active in management domain
Fa0/2     1,13-15
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/2     1
c2960#
```

Ugyanakkor azt is látjuk, hogy a **visszafelé** irányba ez **nem történik meg**, mivel a 2940-es switch felől senki nem kérte ezt a forgalmat, így a 2960-as switch nem továbbítja. Ez normális, a **labor körülmények miatt**, a való életben ritkán van ilyen eset, hiszen a gép így **nem lát ki** a saját VLANjából. Hibakeresésnél, ha ilyen jelenség van, **ezt is vizsgálni kell!**

# Tartsd naprakészen a CV-det!

- A VTP-vel katasztrófális hibát lehet okozni, akár véletlenül, akár rossz szándékkal is.
- A VTP-ben négy fontos dolog van: domain, jelszó, a revision number és az üzemmód.
- Ezek alapértelmezetten: üres, beállítatlan, nulla és szerver.

## Mi történik, ha figyelmetlen vagy?

- Legyen két VTP szerver switchünk
- Válasszuk szét őket (mintha az egyik újként érkezne, még sosem volt a hálózatunkon)
- Az “új” switchet konfiguráljuk szanaszét
- Majd “kössük rá” a hálózatunkra. Mi történik?

```
192.168.25.217 - PuTTY
c2940#sh vlan

VLAN Name                Status    Ports
-----
1      default                active    Fa0/1,
13     svslab                  active
14     abc123                  active
15     qwerty                  active
1002   fddi-default           act/unsup
1003   transf-default         act/unsup
```

Előtte

```
192.168.25.217 - PuTTY
c2940#sh vtp status
VTP Version                : 2
Configuration Revision     : 5
Maximum VLANs supported locally : 16
Number of existing VLANs   : 8
VTP Operating Mode         : Server
VTP Domain Name            : svslab
VTP Pruning Mode           : Enabled
```

```
192.168.25.217 - PuTTY
c2940#sh vlan

VLAN Name                Status    Port
-----
1      default                active    Fa0/
2      anyu                   active
3      apu                    active
1002   fddi-default           act/unsup
```

Utána

```
192.168.25.217 - PuTTY
c2940#sh vtp status
VTP Version                : 2
Configuration Revision     : 10
Maximum VLANs supported locally : 16
Number of existing VLANs   : 7
VTP Operating Mode         : Server
VTP Domain Name            : svslab
VTP Pruning Mode           : Enabled
```

# AAA

- Authentication (Ki vagy?)
  - Authorization (Mit csinálhatsz?)
  - Accounting (Mennyit csinálhatod?)
- 
- A koncepció elsősorban hozzáféréssel és forgalmazással kapcsolatos környezetben merül fel, ahol valamit mérni és számlázni kell
  - A számlázás fontosabb magánál a szolgáltatásnál is (sokkal rosszabb, ha működik a termék de nem tudunk fizettetni érte, mintha nem működik de kiszámlázzuk)
  - Tipikus alkalmazási területek: telefónia (beszélt percek), internet-hozzáférés (forgalomszámlázás), illetve bármi ami ehhez hasonló vagy erre a gyakorlatra illik
- 
- Például telefónia esetén:
    - Authentication: Subscriber Identity Module (SIM) vagy telefonvonal (fizikai kiépítés)
    - Authorization: hívhatsz belföldi számokat, de nem hívhatsz emelt díjas számokat
    - Accounting: hatvan és fél perc, négyszáz forint lesz
- 
- Például internet-hozzáférés esetén:
    - Authentication: kaptál nevet és jelszót (PPP[oE|A]) vagy kihúzták a kábelt, vagy SIM
    - Authorization: nem torrentezhetsz, nem VoIPozhatsz, esetleg APN korlátozás
    - Accounting: nyolc gigabyte, hatezer forint lesz

# AAA (2)

A hálózati világban az AAA-t használják erre is, de hozzáférés-korlátozásra is magához a hálózati eszközökhöz, menedzsment szabályozásra

**Authentication:** név / jelszó

Célja a központosított autentikáció megvalósítása, centralizált felhasználó-menedzsment

**Authorization:** milyen parancsokat adhatsz ki (enable mode vs conf t)

Célja a központosított szabályozás, de ez opcionális

**Accounting:** milyen parancsokat adtál ki (naplózás, audit)

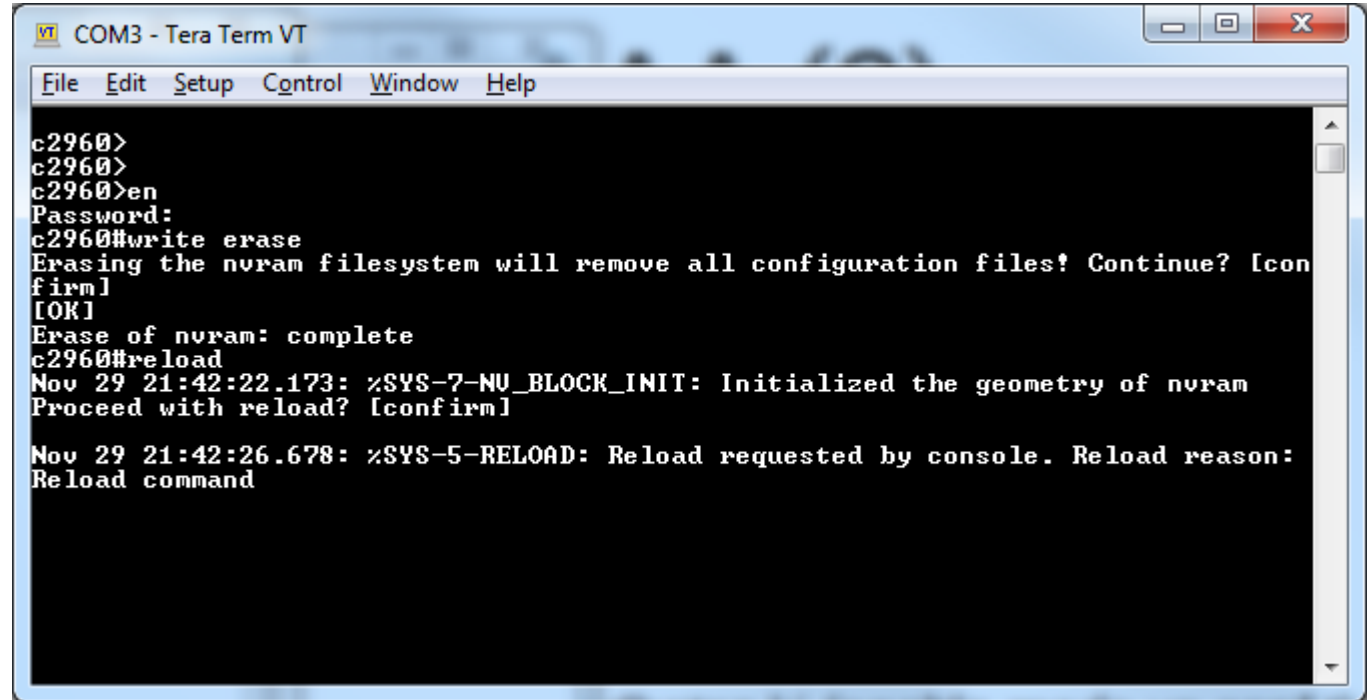
Szintén opcionális, akit nem érdekel az auditálás, nem használja

Konfiguráljuk ezt be. Hozzávalók:

- Switch (lehetőleg üres konfiggal)
- RADIUS / TACACS+ szerver (tanuljuk meg különbséget is, ha már)
  
- Példa:
- freeradius, MS IAS (Internet Authentication Server)
- CSACS (Cisco Secure Access Control Server), ISE (Identity Services Engine), CAR (Cisco Access Registrar)

# AAA (3)

Töröljük a konfigurációt,  
majd rebootoljunk,  
induljunk üres helyzetből



```
COM3 - Tera Term VT
File Edit Setup Control Window Help
c2960>
c2960>
c2960>en
Password:
c2960#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
c2960#reload
Nov 29 21:42:22.173: %SYS-7-NU_BLOCK_INIT: Initialized the geometry of nvram
Proceed with reload? [confirm]

Nov 29 21:42:26.678: %SYS-5-RELOAD: Reload requested by console. Reload reason:
Reload command
```

Majd alkalmazzunk egy  
kvázi-default konfigurációt

- enable jelszó
- lokális felhasználó, lokális jelszóval
- távoli hozzáférés (telnet, ssh)
- hostnév
- kulcsok ssh-hoz
- ssh v2 bekapcsolása
- IP cím ellenőrzése (radius-szal egy tartományból)

# AAA (4)

Radius szerver beállítása – ebben a példában Windows 2000 Advanced Server. Igen, 16 éves szoftver. Miért ez?

- az IAS komponense ugyanaz ma is, mint 16 éve
- demózunk, nem érdekel a biztonság
- erőforrás-igénytelen, HDD: 1.5 GB, RAM: 512 MB

Az IAS ma **nem cél, hanem eszköz**. A cél a RADIUS, mint protokoll megismerése és minden RADIUS szerver **egyformán** hasznos lenne ma erre. Nem az IAS konfigurációt tanulmányozzuk, hanem hálózati eszközök viselkedését **bármilyen RADIUS** szerverrel összekötve.

The image shows two screenshots from a Windows 2000 Advanced Server. The top screenshot is the 'Computer Management' console, displaying the 'Local Users and Groups' folder. The 'Users' folder is expanded, and a red box highlights the 'netadmin' and 'sysadmin' users. The bottom screenshot is a 'Command Prompt' window showing the output of the 'ipconfig' command. A red box highlights the IP address '192.168.25.197'.

Name	Full Name	Description
Administrat...		Buil
Guest		Buil
IUSR_W2KAS	Internet Guest Account	Buil
IWAM_W2K	Launch IIS Process Ac...	Buil
netadmin	netadmin	
sysadmin	sysadmin	
IsInternetU...	IsInternetUser	Thi

```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

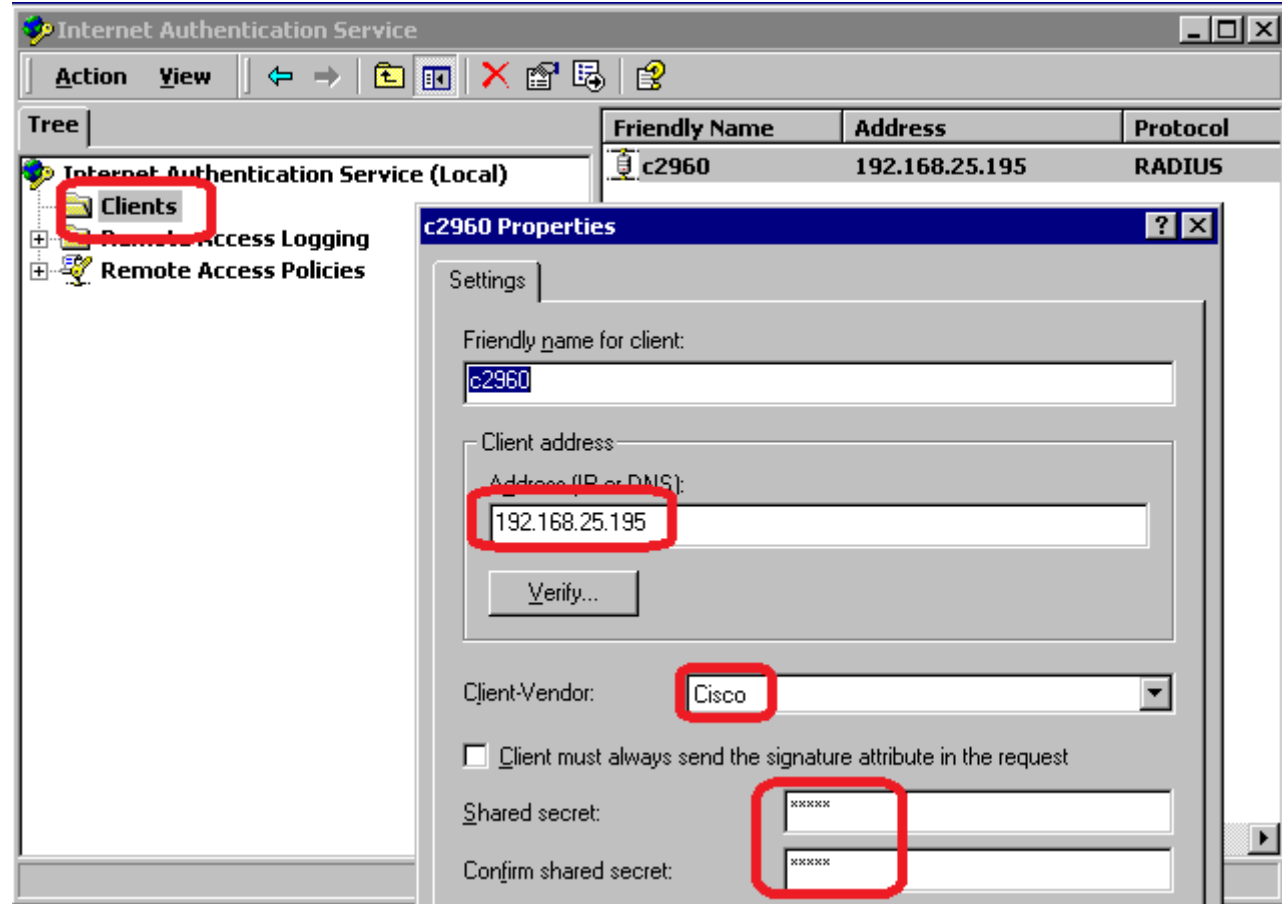
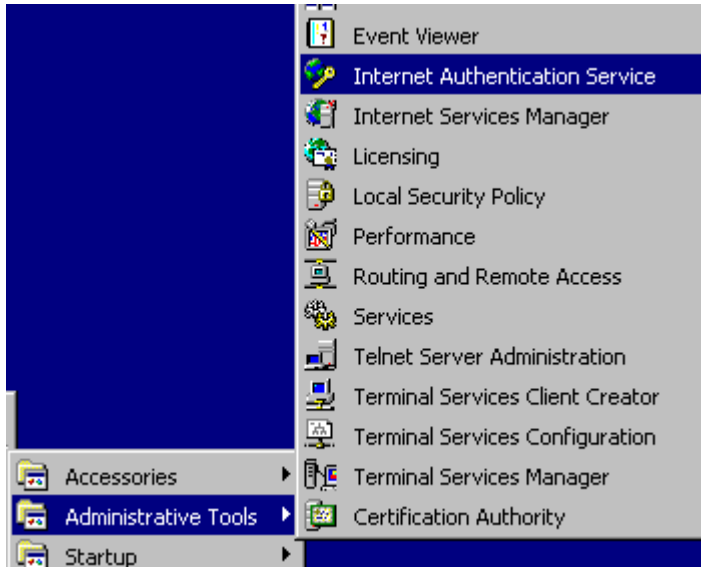
    Connection-specific DNS Suffix . : lan.hon.svs
    IP Address. . . . . : 192.168.25.197
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.25.222
```

Install után minket most csak két új felhasználó érdekel: netadmin és sysadmin. Előbbi RW, utóbbi RO (inkább ne rontson el semmit).

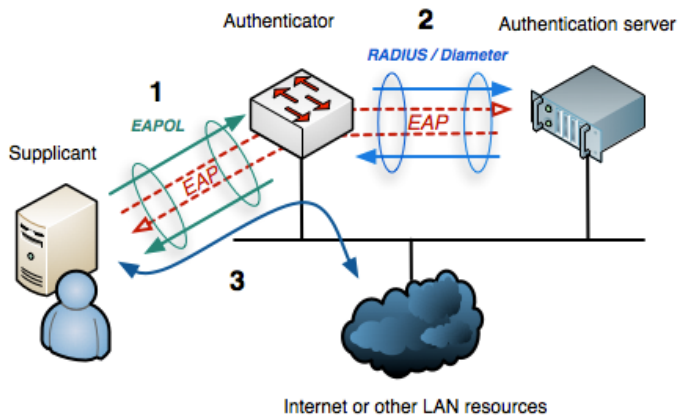
Illetve kell az IP címe is, ez itt most DHCP, mert labor, éles hálózatban nyilván statikus IP cím kell. Az IAS szolgáltatás elindul és várja a kapcsolatokat.

# AAA (5)

Új kliens létrehozása, a kliens-t RADIUS terminológiában kell érteni!



Szerver: a RADIUS szerver  
Kliens: az, aki a RADIUS szerverrel beszélget (nem a végfelhasználó), azaz a switch vagy más eszköz



```
c2960#ping 192.168.25.197
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.25.197,
!!!!
Success rate is 100 percent (5/5), round-trip min/
c2960#
```

# AAA (6)

Switch bekonfigurálása, hogy egyáltalán ismerje a RADIUS szervert

- AAA bekapcsolása általánosságban **(kizárás veszély!)**
- radius szerver IP cím **(és a saját címünk is kell!)**
- autentikáció portszám
- számlázás portszám
- opcionális paraméterek (timeout, retry)
- kulcs (secret)

Switch bekonfigurálása, hogy használja a már beállított RADIUS szervert

- Melyik "A" -t a háromból?
- létrehozunk egy metódust, amire hivatkozni fogunk
- megmondjuk, mi történjen, ha amit szeretnénk, nincs
- megmondjuk, a metódust hol fogjuk használni
- az egészet összedrótozzuk és alkalmazzuk

**aaa authentication login default group radius local**

**aaa authentication = a megfelelő A kiválasztása az AAA-ból**

**login = mikor szeretném használni**

**default = hol szeretném használni**

**group radius = mit szeretnék használni elsődlegesen**

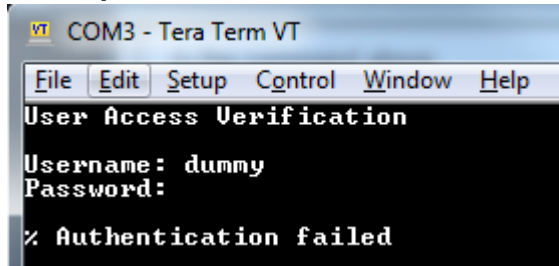
**local = mit szeretnék használni, ha az elsődleges nem működik**

Elemezzük ki, mi történne most, ha kilépnék a konzolról? Szavazatok!



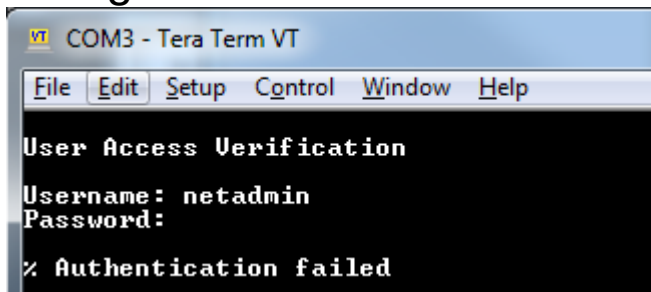
# AAA (7)

Demonstrálandó, hogy a RADIUS kapcsolat működik

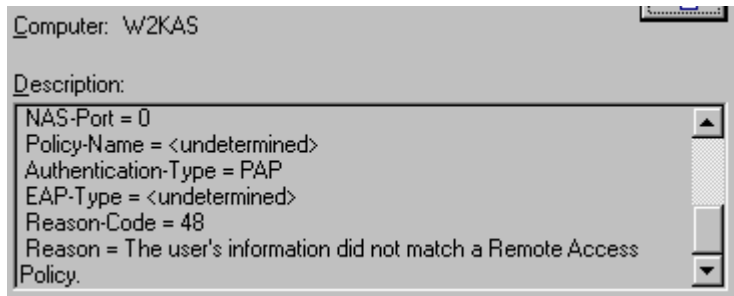


```
COM3 - Tera Term VT
File Edit Setup Control Window Help
User Access Verification
Username: dummy
Password:
% Authentication failed
```

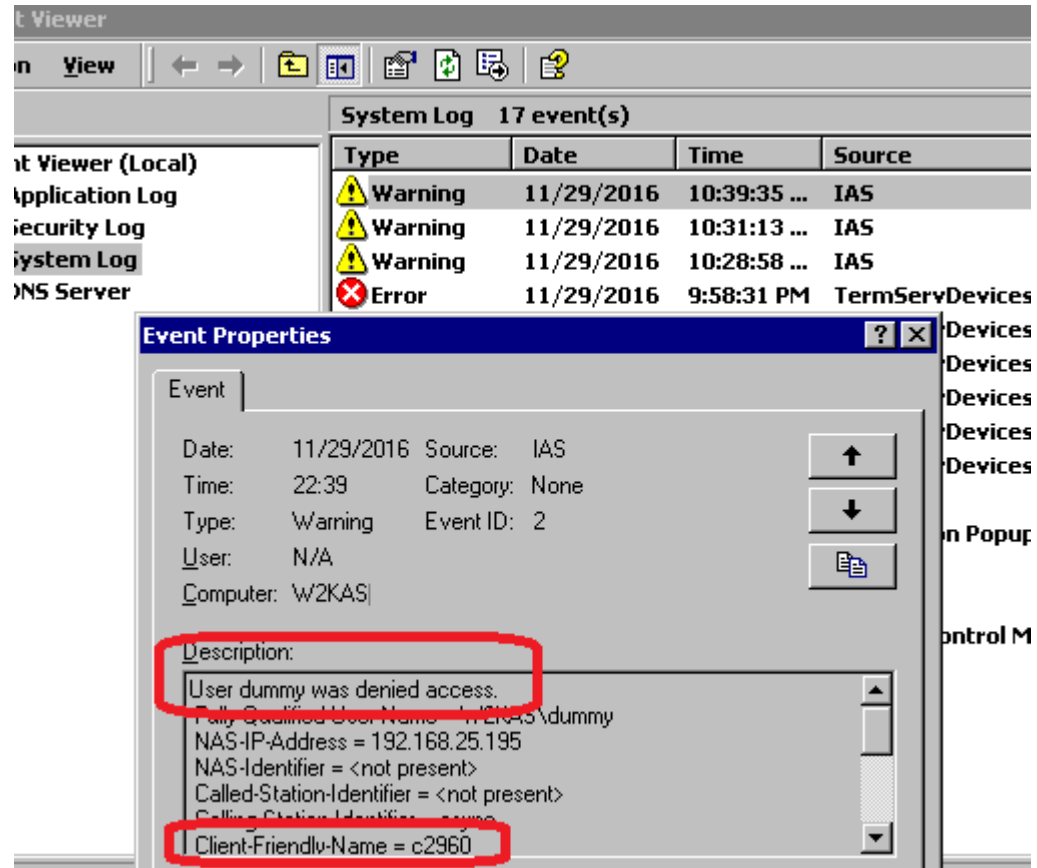
Demonstrálandó, hogy a RADIUS szervert még konfigurálni kell



```
COM3 - Tera Term VT
File Edit Setup Control Window Help
User Access Verification
Username: netadmin
Password:
% Authentication failed
```



```
Computer: W2KAS
Description:
NAS-Port = 0
Policy-Name = <undetermined>
Authentication-Type = PAP
EAP-Type = <undetermined>
Reason-Code = 48
Reason = The user's information did not match a Remote Access Policy.
```



Type	Date	Time	Source
Warning	11/29/2016	10:39:35 ...	IAS
Warning	11/29/2016	10:31:13 ...	IAS
Warning	11/29/2016	10:28:58 ...	IAS
Error	11/29/2016	9:58:31 PM	TermServDevices

Event
Date: 11/29/2016 Source: IAS
Time: 22:39 Category: None
Type: Warning Event ID: 2
User: N/A
Computer: W2KAS
Description: User dummy was denied access.
Fully Qualified User Name: W2KAS\dummy
NAS-IP-Address = 192.168.25.195
NAS-Identifier = <not present>
Called-Station-Identifier = <not present>
Calling-Station-Identifier = <not present>
Client-Friendly-Name = c2960

# AAA (8)

Miért zártuk ki magunkat?

- látható, hogy az IAS **még nincs készen**, policy problémái vannak
- de ettől függetlenül nem halott, válaszol (azt, hogy nem léphetek be)
- tehát a másodlagos metódus nem juthat érvényre, mert a RADIUS **működik!**
- az a válasz az IAS-tól, hogy nem engedélyezett, teljesen jó, nem lehet felülbírálni

Emlékeztetőül: érvényes válaszok: Access-Accept, Access-Reject

Miért fontos ezt megérteni?

- mert valószínűleg ez lesz az első hiba amit el fogsz követni
- nem árt, ha emiatt körültekintően fogsz neki
- és mindig van B terved

A B-tervek most pedig:

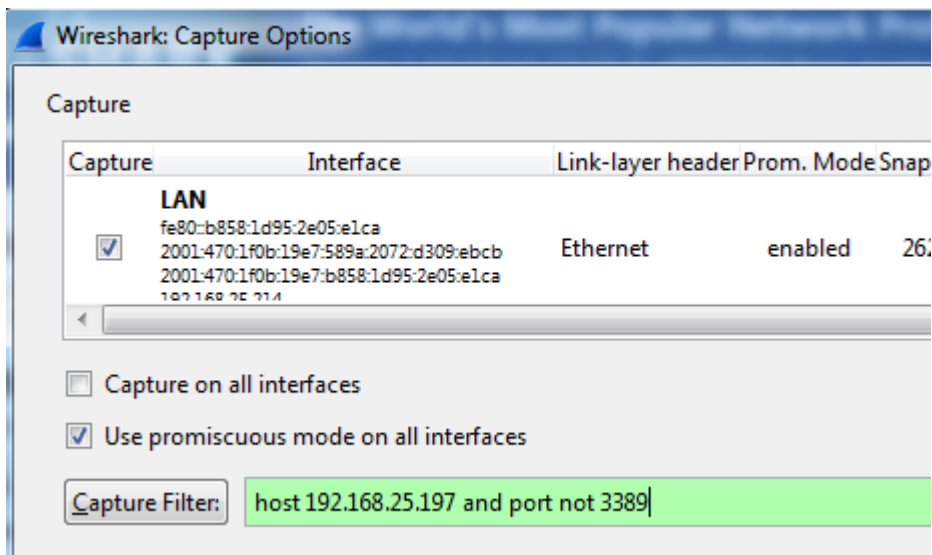
- Megjavítjuk (befejezzük) az IAS konfigurációt
- Elérhetetlenné tesszük a radius szerveret (több kliens esetén nem jó terv)
- Megváltoztatjuk a kliens kulcsát a radius szerveren
- Megváltoztatjuk a kliens IP címét a radius szerveren

Utóbbi három B-terv eredménye, hogy a radius nem fog válaszolni, tehát érvényre fog jutni a másodlagos metódus (lokális felhasználó) amit beállítottunk és bejutunk a switchbe.

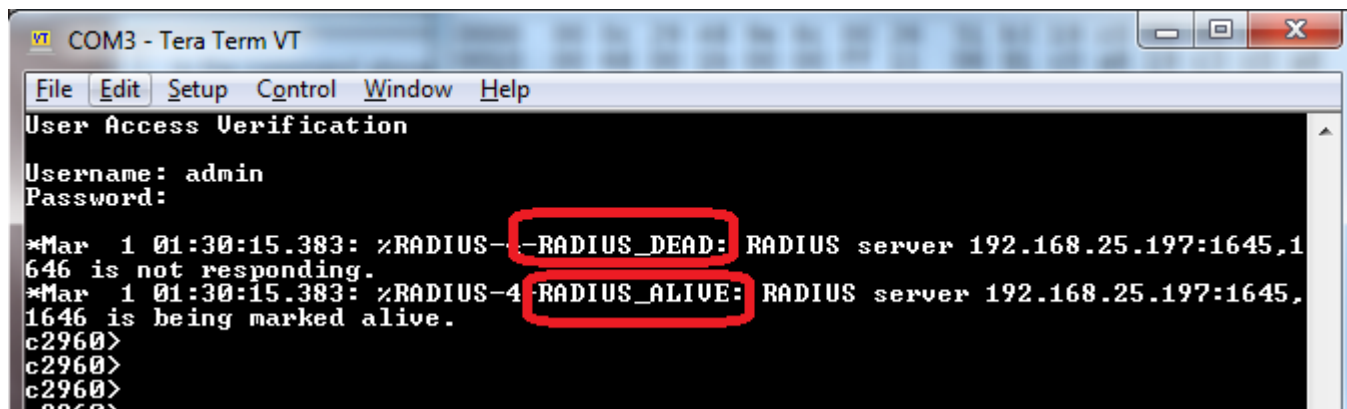
# AAA (9)

Az IP cím megváltoztatásakor az IAS már néma marad (=meghalt) tehát bejutunk, de többet kell várakozni (timeout, retry értékekre emlékezz). Igazoljuk ezt!

Wireshark a barátunk: egy konkrét IP címre vagyunk kíváncsiak, de mivel RDP-n vagyok bejelentkezve, az a forgalom csak zaj lenne az érdekes (IAS) forgalom mellett

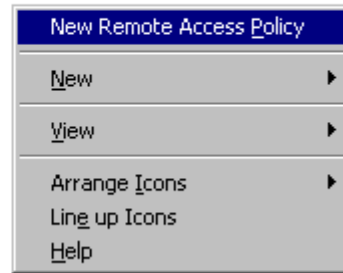


Time	Source	Destination	Info
0.000	192.168.25.195	192.168.25.197	Access-Request (1)
9.022	192.168.25.195	192.168.25.197	Access-Request (1)
18.031	192.168.25.195	192.168.25.197	Access-Request (1)
27.371	192.168.25.195	192.168.25.197	Access-Request (1)
35.93	HewlettP_cc:db:e0	Vmware_48:9e:6c	who has 192.168.25
35.93	Vmware_48:9e:6c	HewlettP_cc:db:e0	192.168.25.197 is



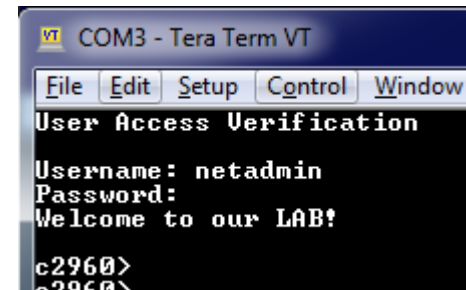
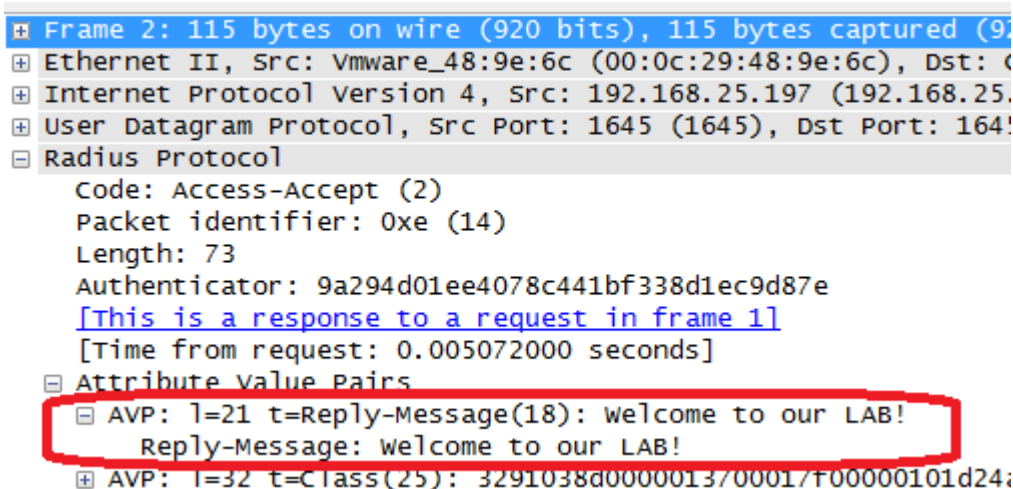
# AAA (10)

Csináljunk policy-t, hogy be tudjunk lépni és lezárhassuk a kérdést.



- Teszt: az admin felhasználó már nem tud belépni
- Ez látszik az IAS logokban is, unknown user (hisz nincs is ilyen)
- Teszt: a netadmin felhasználó viszont be tud már belépni
- Ahogy a sysadmin felhasználó is, ez mind látszik az IAS logokban

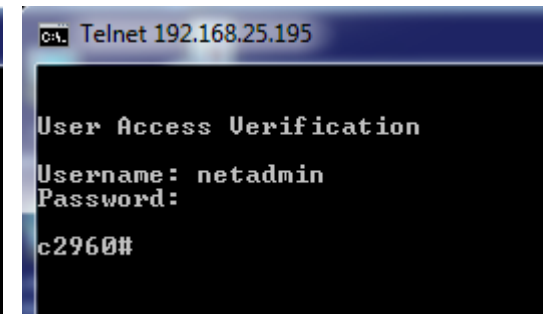
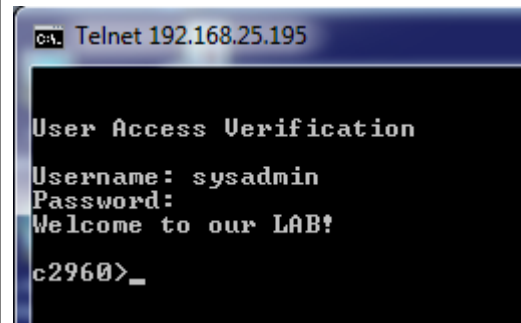
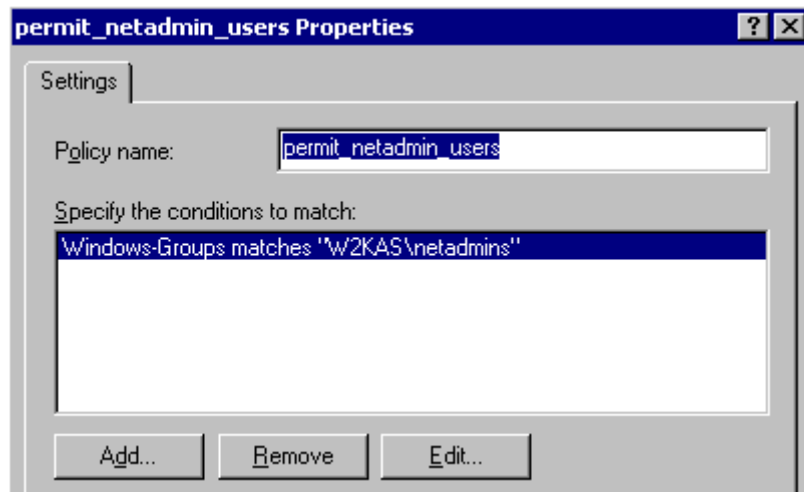
- Adjunk vissza valami reakciót a felhasználóknak, demonstráljuk a RADIUS képességeket!
- A keresett attribútum a Reply-Message



# AAA (11)

Engedjük hozzáférni szerencsétlen sysadmint is, de csak user módba jusson be, míg a netadmin automatikusan enable módba. Hogyan? Ismét a Policy-t fogjuk babrálni és megint valamit a RADIUS szervernek kell visszaadnia, amire a hálózati eszköz valamit csinálni fog.

- Hozzunk létre két új csoportot (netadmins, sysadmins) az IAS szerveren
- A felhasználókat szórjuk a megfelelő csoportba
- Módosítsuk a meglévő policy-t, hogy csak egy csoportra legyen érvényes (sysadmins)
- Hozzunk létre egy új policy-t, ami a netadminokra érvényes és enable módot ad



# AAA - Gondolatok

- Az AAA, mint koncepció a hálózatok minden területén jelen van és minden centralizált hozzáférés- és jogosultság ellenőrzés, valamint számlázás alapja.
- Ismerkedj meg az AAA alapjaival és a világban bárhol legyen is a következő munkahelyed, nem leszel elveszett ember
- A RADIUS / TACACS+ csak egy protokoll, az aktuális környezet dönti el, melyik a jobb, az alapkoncepció mindkettő esetében ugyanaz
  - Központosított azonosítás, jogosultság-kezelés, számlázás bárhol a hálózatok világában
    - ✓ Menedzsment hozzáférés
    - ✓ Hálózathoz hozzáférés: 802.1x vezetékes, vagy vezeték nélküli környezetben
    - ✓ VPN megoldások (PPTP, L2TP, IPSec,)
  - Szerver szolgáltatásokhoz való hozzáférés-kezelés
    - ✓ SMTP: exim, postfix mind tud radius alapú azonosítást
    - ✓ HTTP: apache – mod\_auth\_radius, nginx – szintén van modul
    - ✓ IMAP: dovecot – PAM-on keresztül támogatja
    - ✓ VoIP: asterisk – teljes radius támogatás, számlázás is (CDR)
    - ✓ VPN: openvpn – pluginnal támogatott
- Gyakran a RADIUS a felhasználói adatokat valamilyen háttér adatbázisból veszi
- Ez lehet tényleg valamilyen adatbázis (SQL)
- De lehet bármilyen AD, LDAP háttér
- Vagy csak simán lokális állományok (freeradius: users.conf)
- **Az AAA a hálózatok világában eléggé központi kérdés, aki karriert tervez ebben az iparágban, jobb, ha szoros barátságot köt a témával**

# 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!**

