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 hozzárférés
    - 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

Smart Vision Solutions
taking you one step ahead

VLAN konfigurálás, a konzisztencia fenntartása

- VLAN (Emlékeztető)
  - Azonos fizikai eszözben 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

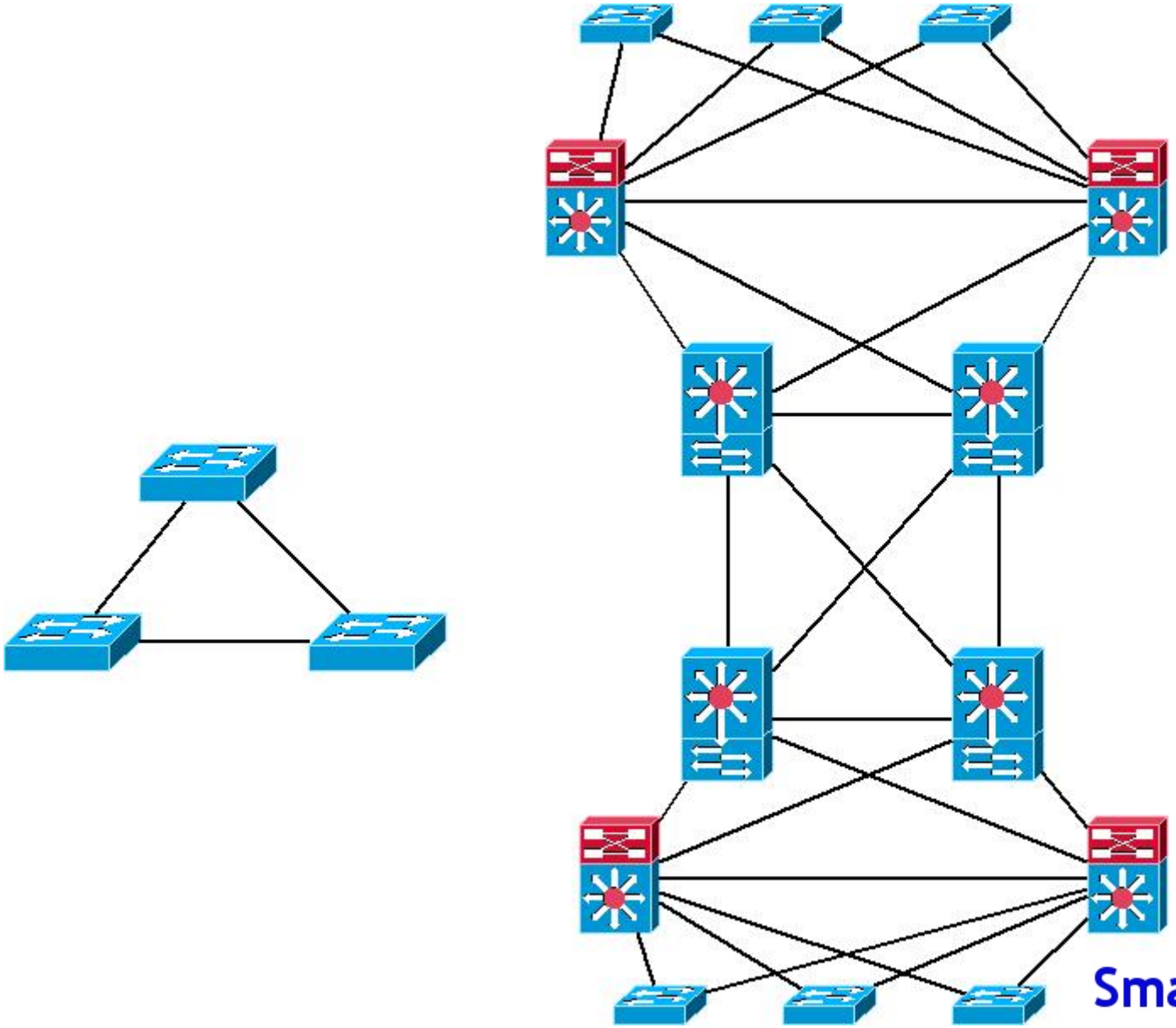
- Milyen problémáink vannak?

- 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

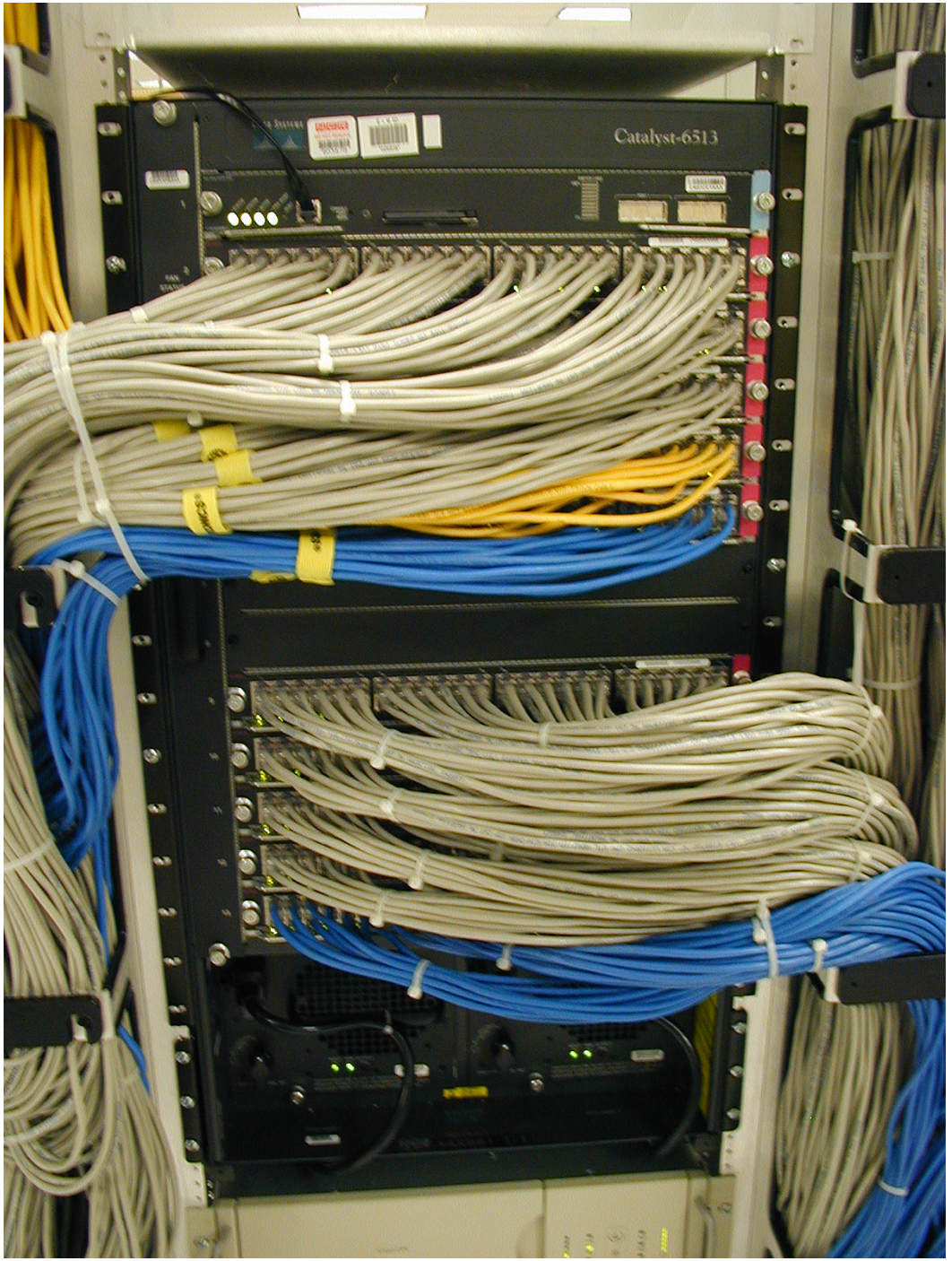
- Ne három, vagy öt switchben gondolkozzunk – a probléma a skálázhatóság
- Átlag Bélánál van 150 végpont és hat switch – fejben tartja
- Egy hálózati mérnöknek több tízezer végpontja, néhány ezer eszközön
- Néha nem, hogy több épületben, de több kontinensen is elszórva

VLAN konfigurálási problémák



Smart Vision Solutions

taking you one step ahead

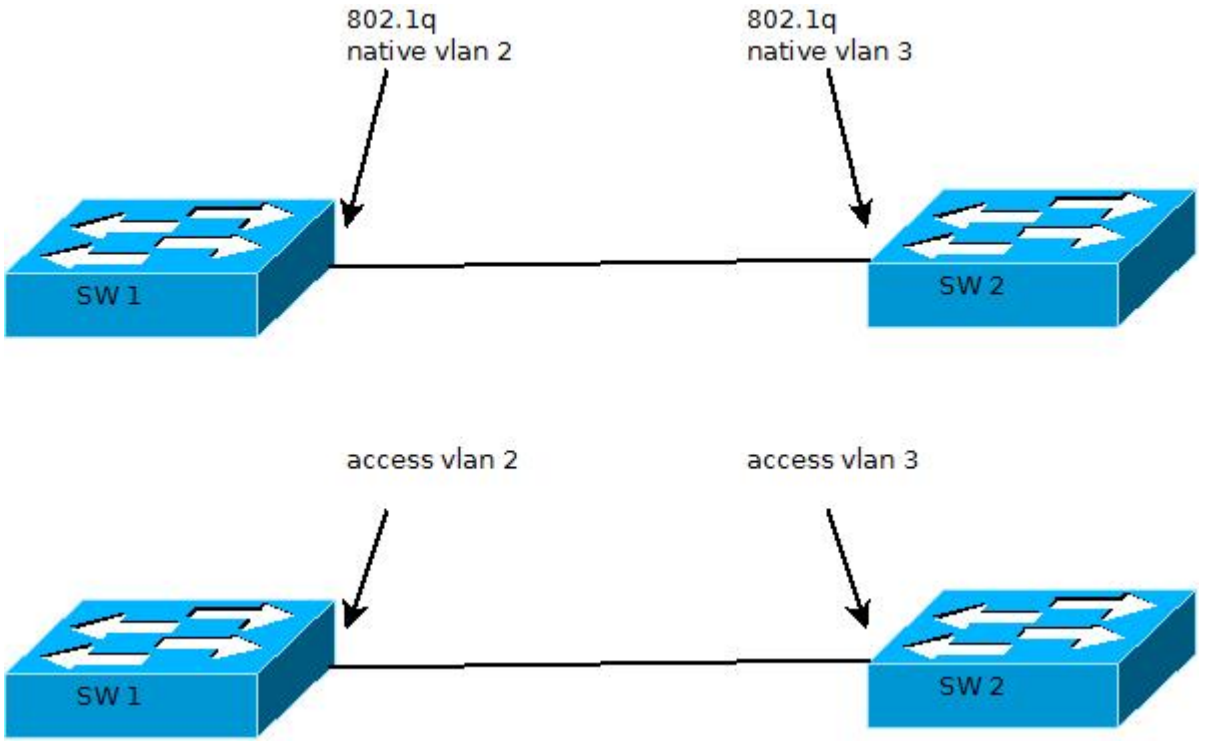


Smart Vision Solutions

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?

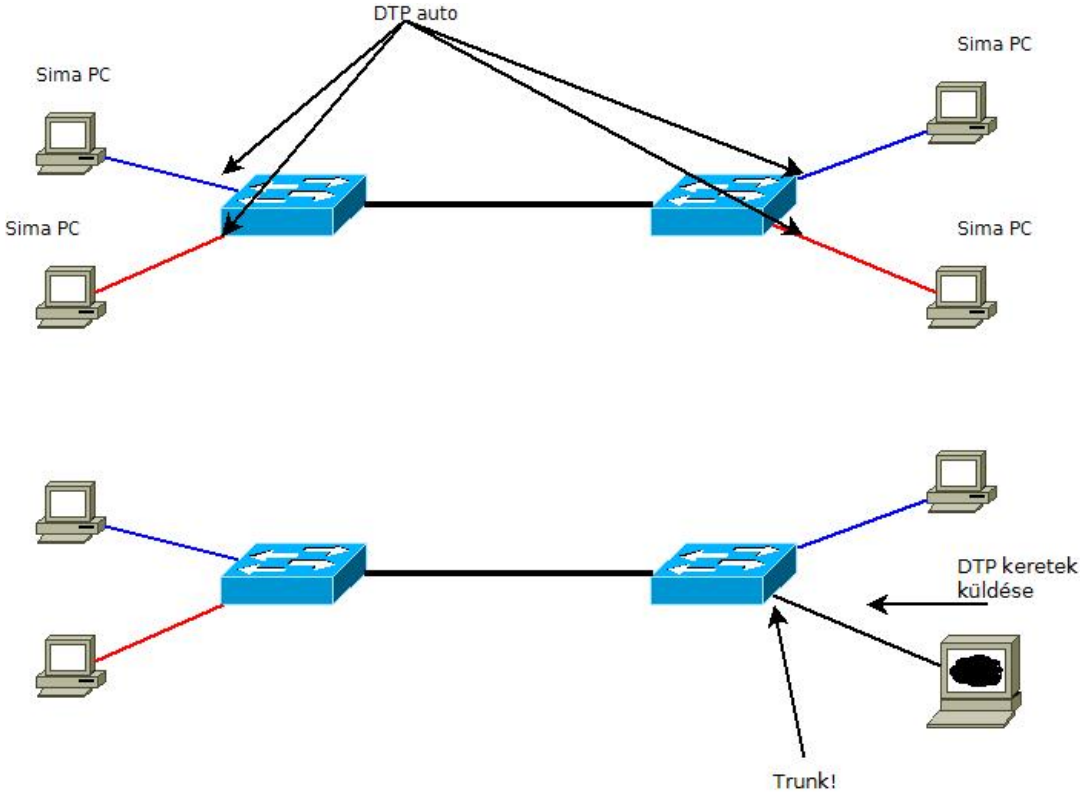
Miért biztonsági kockázat?

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 alapértemezetten 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, ezetúl megkaphatja bármelyik, switchen engedélyezett vlan forgalmát.

A két vlan között akár átjáróként is működhet.

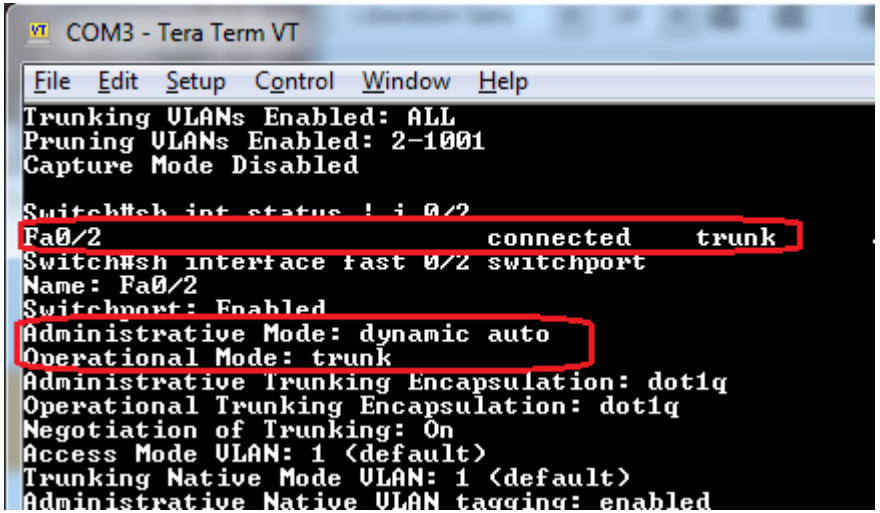
A DTP jeletősége

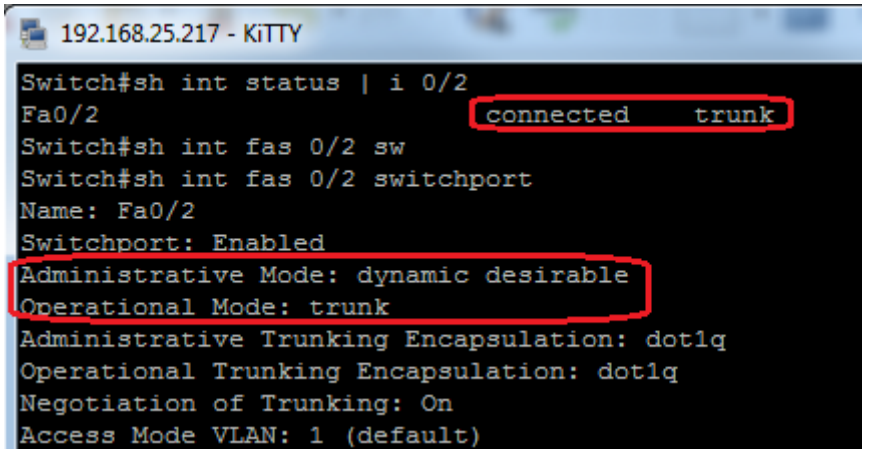
Amennyiben egy switchport lehet trunk, akkor erről többnyire egyezkedni is tud. Miről kell egyezkedni?
- Egyátalán legyen-e trunk vagy sem
- Ha legyen, akkor milyen protokoll szerint (802.1q, ISL, egyéb)

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:





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 vlan x 100 eszköz x 10 mp = 100 000 mp = 27 óra = **3.5 munkanap** valakinek

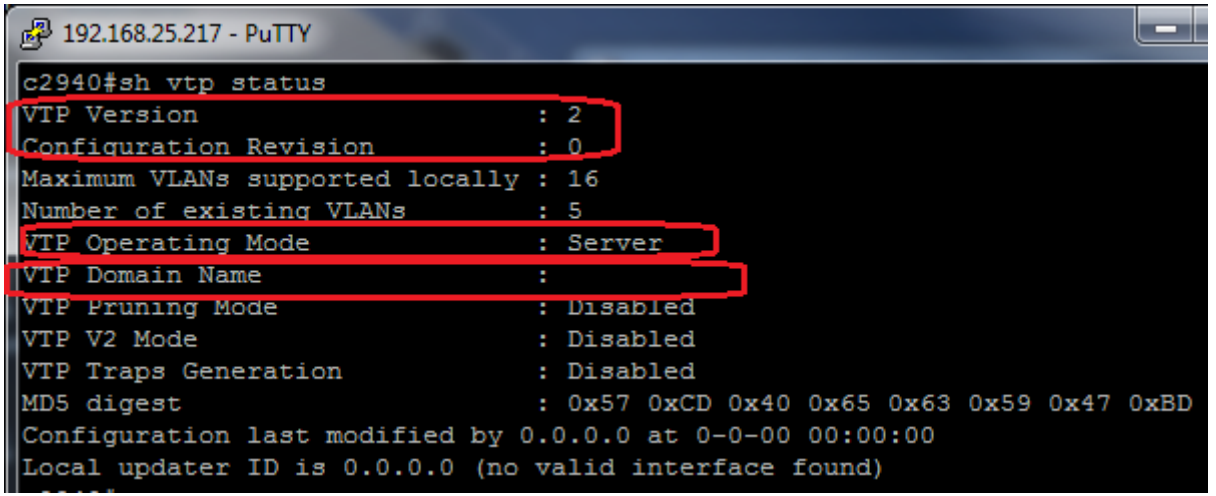
VTP esetén egy helyen konfigurálunk, azaz 100 vlan x 10 mp x 1 = **17 perc** alatt megvagyunk

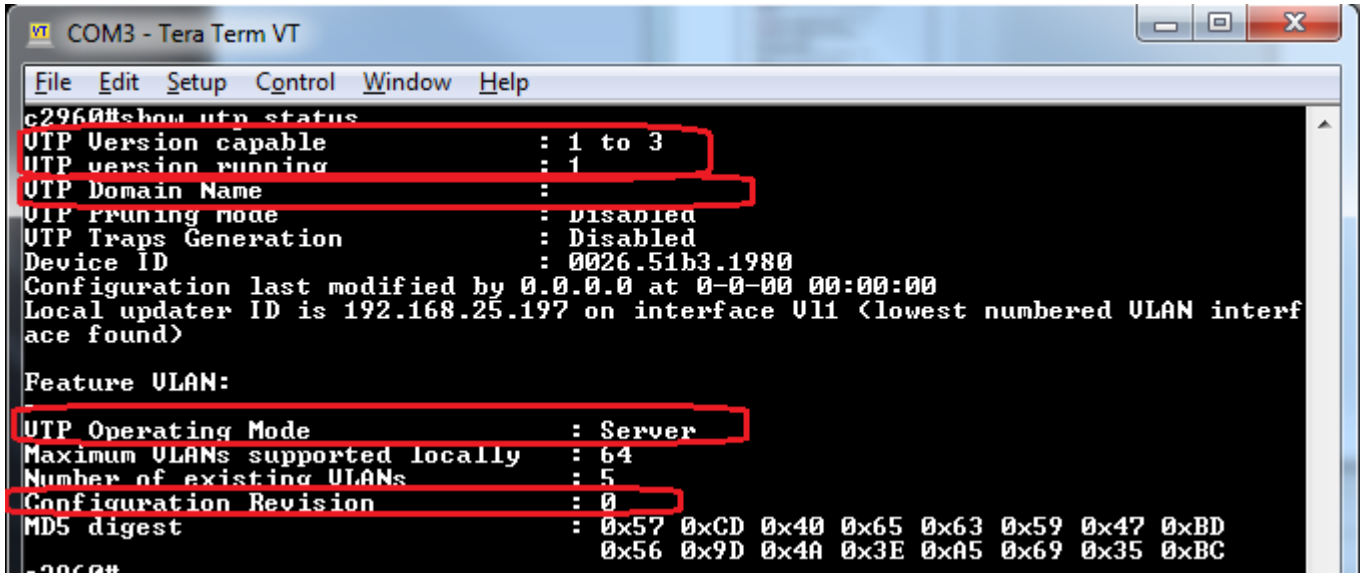
Client	Lokális konfiguráció nincs, VTP domainen belül szervertől tanul
Server	Lokális konfiguráció, az eredményt a kliensek tanulják domainben
Transparent	Lokális konfiguráció, VTP kereteket átpasszolja magán

Smart Vision Solutions
taking you one step ahead

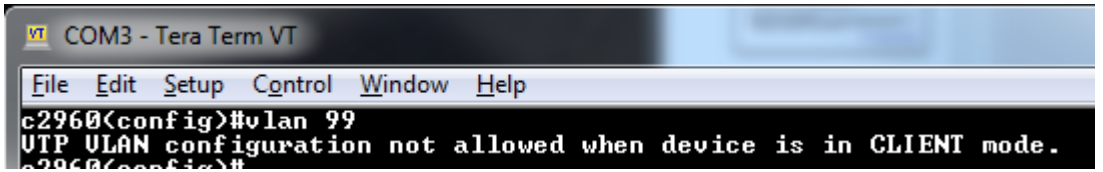
VTP

- 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

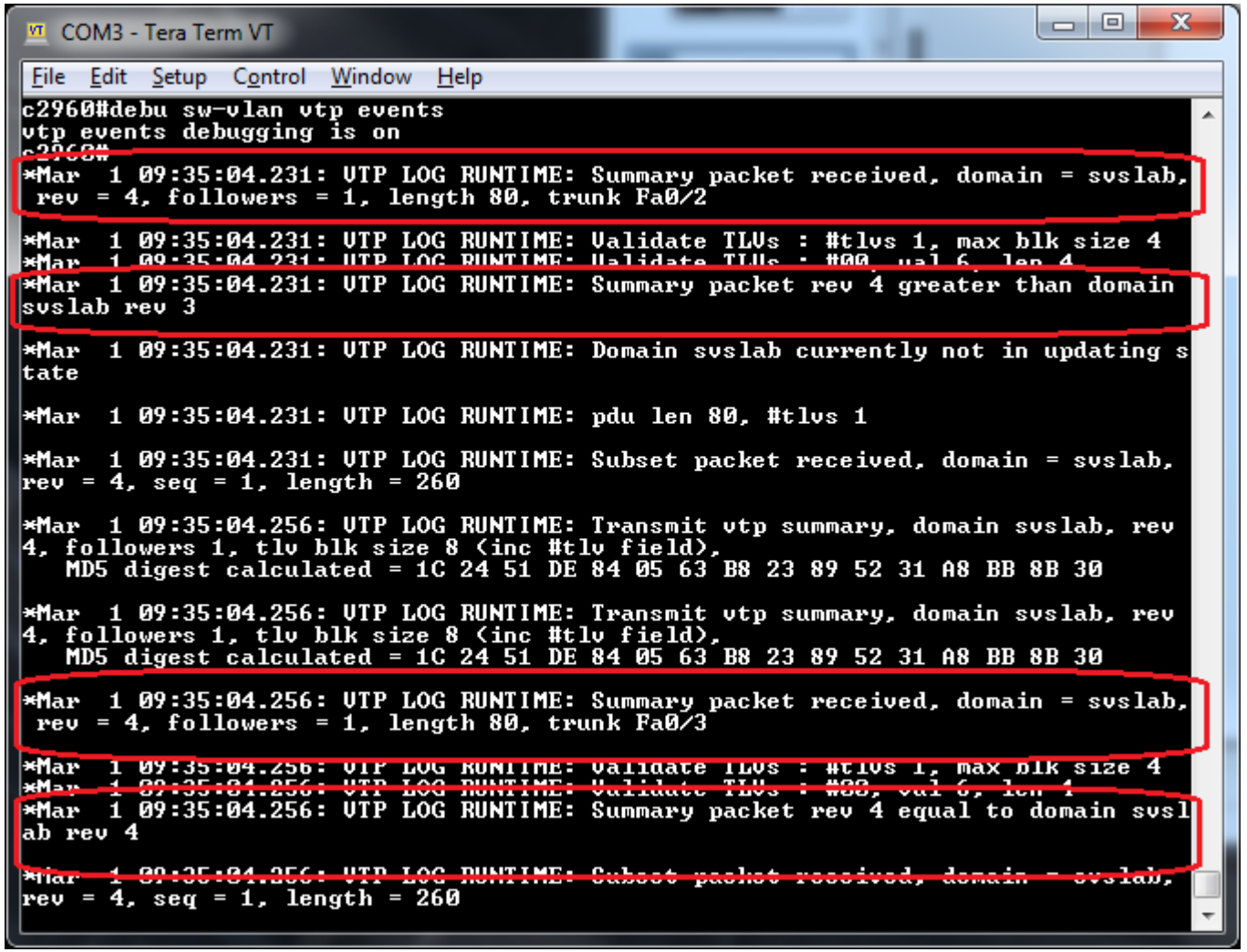




VTP (2)



Látható, hogy kliens módban nem lehet VLANokat konfigurálni



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

A Fa 0/3 -mon is érkezik VTP, de eddigre a négyes verziójú konfiggal 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 sebességemmel egy VLAN egy eszközben 10 mp, akkor szumma 3.5 napnyi munka.

Ez jó.

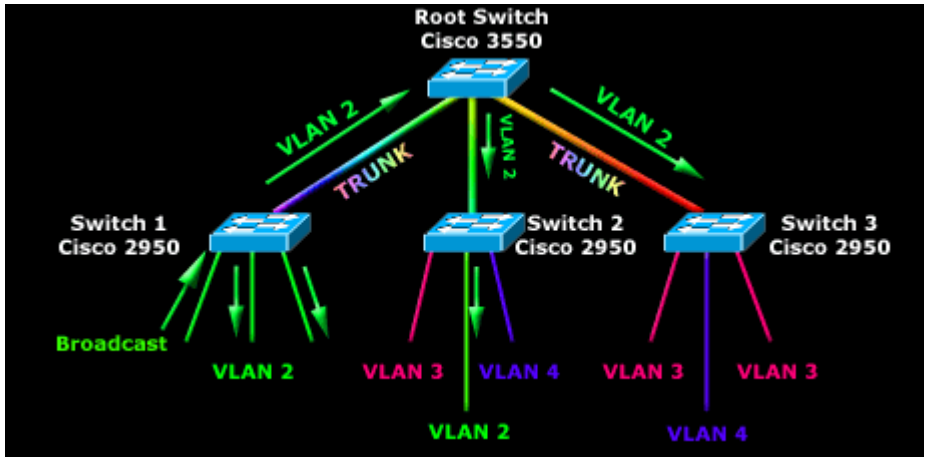
Viszont, ha nincs minden munkaállomás mindenhol jelen, azaz nincs minden VLANra minden switchben szükség, akkor minden switch 100 darab feszítőfát számol, 100 darab ARP táblát, 100 darab CAM táblát tart nyilván, interfész billenéskor legrosszabb esetben 100 VLANban egyszerre számol újra feszítőfát. Ez 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.

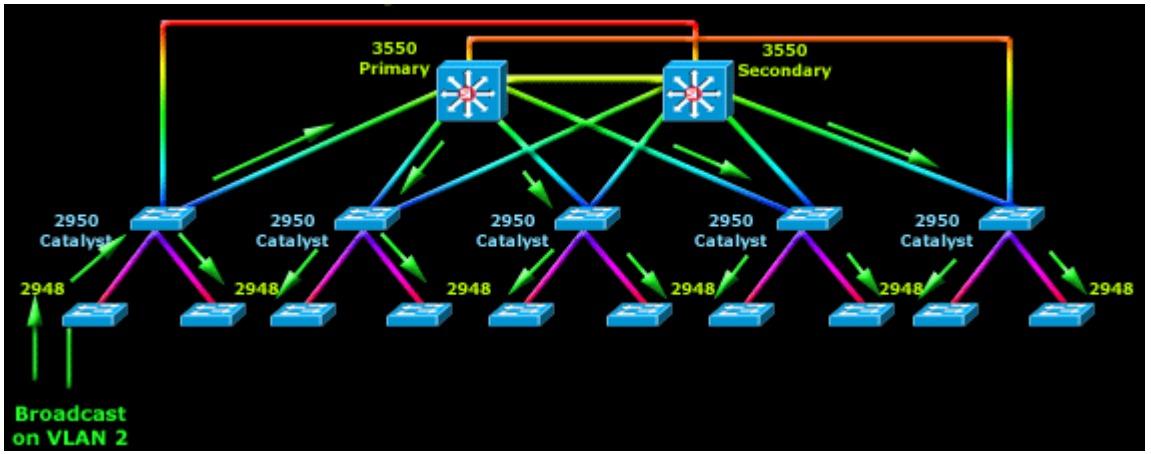
A csodálatos VTP protokoll, bár megoldja a konfiguráció konzisztencia problémáját, bevezet két problémát: egy **erőforrás** problémát és egy **kapacitás** problémát.

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”).



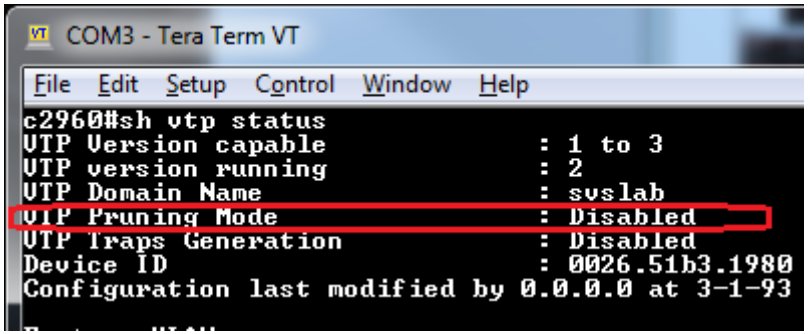
Nagyobb, vagy egyenesen nagy hálózatokban viszont olyan jelentős túlterhelést okozhat a meggondolatlan VTP használat, ami már hasznos sávszélességet vesz el a felhasználóktól.

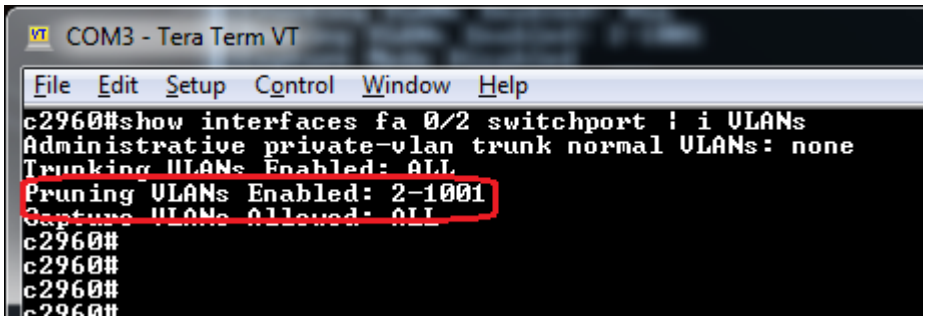
VTP pruning

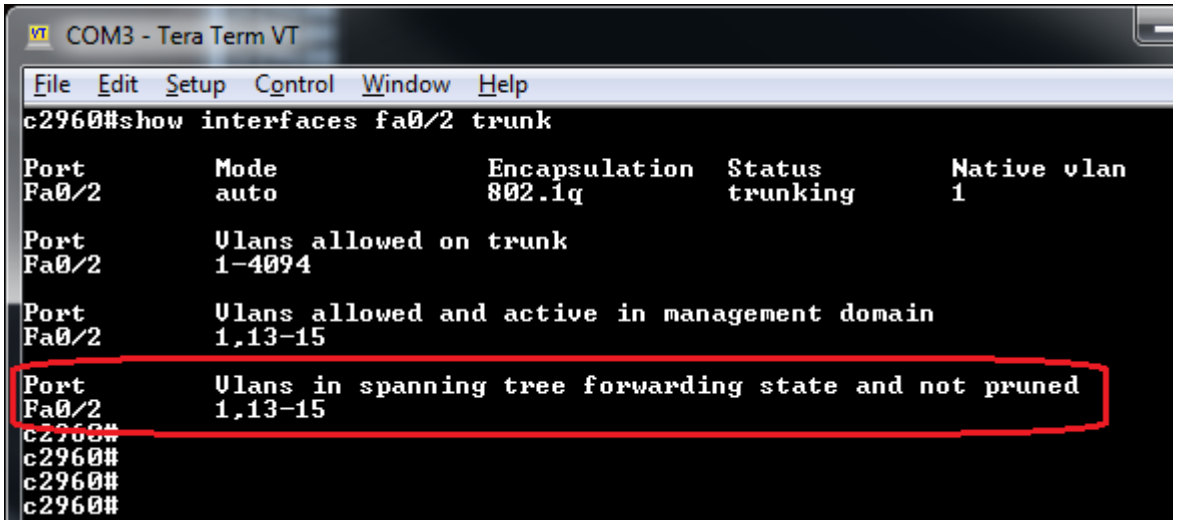
A dolgot kézzel is lehetne kezelni, de akkor megint manuálisan kéne konfigurálni a dolgokat, a VTP-nek semmi értelme nem lenne.

- 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.







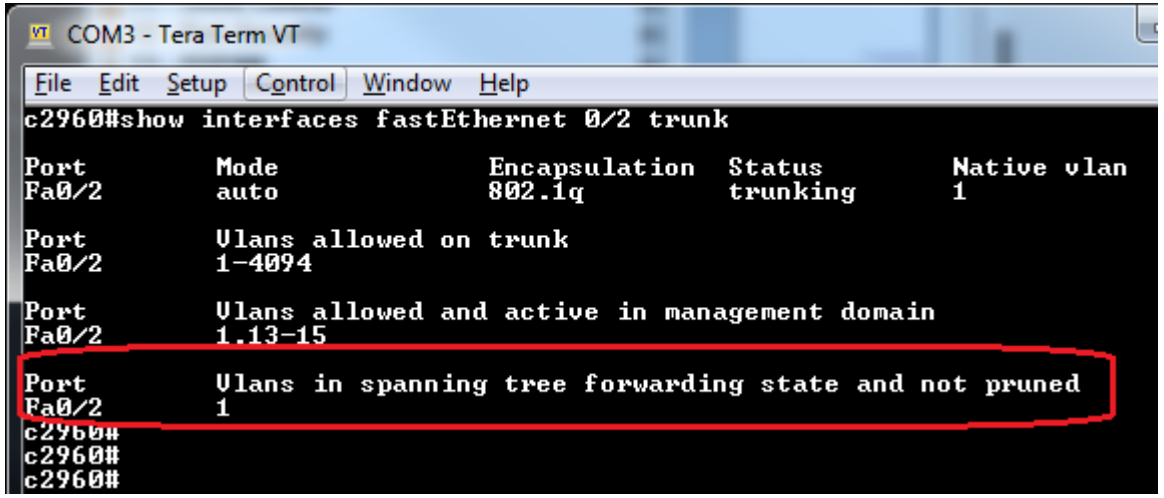
A pruning lehetősége alapértelmezetten adott, de kikapcsolt

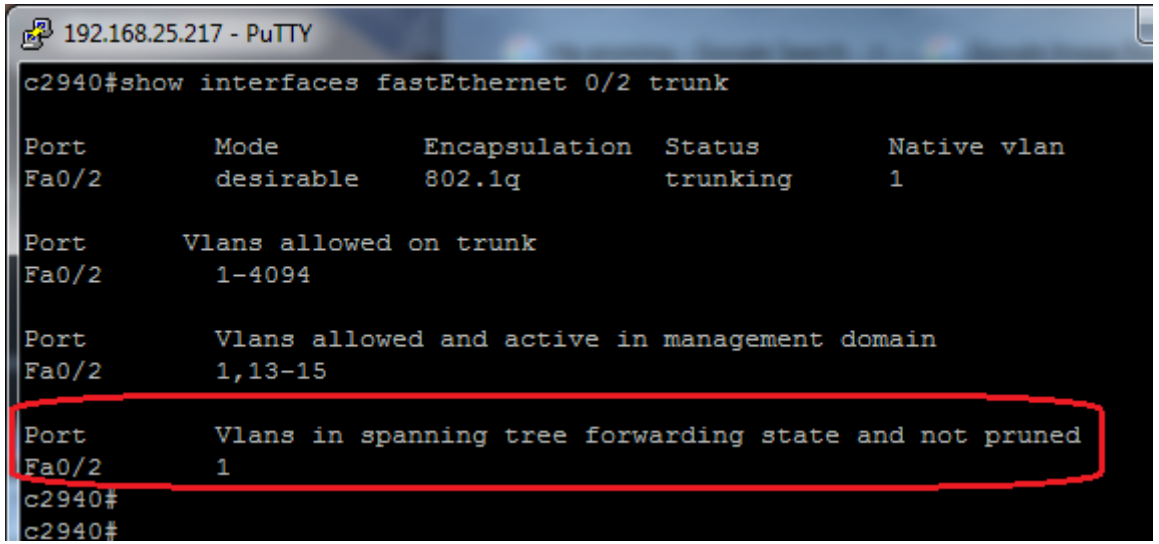
Smart Vision Solutions
taking you one step ahead

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 protról lekerül minden olyan VLAN, aminek nem kell ott lennie (1-en kívül mind lekerül)



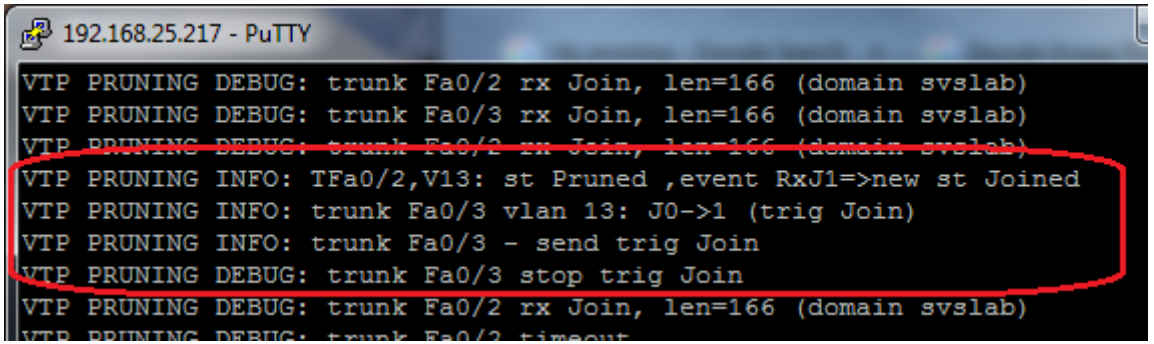


Egyetlen helyen, a szerveren beállítva elterjed a pruning beállítás és mostantól a switchek lebeszélik egymással, melyik VLAN-t hova kell és hova nem kell továbbítani.

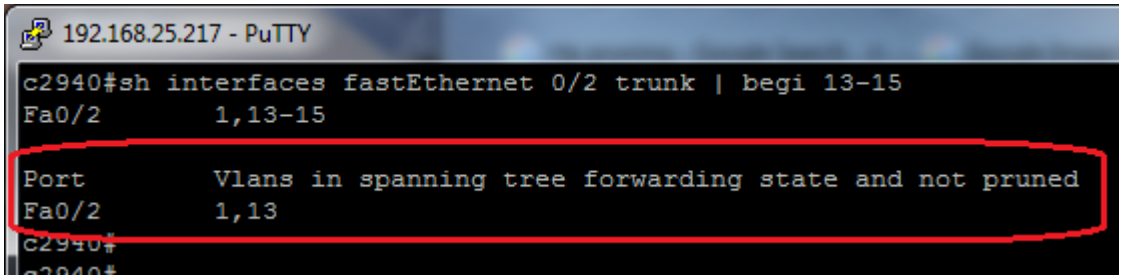
Amint megjelenik egy valós érv arra, hogy a VLAN mégis kell, meg fog jelenni. Ez az érv lehet:

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

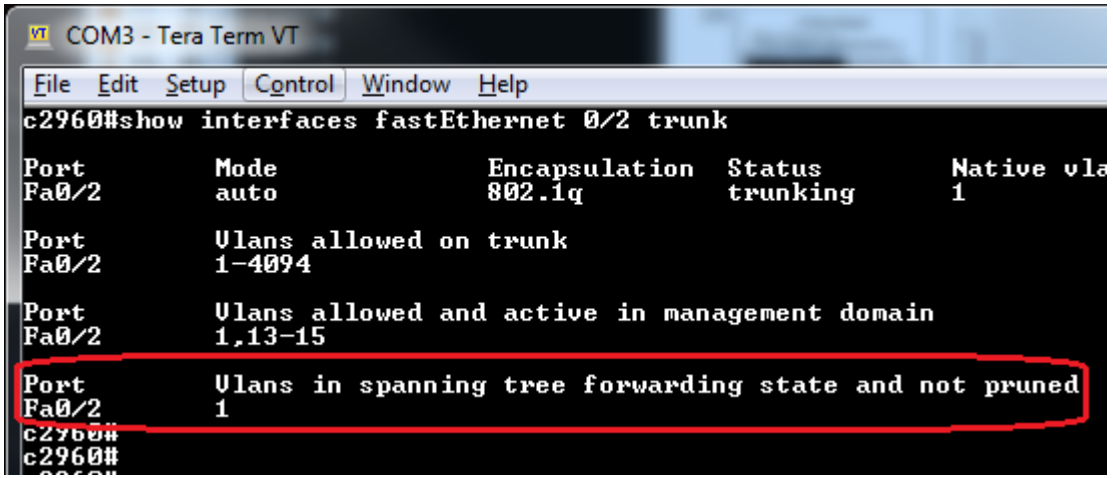
VTP pruning (3)



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



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



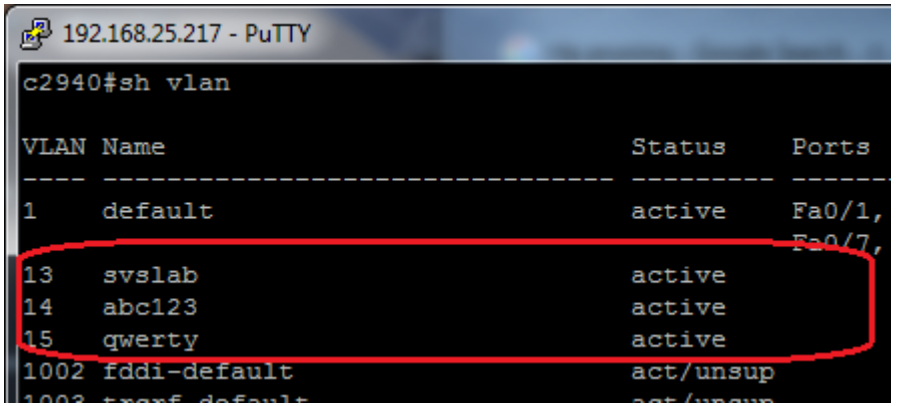
Ugyanakkor azt is látjuk, hogy a **visszafelé** irányba ez **nem történik meg**, mivel a 2940-es switch felől senki nem kérte ezt a forgalmat, így a 2960-as switch nem továbbítja. Ez normális, a **labor körülmények miatt**, a való életben ritkán van ilyen eset, hiszen a gép így **nem lát ki** a saját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

Tartsd naprakészen a CV-det!

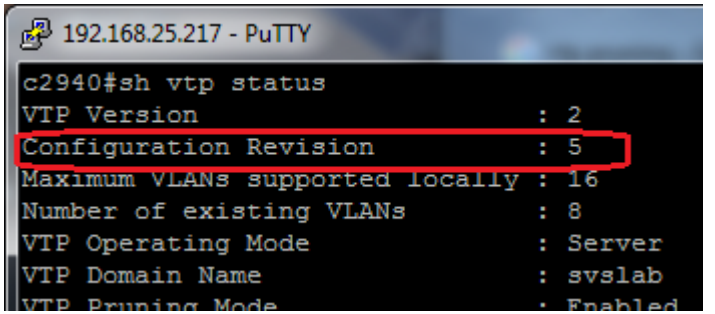
- A VTP-vel katasztrófális hibát lehet okozni, akár véletlenül, akár rossz szándékkal is.
- A VTP-ben négy fontos dolog van: domain, jelszó, a revision number és az üzemmód.
- Ezek alapértelmezetten: üres, beállítatlan, nulla és szerver.

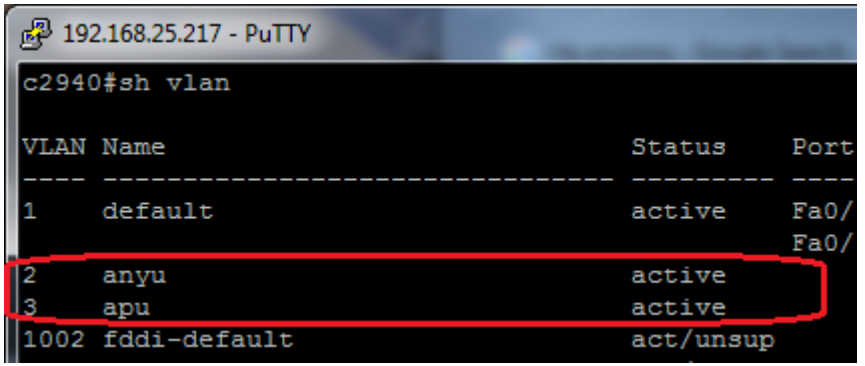
Mi történik, ha figyelmetlen vagy?

- 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?

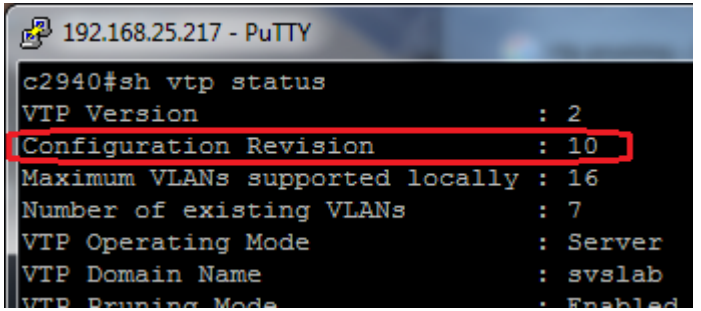


Előtte





Utána



Smart Vision Solutions
taking you one step ahead

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

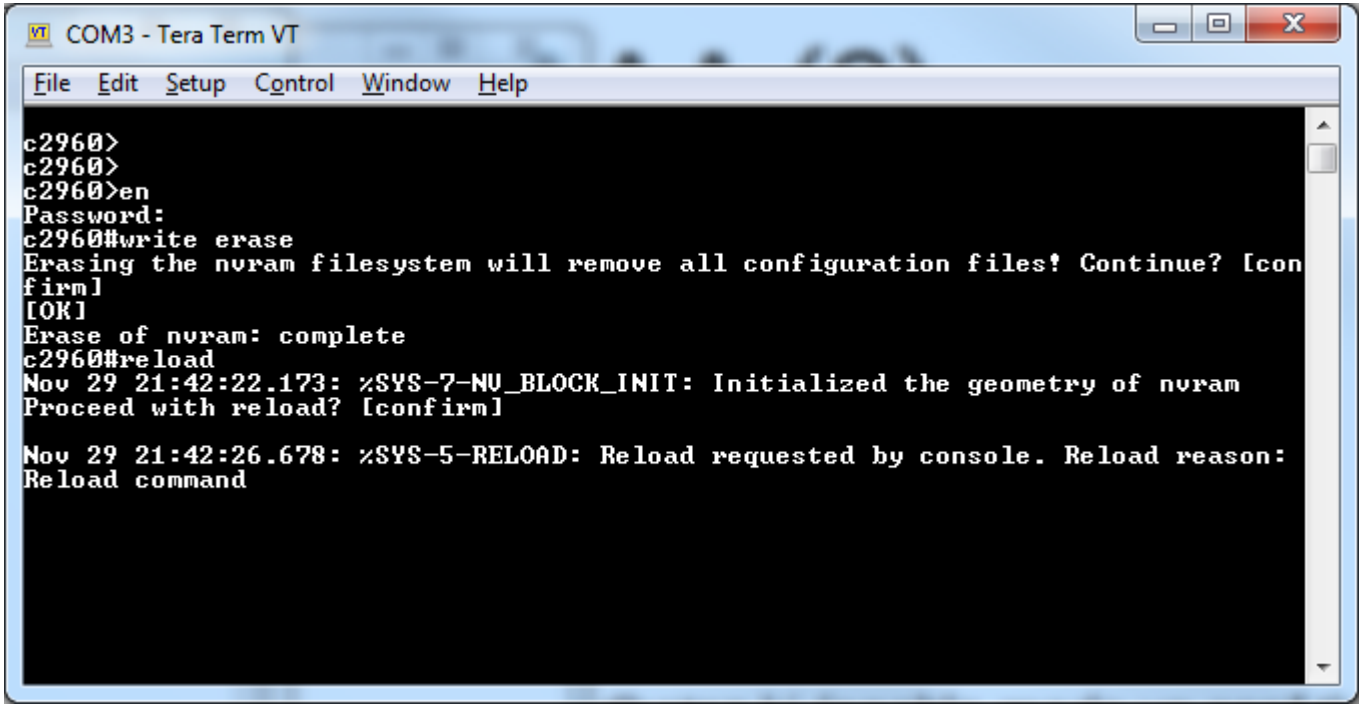
Konfiguráljuk ezt be. Hozzávalók:

- 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



Majd alkalmazzunk egy kvázi-default konfigurációt

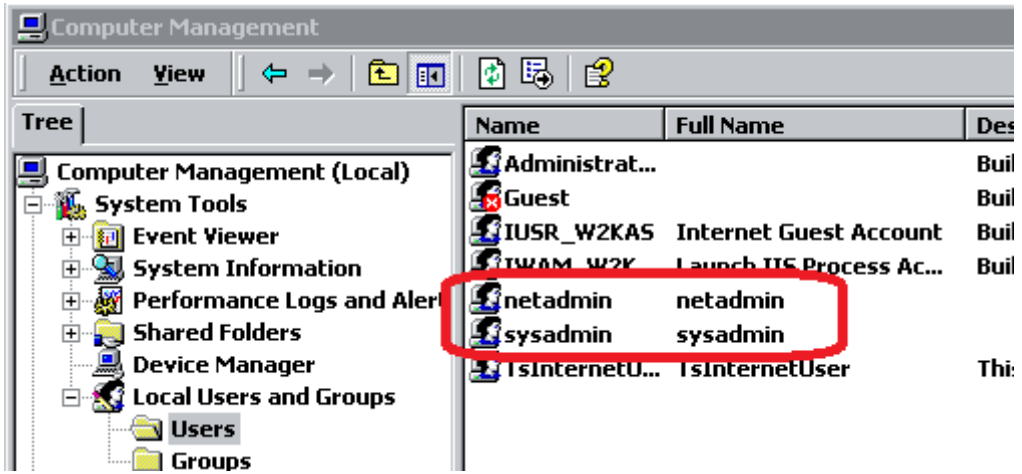
- enable jelszó
- lokális felhasználó, lokális jelszóval
- távoli hozzáférés (telnet, ssh)
- hostnév
- kulcsok ssh-hoz
- ssh v2 bekapcsolása
- IP cím ellenőrzése (radius-szal egy tartományból)

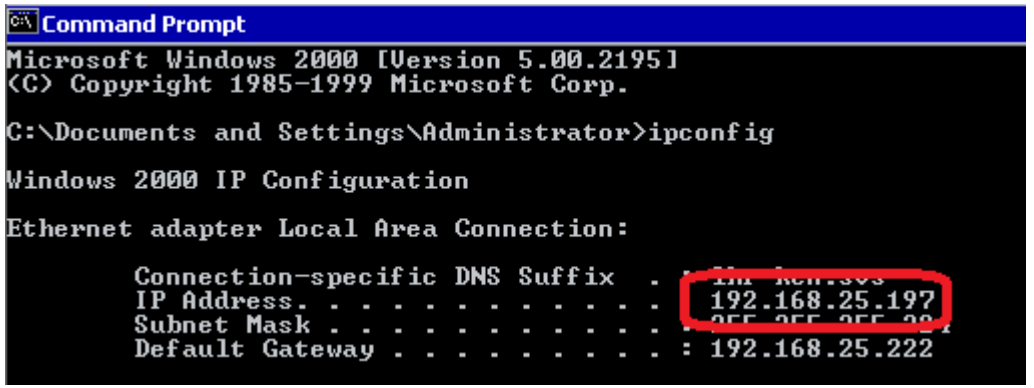
AAA (4)

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.

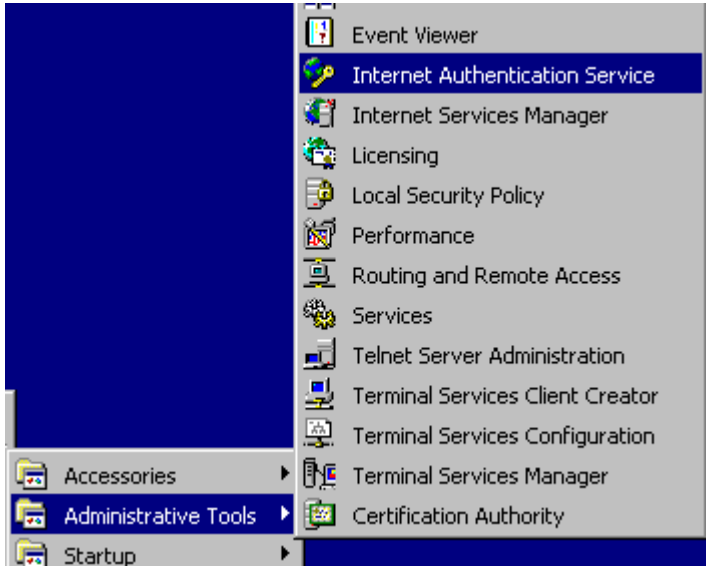




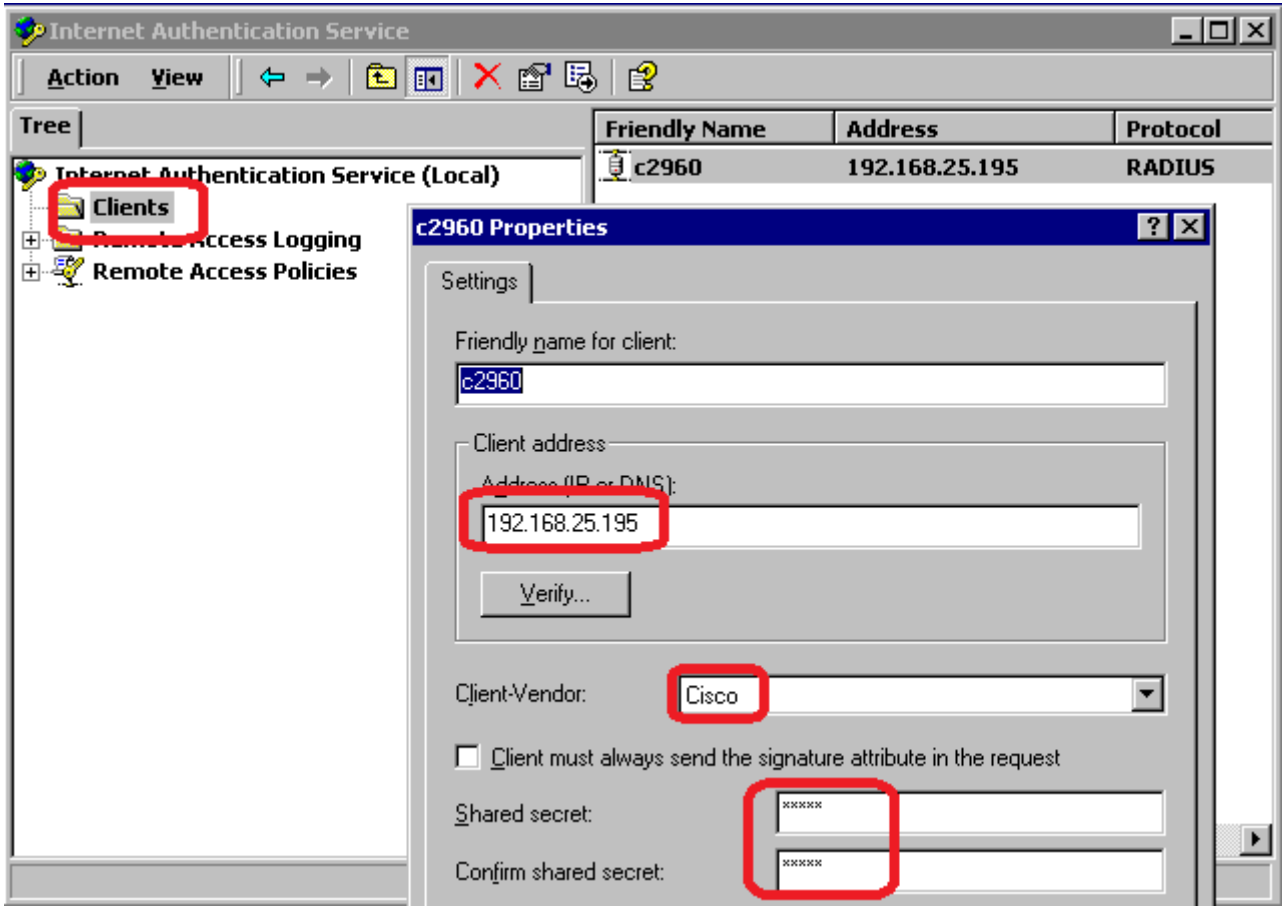
Install után minket most csak két új felhasználó érdekel: netadmin és sysadmin. Előbbi RW, utóbbi RO (inkább ne rontson el semmit).

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.

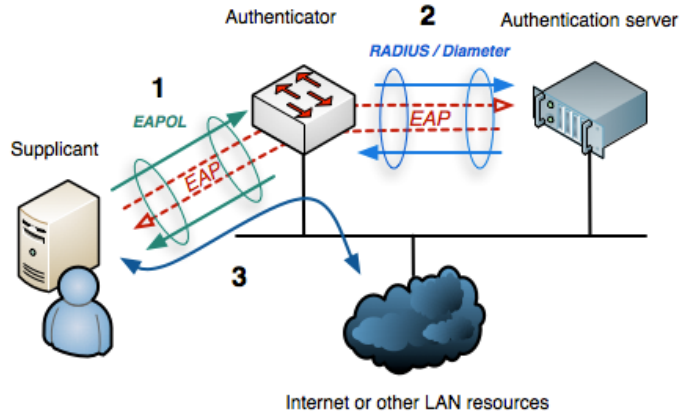
AAA (5)



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#
```

Smart Vision Solutions
taking you one step ahead

AAA (6)

Switch bekonfigurálása, hogy egyátalán 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

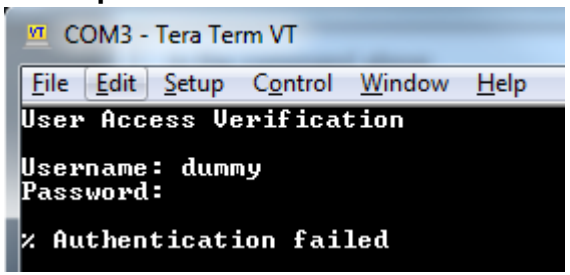
aaa authentication login default group radius local

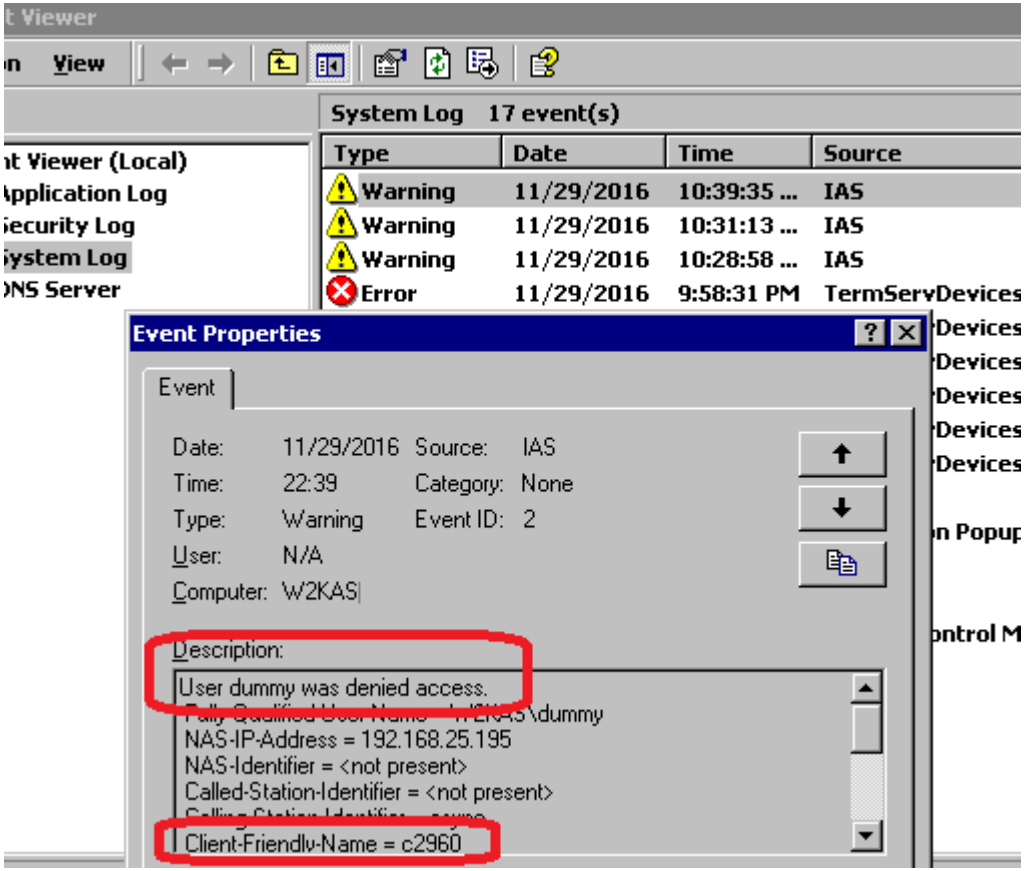
aaa authentication = a megfelelő A kiválasztása az AAA-ból
login = mikor szeretném használni
default = hol szeretném használni
group radius = mit szeretnék használni elsődlegesen
local = mit szeretnék használni, ha az elsődleges nem működik

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

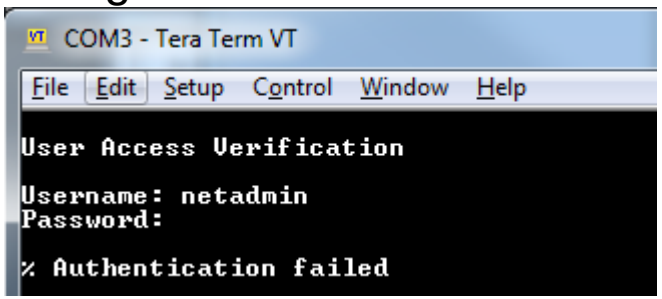
AAA (7)

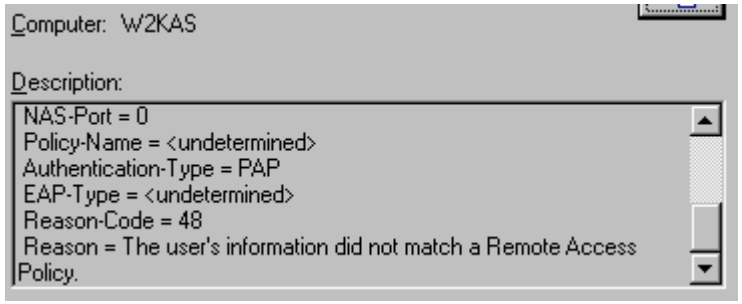
Demonstrálandó, hogy a RADIUS kapcsolat működik





Demonstrálandó, hogy a RADIUS szervert még konfigurálni kell





Smart Vision Solutions
taking you one step ahead

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:

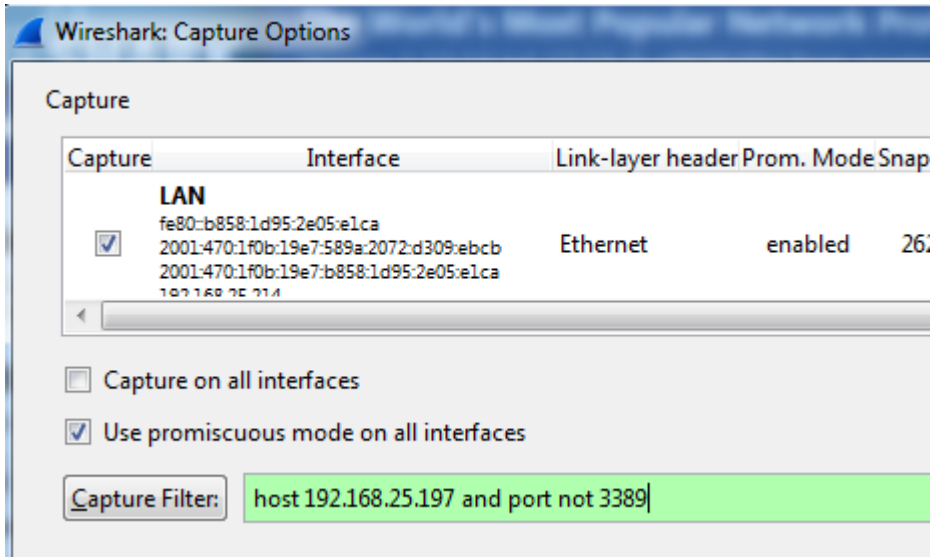
- Megjavítjuk (befejezzük) az IAS konfigurációt
- Elérhetetlenné tesszük a radius szervert (több kliens esetén nem jó terv)
- Megváltoztatjuk a kliens kulcsát a radius szerveren
- Megváltoztatjuk a kliens IP címét a radius szerveren

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.

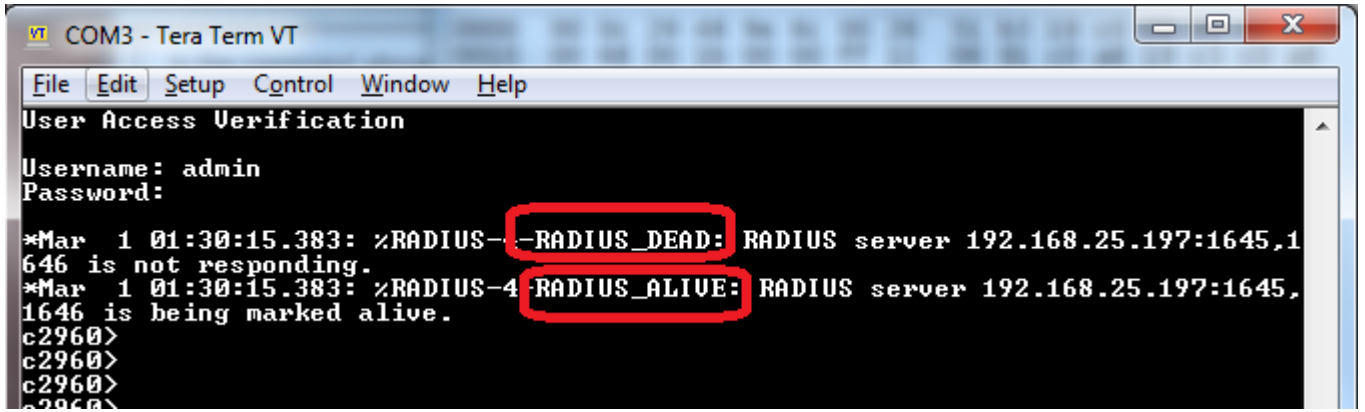
AAA (9)

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



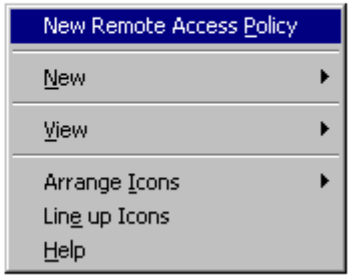
Time	Source	Destination	Info
0.000	192.168.25.195	192.168.25.197	Access-Request(1)
9.022	192.168.25.195	192.168.25.197	Access-Request(1)
18.03	192.168.25.195	192.168.25.197	Access-Request(1)
27.37	192.168.25.195	192.168.25.197	Access-Request(1)
35.93	HewlettP_cc:db:e0	Vmware_48:9e:6c	Who has 192.168.25
35.93	Vmware_48:9e:6c	HewlettP_cc:db:e0	192.168.25.197 is



Smart Vision Solutions
taking you one step ahead

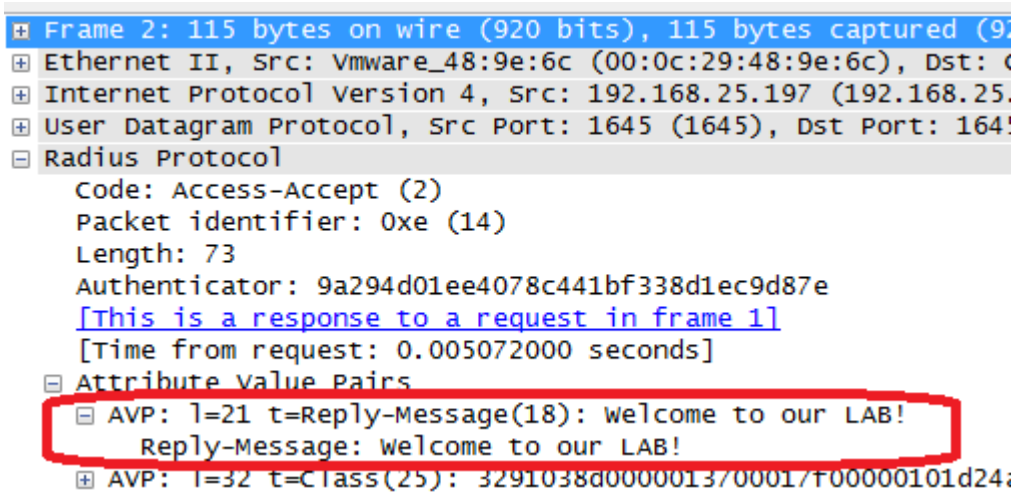
AAA (10)

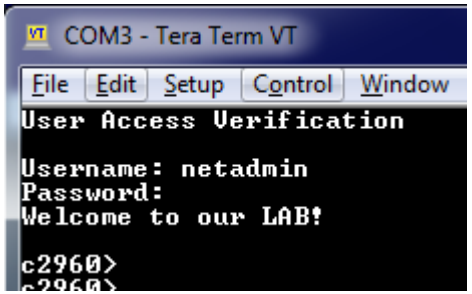
Csináljunk policy-t, hogy be tudjunk lépni és lezárhassuk a kérdést.



- 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



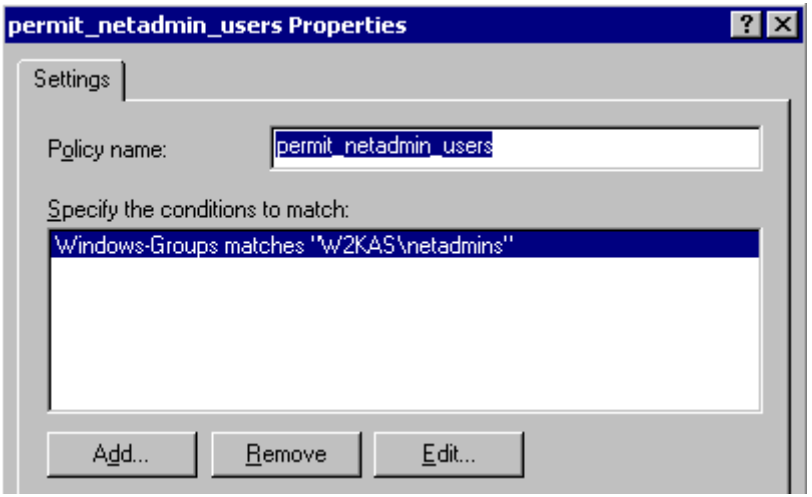


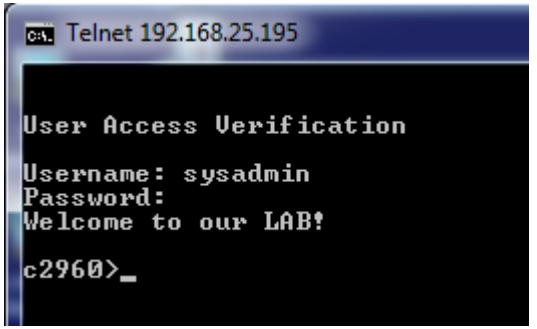
Smart Vision Solutions
taking you one step ahead

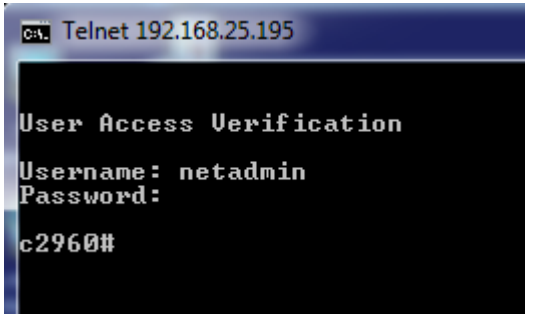
AAA (11)

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!

facebook.com/svsltduk