Hálózati alapok

Bevezetés az adatkapcsolati réteg protokolljaiba

Ingyenes online előadás
2016. november 3.

Smart Vision Solutions
taking you one step ahead

Hol tartunk?

- A rétegek, rétegződés
- Megfelelő fogalmak

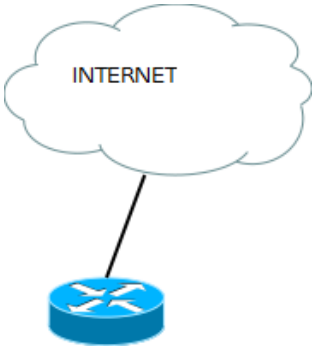
Hozzáférések:

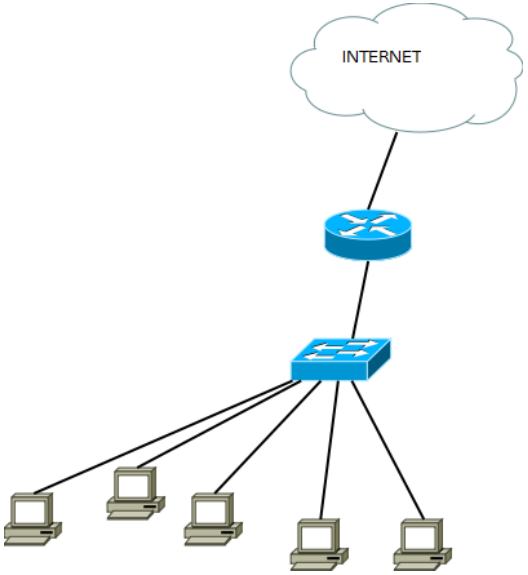
- Helyi
- Távoli
- IP címzés, biztonság, best practice

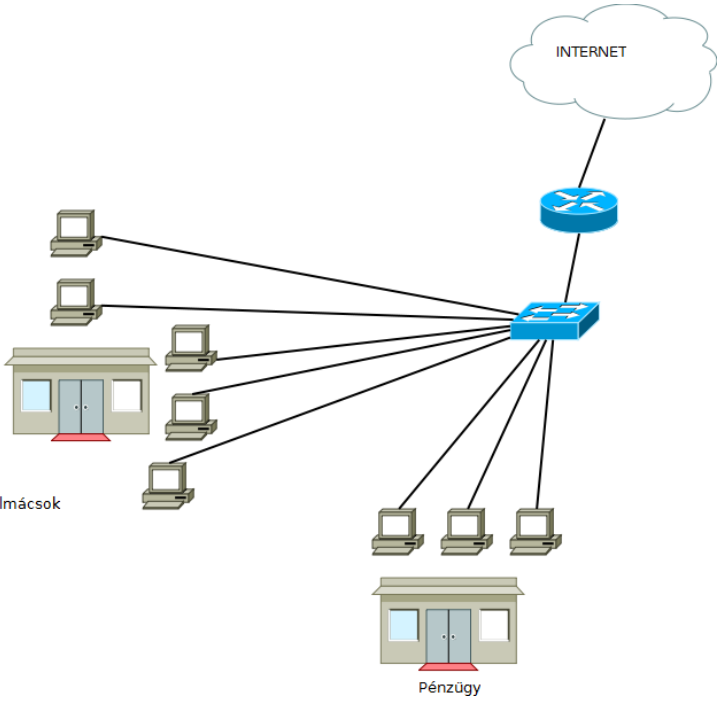
Mai protokollok:

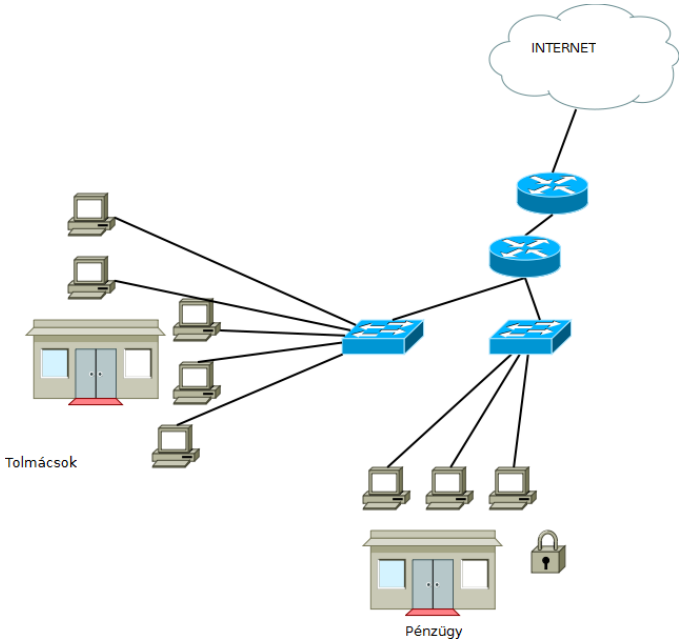
- Vlan
- CDP
- STP
- Etherchannel

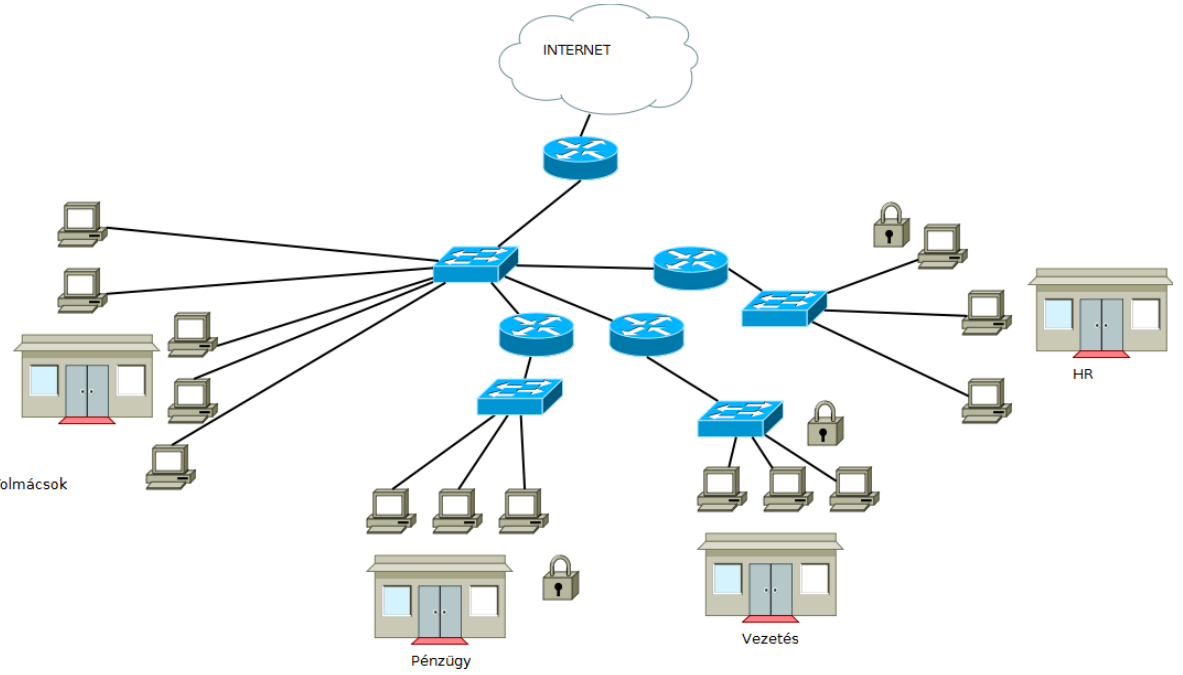
VLAN







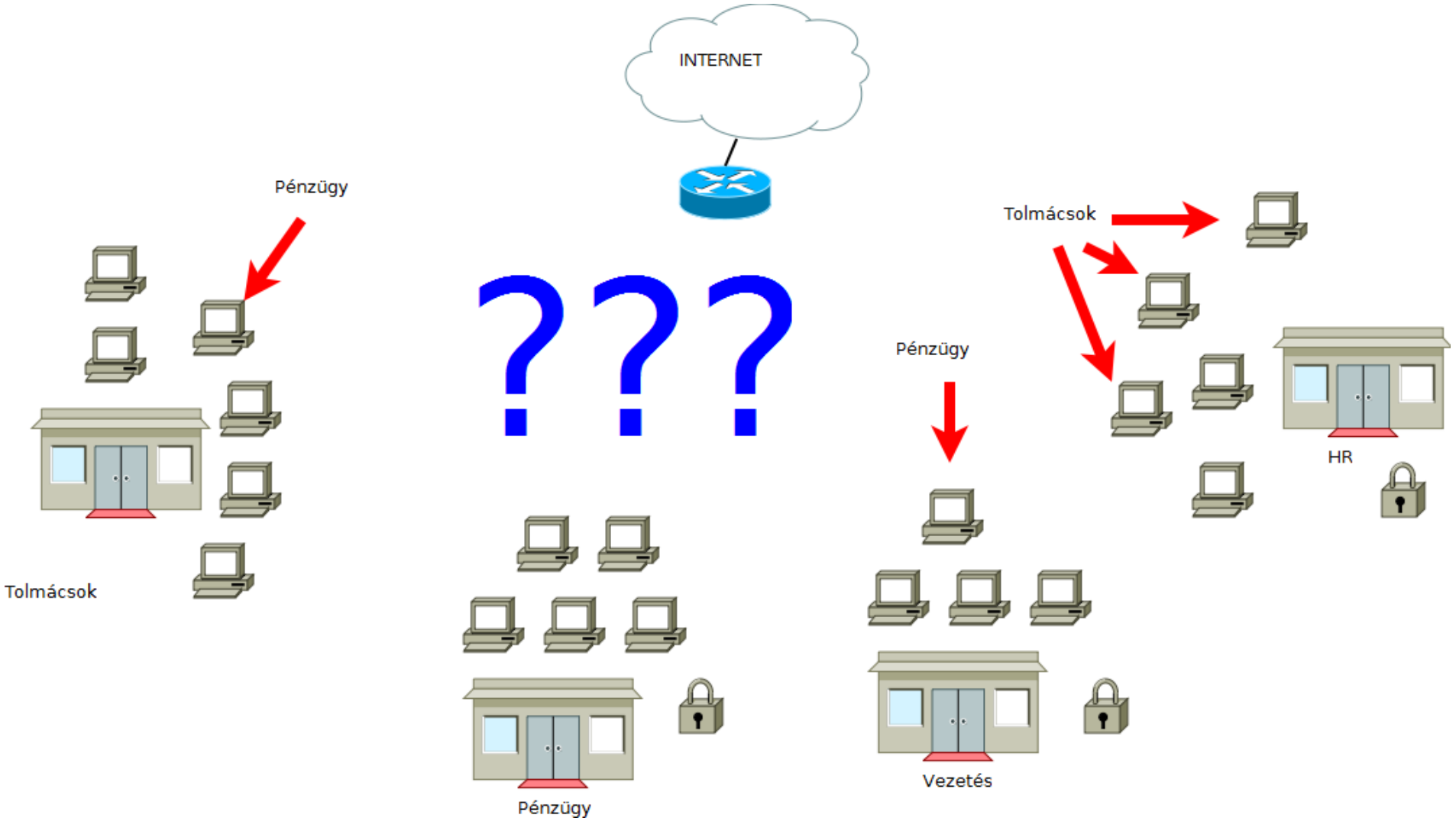




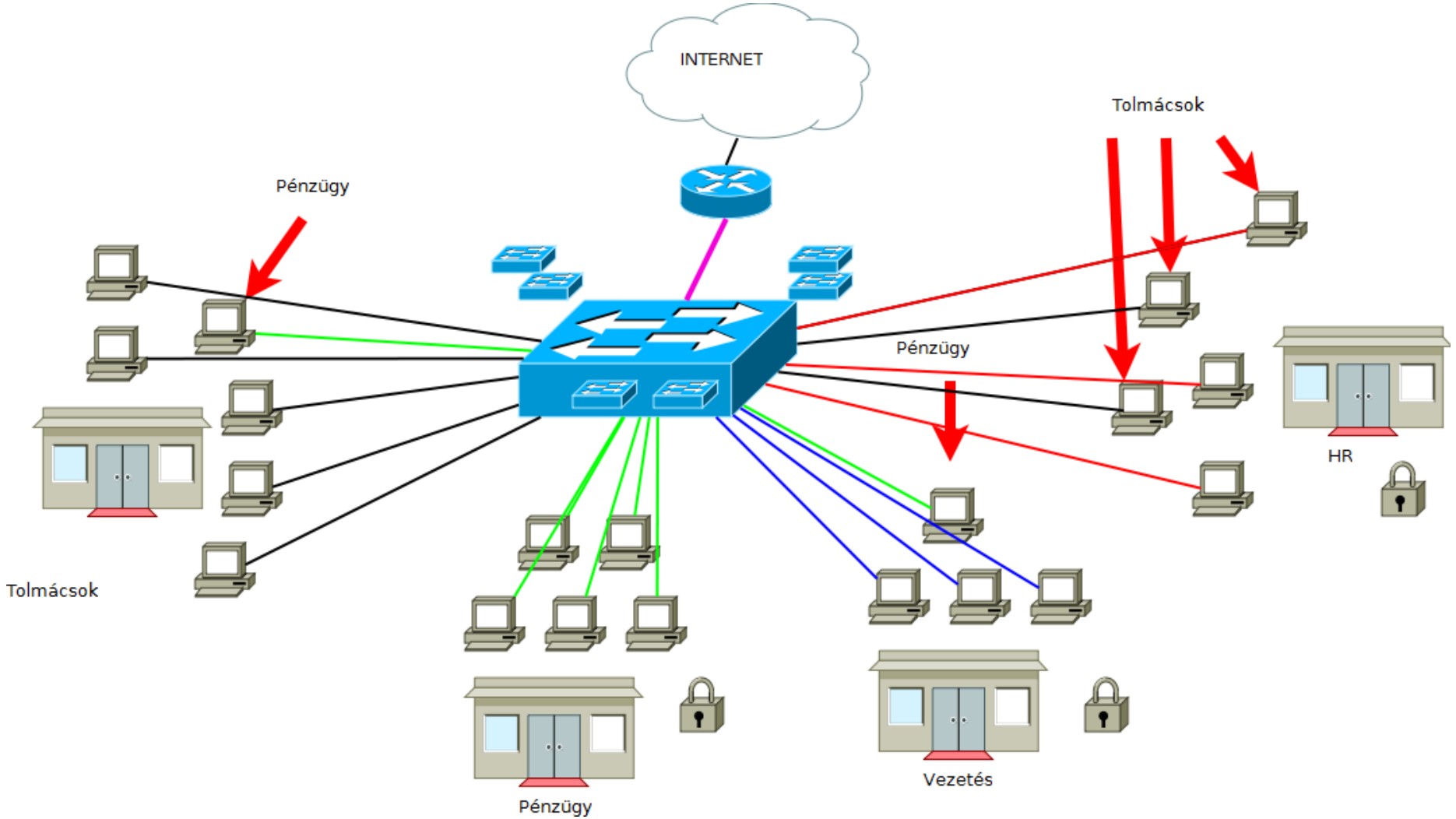
Smart Vision Solutions

taking you one step ahead

VLAN



VLAN

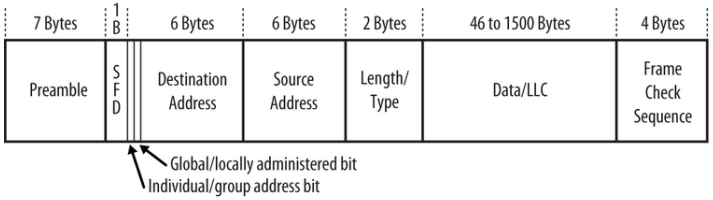


VLAN

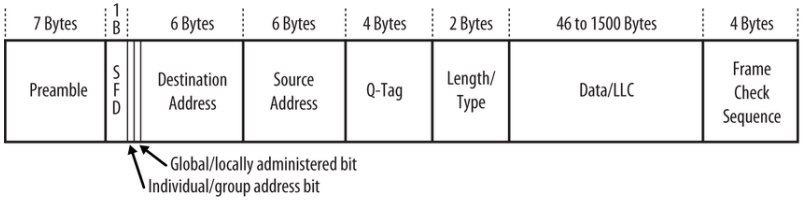
- Csökkennek a kábelezési gondok
- Csökkennek az üzemeltetési költségek, olcsóbb ugyanazt kiépíteni
- Kevesebb eszköz, kevesebb hiba (ugyanakkor komplexebb hibák merülhetnek fel)
- Nem az embereknek kell a hálózathoz alkalmazkodni, hanem fordítva
- Bevezetünk egy **új biztonsági réteg**et, amivel szeparálni lehet a gépeket
- Rugalmasabban lehet követni a módosításokat (szervezeti, fizikai)
- Gondoljunk rá, mintha **ugyanabban** a fizikai kábelben **több kisebb**, virtuális kábel futna
- Sőt, ezeket később “újrakábelezhetjük” úgy, hogy semmihez nem nyúlunk fizikailag
- Sőt, anélkül, hogy bármihez nyúlnánk, vagy tudnánk arról egyátalán, hogy meg kellene csinálni – a hálózat **maga veszi észre**, hogy újra kell kábelezni és **azonnal meg is teszi** helyettünk

Az adatkapcsolati réteg fejléce megint

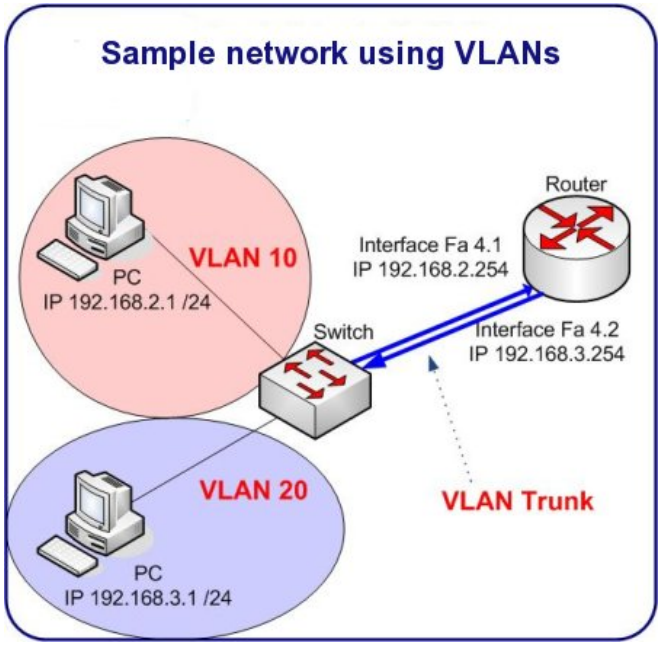
- 4 byte Q-Tag
- Mi történik, ha taggelt keretet kap egy azt nem ismerő?
- **Mindenkinek ismernie kell, aki foglalkozik a fejléccel!**



IEEE 802.3 Basic Frame = Min 64 Bytes, Max 1518 Bytes + preamble



IEEE 802.3 Basic Frame with Q-Tag = Min 64 Bytes, Max 1522 Bytes + preamble

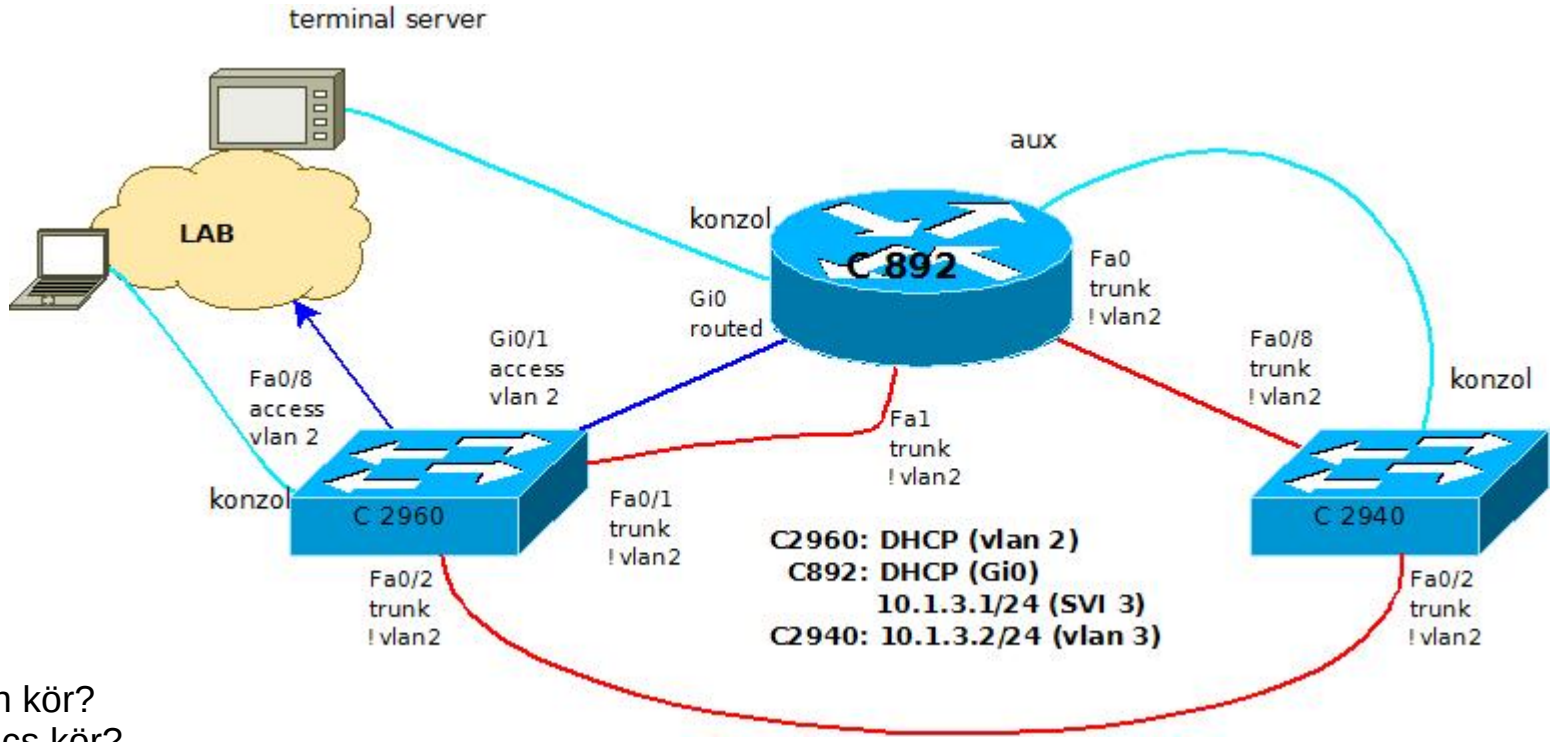


Smart Vision Solutions

taking you one step ahead

Gyakorlat - VLAN

- Vlanok létrehozása
  - elnevezés
  - sorszámozás
- Portok konfigurálása
  - access port
  - trunk port – ISL, 802.1q
  - engedélyezett vlanok
  - natív vlan
- IP címzés
  - sok sok magyarázattal
  - ezt a labort használjuk későbbi feladatokhoz is



- Hol van kör?
- Hol nincs kör?
- **Eddig tanultak hasznosítása:**
  - AUX port – távoli konzol
  - vlanok nagy dózisban
  - konzol hozzáférés és alapvető parancsok
  - IP címzés (statikus és DHCP)

Hol tartunk?

- A rétegek, rétegződés
- Megfelelő fogalmak

Hozzáférések:

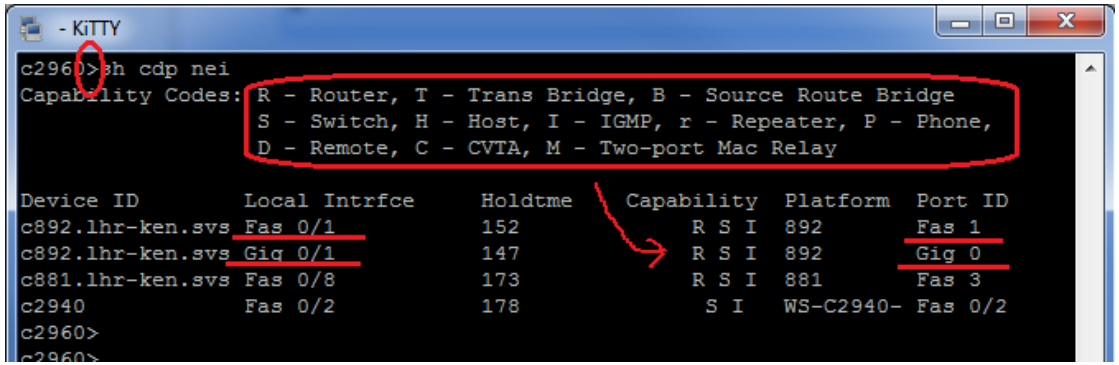
- Helyi
- Távoli
- IP címzés, biztonság, best practice

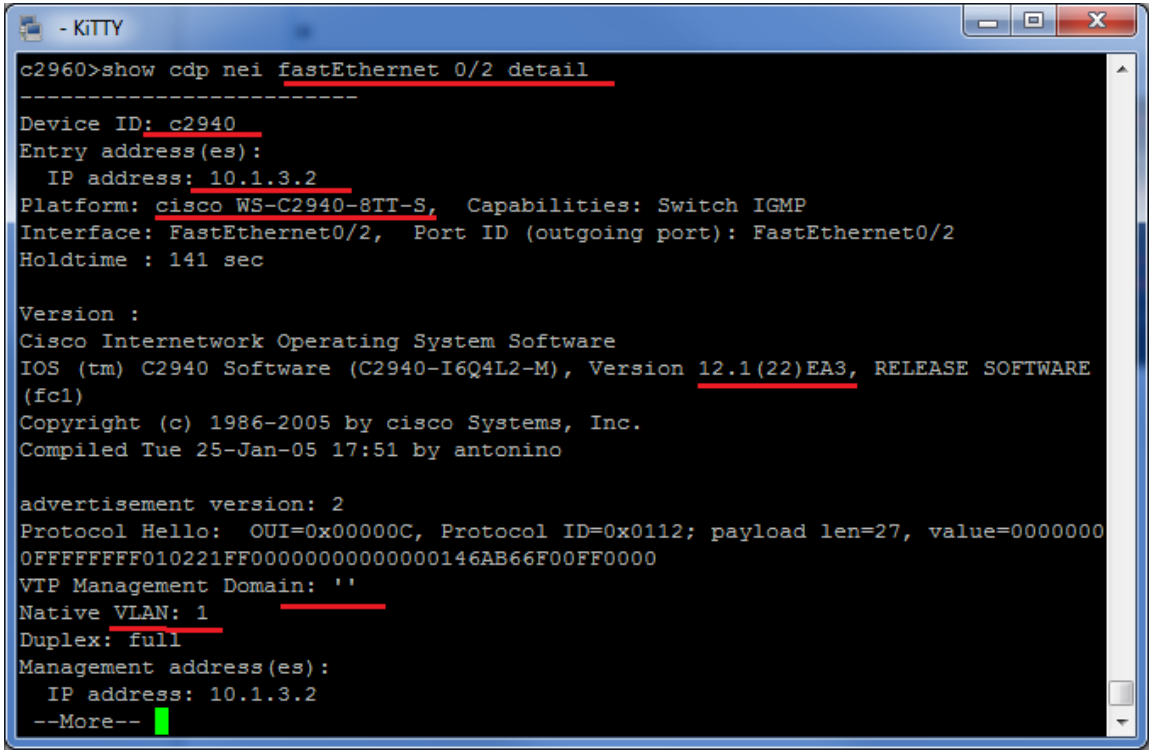
Mai protokollok:

- Vlan
- CDP
- STP
- Etherchannel

CDP

- Nem véletlenül töltöttünk ennyi időt a labor megépítésével, hostnevekkel
- Az első protokoll amit tanulmányozunk: Cisco Discovery Protocol
- Egyszerű, mint a faék: adott időnként információt közöl (counter)
- A letiltáson és időzítésen kívül sokat nem érdemes konfigurálni rajta
- Letiltható globálisan és interfészenként is
- Nem csak Cisco eszközök beszélik
- Nem minden Cisco eszöz beszéli





Smart Vision Solutions
taking you one step ahead

Hol tartunk?

- A rétegek, rétegződés
- Megfelelő fogalmak

Hozzáférések:

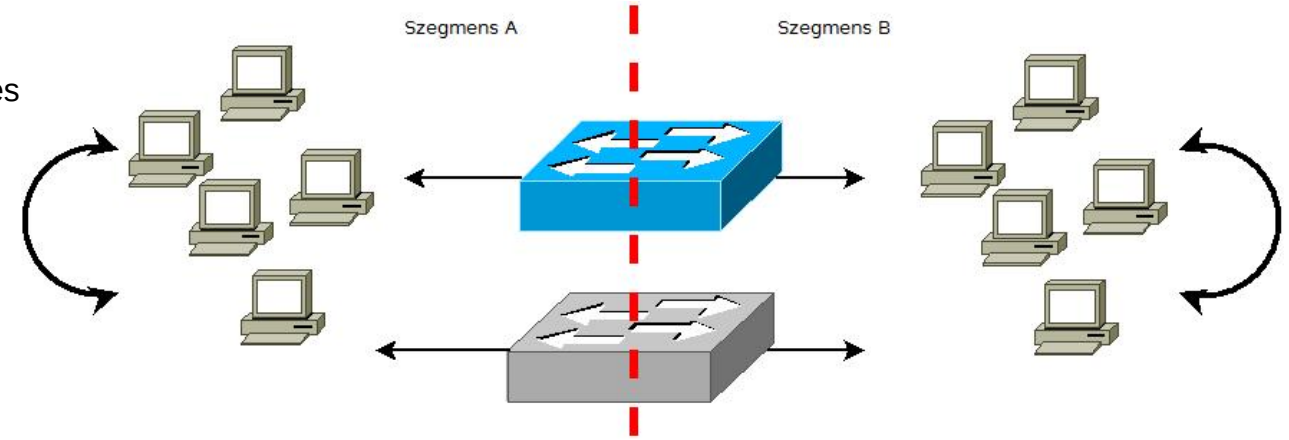
- Helyi
- Távoli
- IP címzés, biztonság, best practice

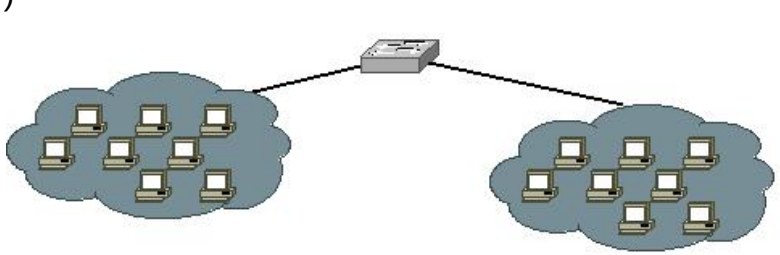
Mai protokollok:

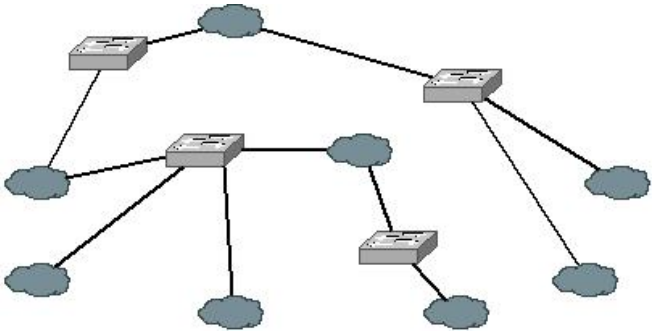
- Vlan
- CDP
- STP
- Etherchannel

STP

- Spanning Tree Protocol
- Hatalmas témakör, több önálló, 90 perces oktatást tartunk róla, önálló laborral
- Kivételesen nem csak Cisco támogatta protokoll (kivéve azokat, amik igen)
- Típusok:
  - klasszikus (802.1d - STP),
  - rapid (802.1w - RSTP),
  - per-vlan (cisco - PVST),
  - per-vlan+ (cisco - PVST+),
  - rapid per-vlan (cisco - RPVST),
  - multiple (802.1s – MST)
- **Na de mire jó?**



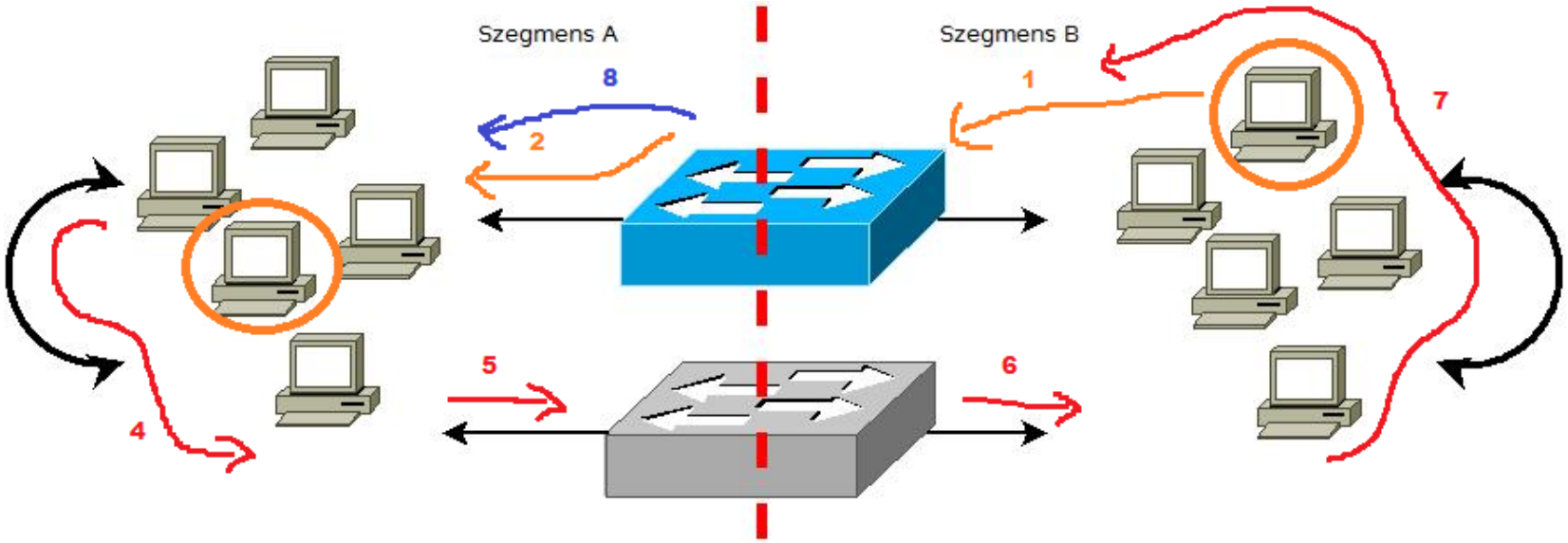




Időben visszamegyünk 1970-be

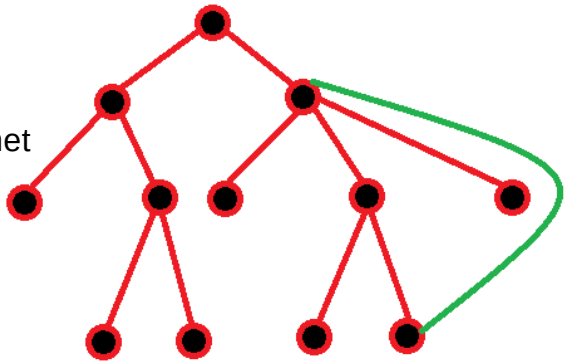
- **hub**: buta eszköz a fizikai rétegben – ami beérkezik azt kiküldi
- **bridge**: nem buta eszköz, MAC címeket tanul meg, csak oda küld ki, ahova kell
- **switchek**: multiport bridge-ek, cut-through vagy store-and-forward elven
- ideális eszköz nagy belső forgalmak elválasztására
- ezáltal **SPoF** is lesz – ha elromlik **szigetek jönnek létre**
- kézenfekvő megoldás lenne **duplikálni**
- ez azonban **végtelen ciklus**t indíthat el és lefekteti a teljes hálózatot

A végtelen ciklus



Vegyünk észre pár dolgot:

- Irreleváns, hogy a kék bridge tudja-e hol a címzett: ha tudja azért, ha pedig nem, azért továbbít
- Irreleváns, hogy a címzett fogadja-e a forgalmat: ha fogadja is, attól a drótról még nem tűnik el
- Ha nem lenne a két bridge összekötve, nem lenne probléma: de nem is adna redundáns védelmet
- A valóságban nem egyetlen pár forgalmaz, sok ezer keret kering a hálózaton másodpercenként
- Pillanatok alatt a használhatatlanságig lassul a hálózat – lásd CSMA/CD működési elve
- Az egész probléma oda vezethető vissza, hogy a hálózat gráfjában kör keletkezett



A STP feladata ezeket a köröket **megtalálni és menedzselni** úgy, hogy egyensúlyt teremtsen a **redundancia** és a **használhatóság** között.

Az STP működése

Fogalmak:

- választások
- BPDU
- MAC address
- prioritás
- root bridge
- port szerepek:
  - root
  - designated
  - non-designated
- port állapotok:
  - **blocking**
    - ha a port nem lenne blokkolva, kör lenne a gráfban. BPDU csere zajlik
  - **listening**
    - BPDU-ra vár, hogy a switch döntést hozhasson
  - **learning**
    - adatforgalom még nincs, de már tanulja a MAC címeket
  - **forwarding**
    - normál adatforgalom
  - **disabled**
    - nem az STP része, lekapcsolt port

A protokoll működése:

- A switchek a portokon BPDU-kkal kommunikálnak
- A BPDU tartalmazza:
  - port információ (sebesség, prioritás)
  - switch információ (prioritás, MAC, időzítők
  - prioritások, vlan információk
- A protokoll először kitalálja, hol legyen a feszítőfa gyökere
- Ha ez megvan, az információt elterjeszti, hogy mindenki kiszámolhassa az optimális útvonalat oda
- Megtörténik a port szerepek kiosztása
- Közben megtörténnek a port állapot-változások
- A hálózat működőképes lesz, mert
  - A protokoll felépített egy feszítőfát, ami körmentes
  - A protokoll megtalálta a hurkokat és ezeket lekapcsolta
  - A protokoll képes arra, hogy topológiaváltás esetén az alternatív útvonalakat engedélyezze
  - Ezáltal minden időpontban pontosan egy útvonal lesz bármely két csomópont között

Az STP implementációk különbségei:

- Az idő, ami a felfedezéshez szükséges
- Az idő, ami a konvergáláshoz szükséges
- A tartalék útvonalak előre kiszámolása
- A lehetséges port állapotok száma
- A szükséges erőforrások mennyisége

Az STP működése (II)

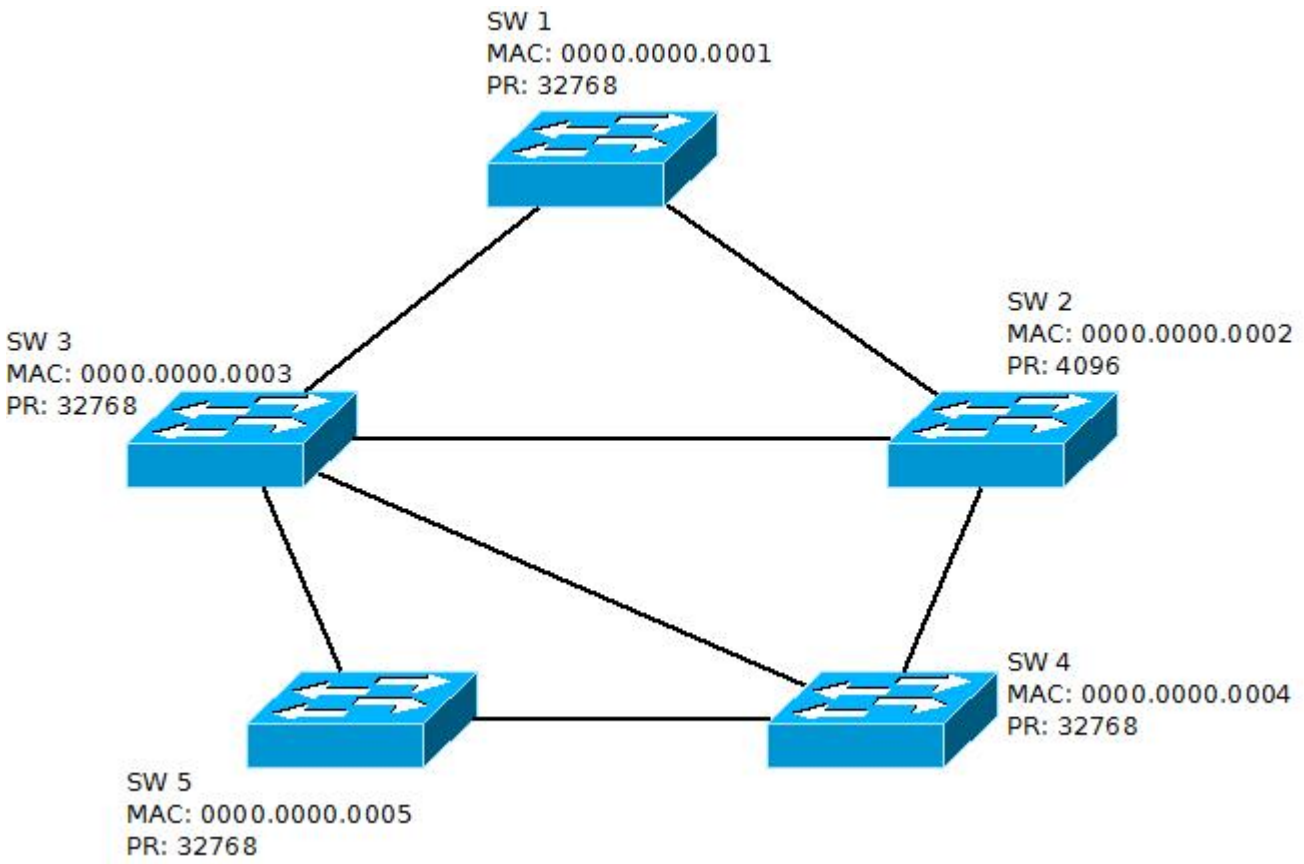
A választás menete

1) Bekapcsolás után minden switch root-nak hiszi magát
2) Teljesen mindegy milyen sorrendben, az egyik switch elkezd BPDU-kat küldözgetni, magát root-nak hirdetve
3) Amennyiben az ezt meghalló másik switch prioritása magasabb számérték, tehát kevésbé root, a hirdetést elfogadja és lemond a saját root szerepéről
4) Amennyiben az ezt meghalló másik switch prioritása alacsonyabb számérték, tehát jobban root, a hirdetés alapján megállapítja, hogy a hirdető tévesen hiszi magát root-nak
5) A következő lépésben mindazok a switchek, amelyek magukat a hallott hirdetéssel szemben jobb root-nak tartják magukat, ezt hirdetni kezdik ugyanúgy, ahogy a korábbi hirdetés történt
6) Azok a switchek akiknek nem osztottak lapot (már a 3. lépésben kiestek a választáson) némán figyelik a nagyok csatáját, mindig feljegyezve a legjobb hallott hirdetés feladóját, mint root switchet
7) Azok a switchek, akik még mindig root-nak hiszik magukat előbb utóbb meghallják a náluk jobb prioritással bíró hirdetéseket és lemondanak a root szerepről

A választás utáni lépések

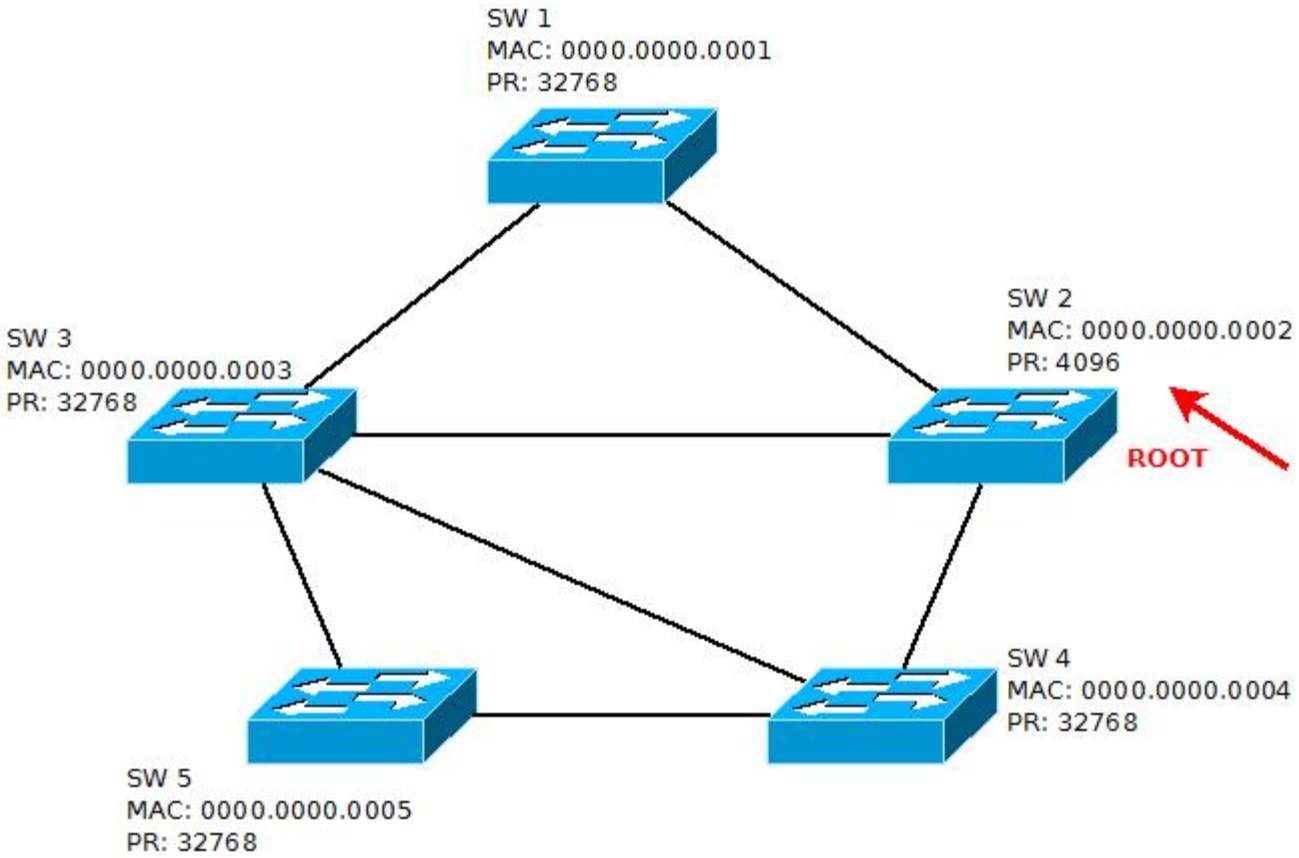
1) Pontosan egy root switch van és mindenki tudja melyik switch ID volt az
2) Minden nem-root switch **kiválaszt egy portot**, amelyik a **root** felé néző port lesz (Root Path Cost alapján)
3) Minden szegmensben a legmagasabb RPC-jű nem-root port designated port lesz (szegmens a kábel a switchek között)
4) Ebből következik, hogy a **root switchen csak designated** port van (mert ő maga a root)
5) A root és designated portok elkezdenek tanulni, majd forgalmazni
6) Minden port ami se nem root, se nem designated, ún. non-designated port, blocking állapotba kerül
7) Ezen a ponton a hálózatban nincs kör, az STP konvergencia befejeződött
8) Ebben az állapotban a switchek a megfelelő portokon továbbra is BPDU-kat küldenek, a blocking port felé is
9) Amennyiben 20 másodpercig nem érkezik BPDU, a switch hibát feltételez és a blocking portot felengedi

Az STP szemléltetése – I.



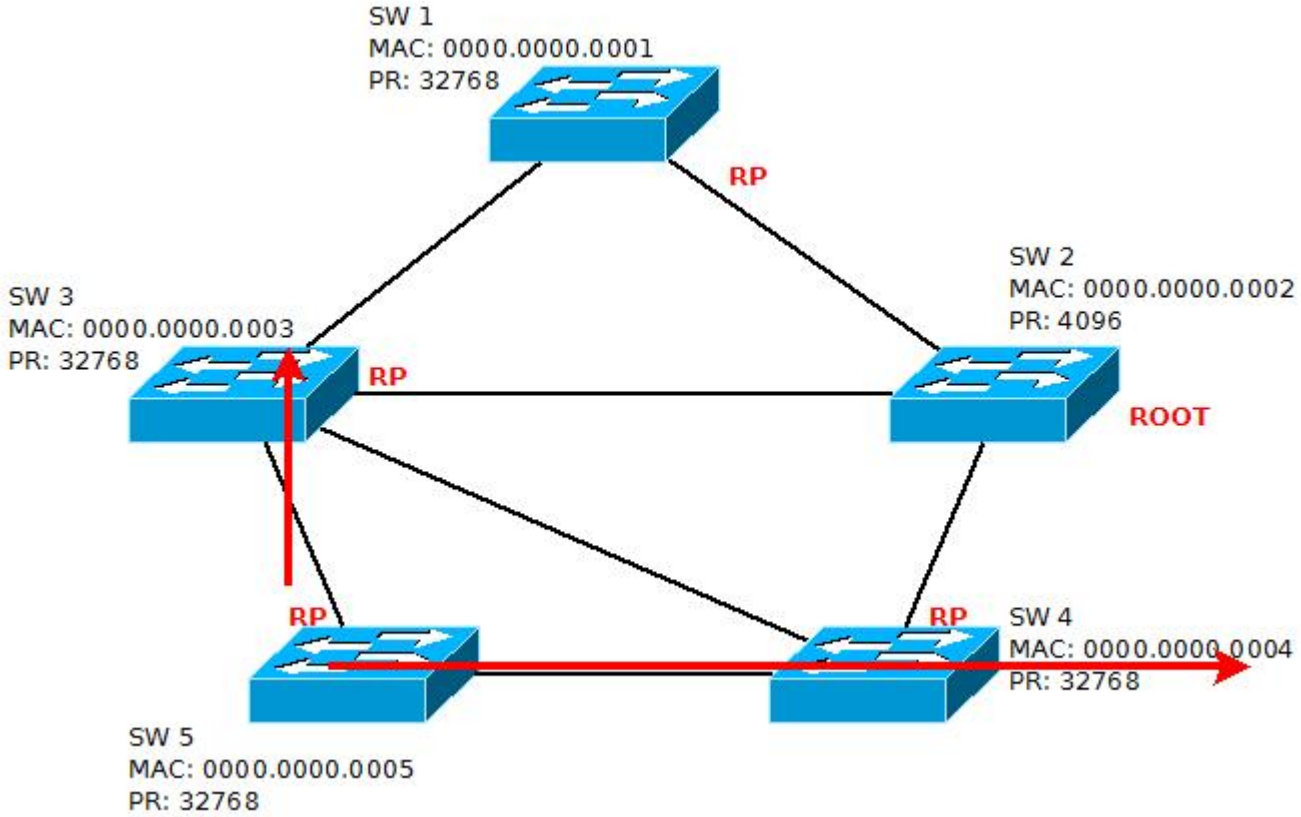
- Kiinduló állapot, mindenki root-nak hiszi magát
- Megkezdődnek a hirdetések (prioritások + MAC címek)
- Látható, hogy SW2 lesz a root, mivel a prioritása neki a legkisebb
- Erre legkésőbb SW5 fog rájönni, mivel ő két ugrásnyira van SW2-től

Az STP szemléltetése – II.



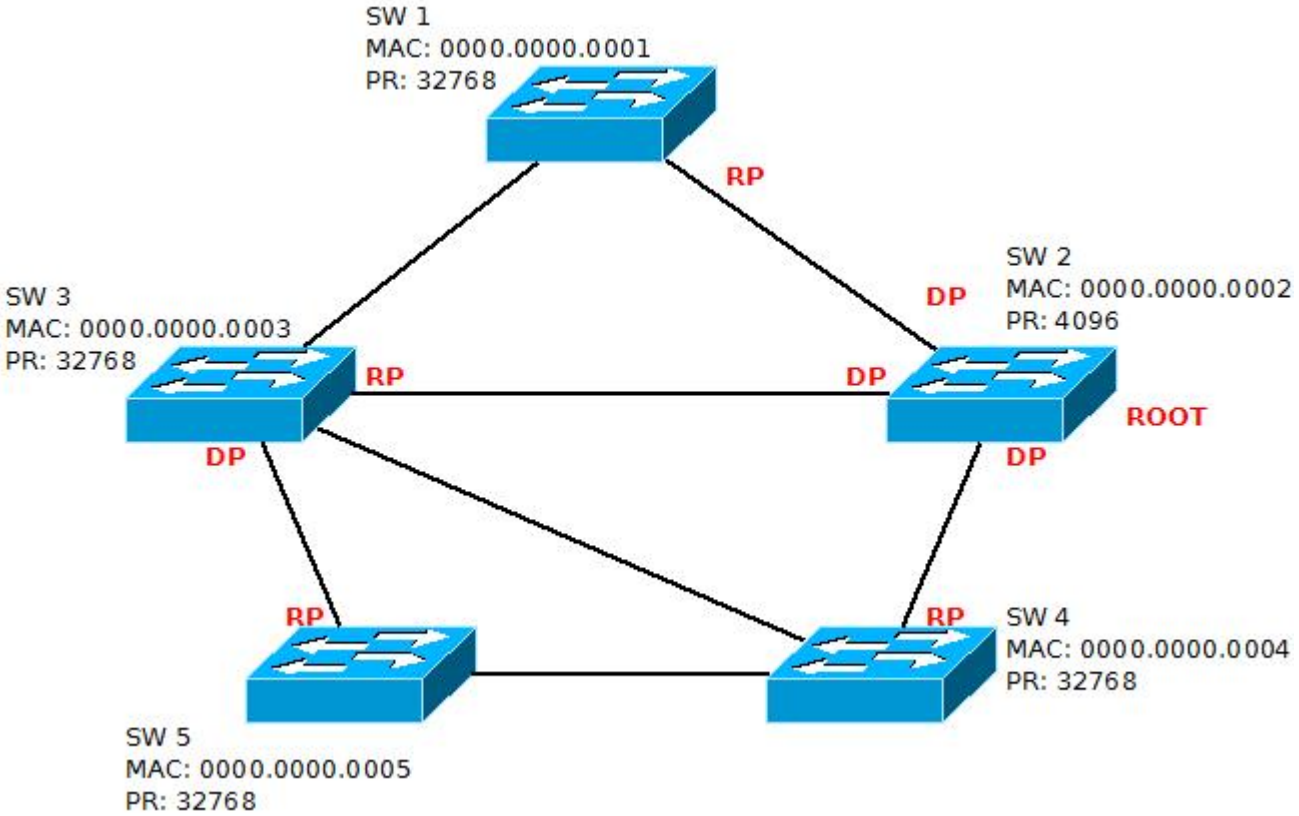
- A nyíl jelöli a prioritás értékét ami miatt SW2 győzött
- A következő lépés a root portok (RP) meghatározása
- Minden switch, aki direktben kapcsolatban áll SW2-vel, automatikusan RP-nek jelöli a portot, ami SW2 felé néz
- Egyedül SW5 nem áll közvetlen kapcsolatban SW2-vel, itt nem triviális, melyik port lesz RP

Az STP szemléltetése – III.



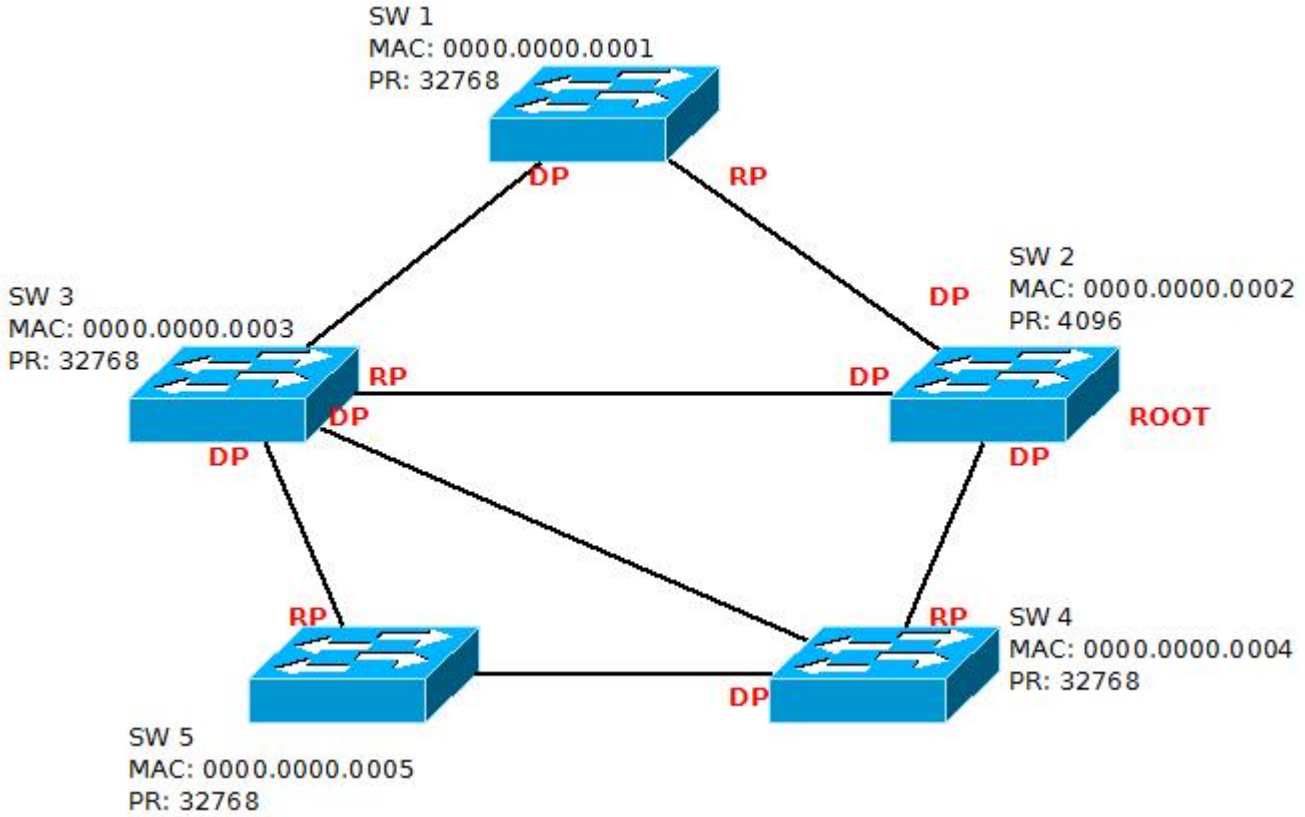
- Az ábrán bejelölve láthatók a root portok
- SW5 a kisebb RPC (Root Path Cost) felé fog RP-t választani
- Mivel ebben a hálózatban minden port egyenlő sebességű (mondjuk 100 mbit/s), a költség mindenhol 19
- Az egyetlen különbség a switchek MAC címe: SW3 jobb, mint SW4, így az RP SW3 felé fog mutatni
- Amennyiben mondjuk SW3 és SW5 között 10 mbit/s lenne a kapcsolat, nyilván SW4 felé lenne az RP
- A következő lépés minden RP-vel szemben egy DP-t jelölni, hiszen az RP-vel szemközti oldal DP lesz

Az STP szemléltetése – IV.



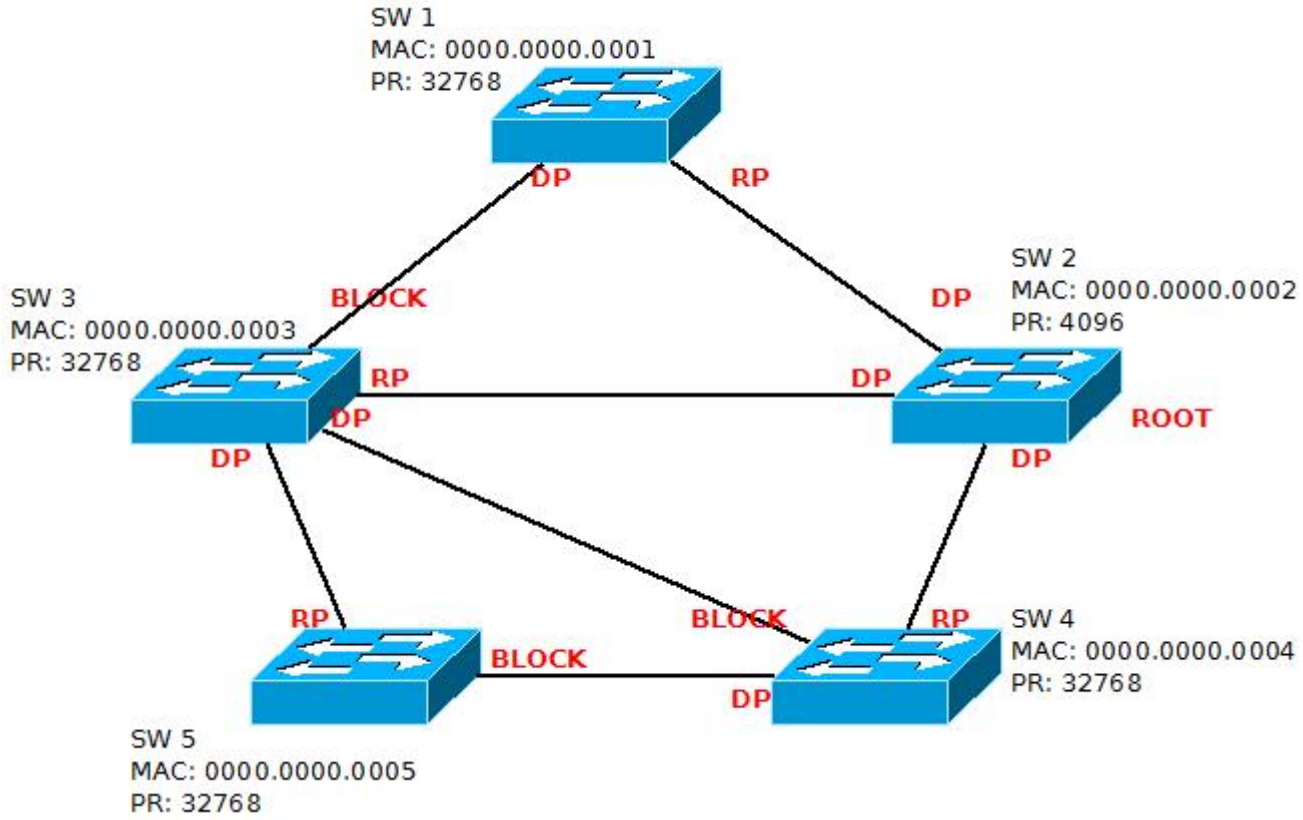
- Minden RP-vel szembeni DP-t megjelöltünk
- Hátra vannak a szerepek kijelölése SW1 és SW3, SW3 és SW4, valamint SW4 és SW5 között
- A fenti három kábel felesleges, mivel mindkét végük olyan switchbe van kötve, aminek már van RP-je
- Az RP egy jobb (gyorsabb, közvetlenebb) kapcsolatot jelöl, tehát ezek a kábelek nem lehetnek jobbak – ilyen volt a kiválasztási algoritmus
- Ezek a kábelek tehát feleslegesek, ezeken valahol blokkolni kell, mert kört okoznak
- A kábelek “jobb” felén tehát DP lesz, a rosszabb felén pedig blokkolás

Az STP szemléltetése – V.



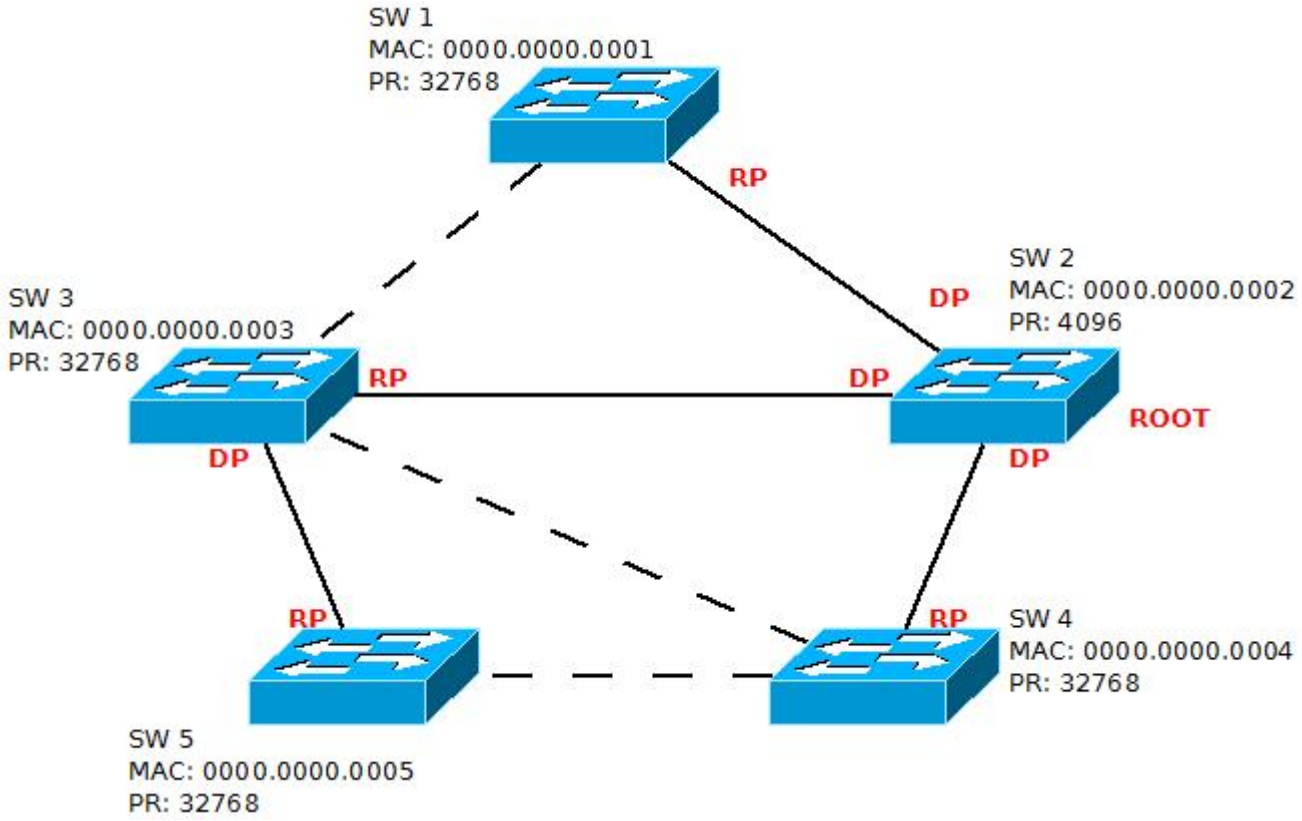
- A három kábelen (SW1 – SW3, SW3 – SW4, SW4 – SW5) bejelölve a “jobbik” oldal, ahol DP lesz
- A velük szemközti portok lesznek blokkolva

Az STP szemléltetése – VI.



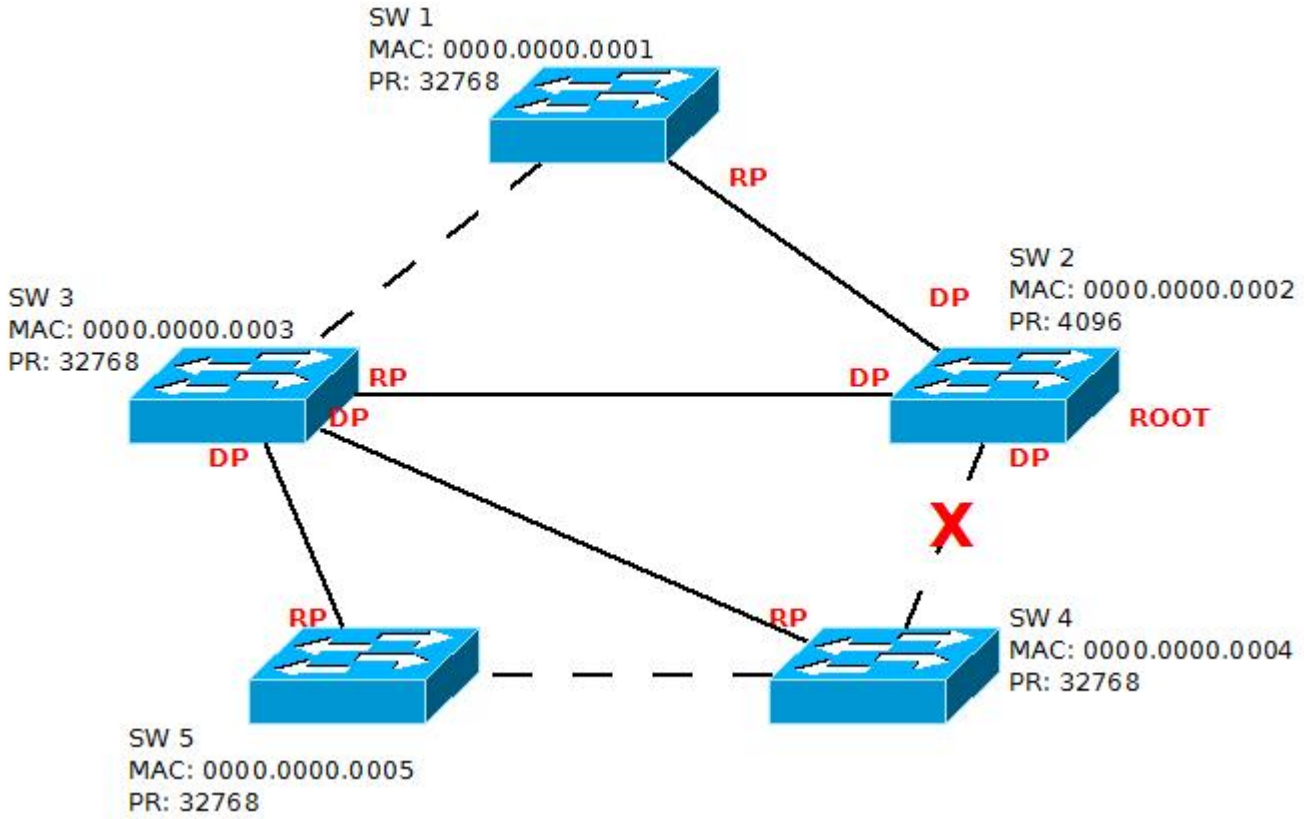
- Megjelölve minden port, a blokkolt portok is
- Ezzel a topológiát a switchek feltérképezték a küldött BPDU-k segítségével
- Összeállt a végleges feszítőfa, amely már nem tartalmaz kört

Az STP szemléltetése – VII.



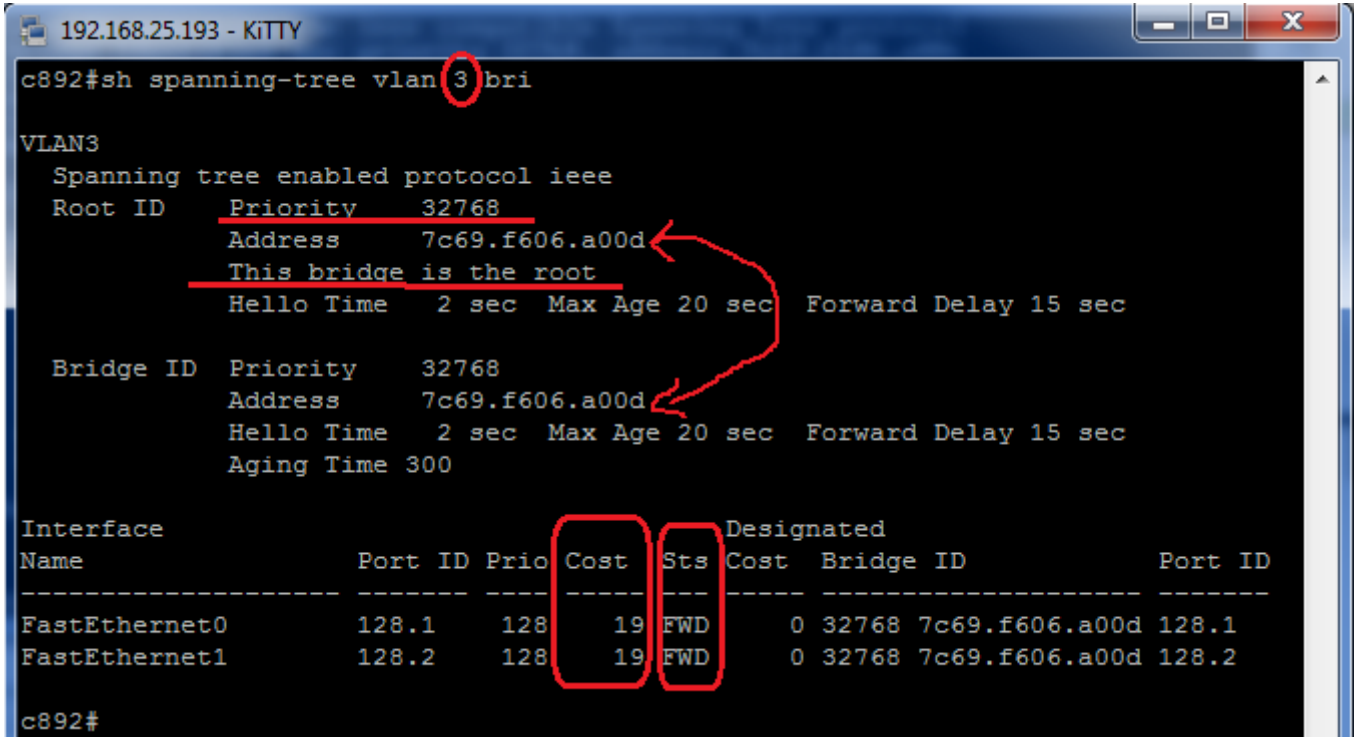
- A szaggatottal jelölt kábeleket a switchek egy oldalon blokkolták, szakadást okozva
- A folyamatos vonalon zajlik a hálózati forgalom, az STP konvergencia végetért
- Pontosan látható, hogy a root switch választás kritikus fontosságú
- Ha nem állítjuk be kézzel a prioritásokat, a MAC címek győznek
- Előfordulhat, hogy egy csoffadt, régi switch nyeri a root címet, rajta megy át minden forgalom
- Ezzel esetleg meg sem tud küzdeni: lefagy, újraindul, instabil lesz
- A root switch kritikus fontosságú, ha kiesik,
  átmenetileg izolált szigetekre szakad a hálózat
- Nézzük meg, mi történik kábelhiba esetén?

Az STP szemléltetése – VIII.



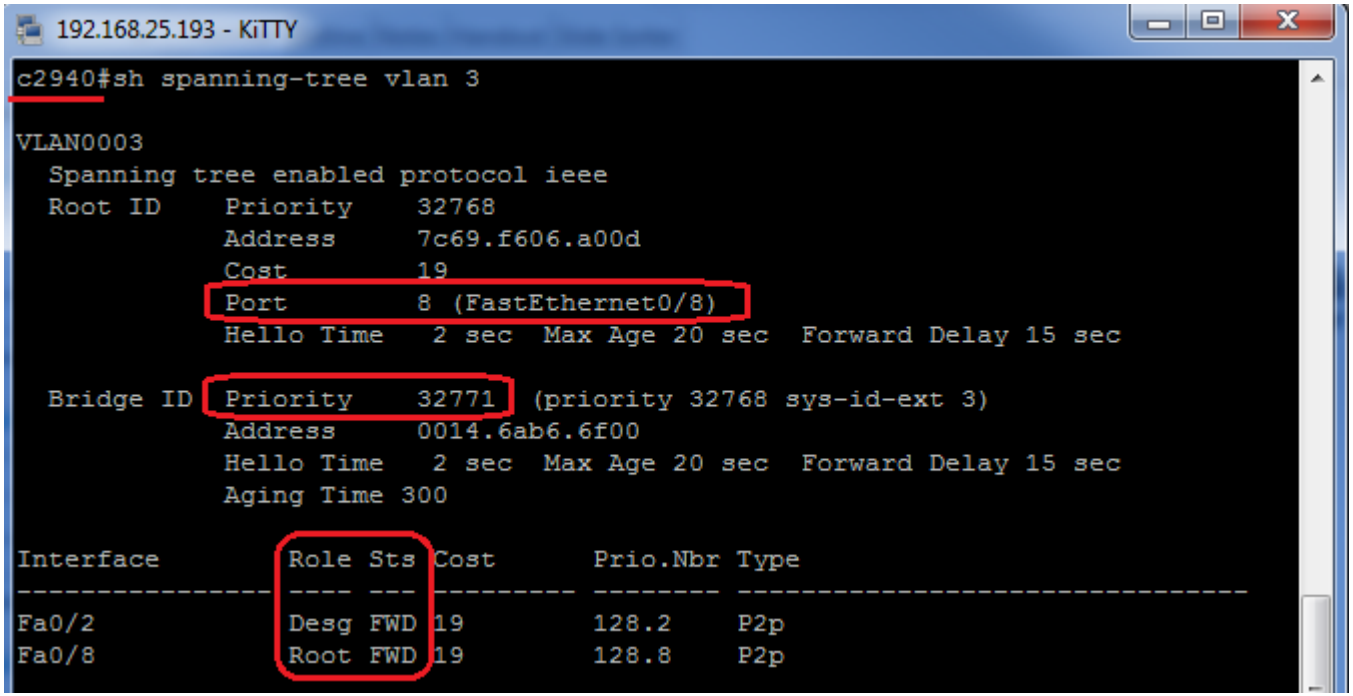
- A piros X jelzi a kábelhiba helyét, itt eredetileg ment forgalom
- A szakadás pillanatától kezdve SW4 nem kap BPDU-kat SW2-től
- Viszont továbbra is kap BPDU-kat SW3-tól és SW5-től
- A dead timer lejárta után (20 mp) SW4 szakadtnak nyilvánítja a hibás kábelt
- Ezzel egy időben hallgatózni kezd, hogy a két alternatív útvonal közül melyiket válassza
- A sebességek, prioritások egyformák, így a MAC dönt: SW3 felé lesz az új RP
- SW4 felengedi a korábban SW3 felé blokkolt portot, további kb. 10-15 mp után a hálózat megjavította magát
- Szemmel láthatóan SW3 a jó döntés, SW5 csak egy felesleges extra ugrás a root switch irányába

Az STP szemléltetése – IX.



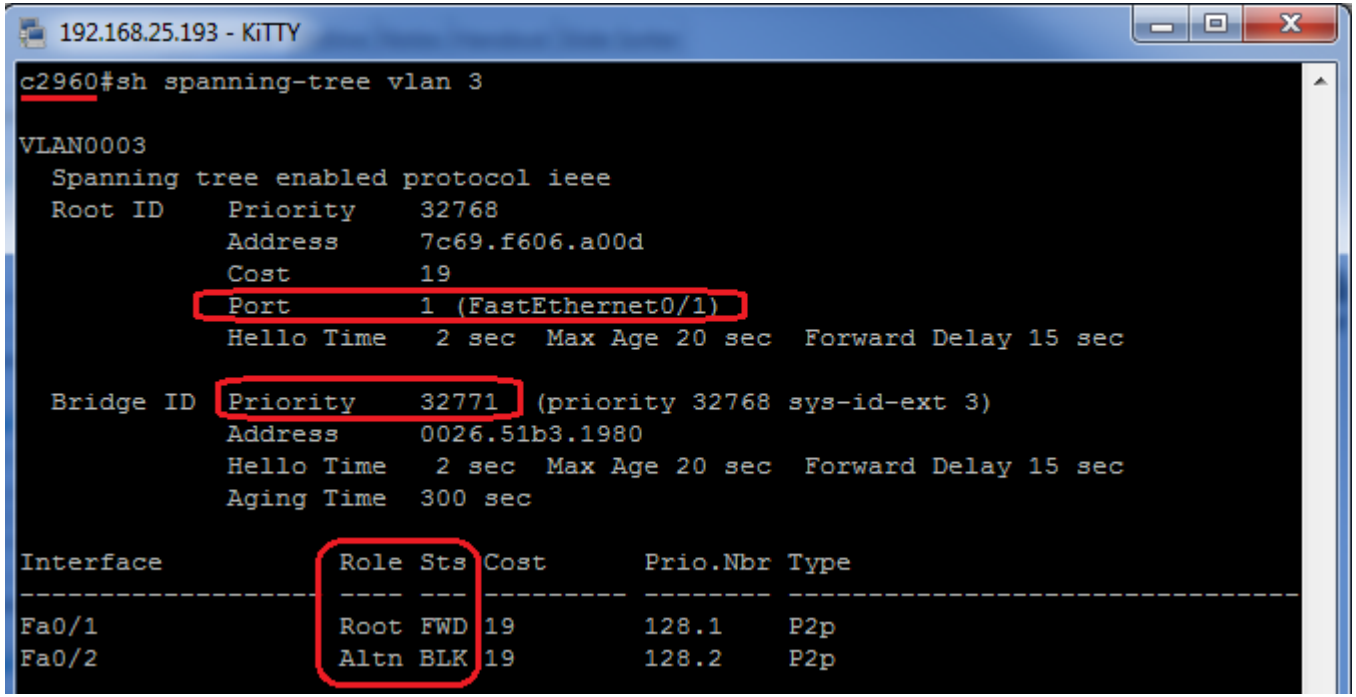
- Látható, hogy csak egy VLAN-ra történt lekérdezés
- Klasszikus STP fut (protocol ieee)
- A root ID és a saját ID megegyezik, azaz mi vagyunk a rootok
- Látható, hogy a FastEthernet (100 mbit/s) költsége 19
- Mindkét switchport forwarding állapotban van
- Láthatóak a számlálók: hello, max age, forward delay
- Érdekesség: miért nem szerepel a Gigabit 0 port a listában?
- A Gigabit 0 port nem switchport, hanem ún. routed port, azaz harmadik réteg-beli port
- A STP egy második réteg-beli protokoll, nem fut routed portokon

Az STP szemléltetése – X.



- Ugyanez a 2940-es switch nézőpontjából: a root switch a Fa 0/8 porton át érhető el
- Látható lent, hogy az RP is a Fa 0/8
- Érdekes megfigyelni a prioritást, ez nem más, mint a default (32768) plusz a vlan ID (3)

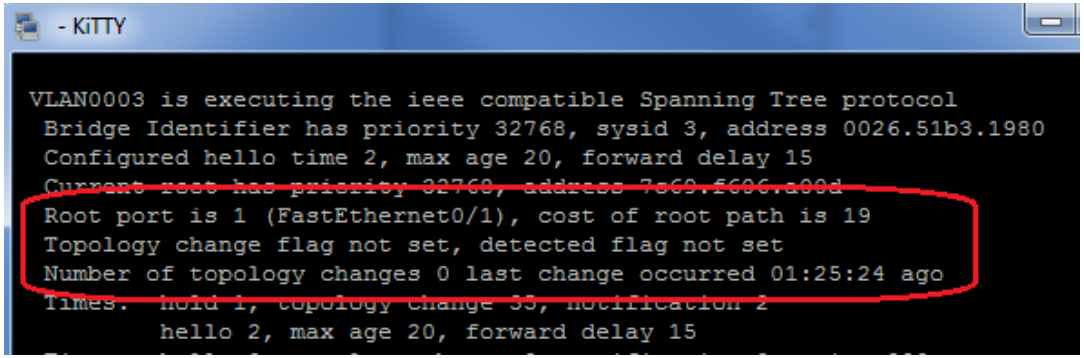
Az STP szemléltetése – XI.



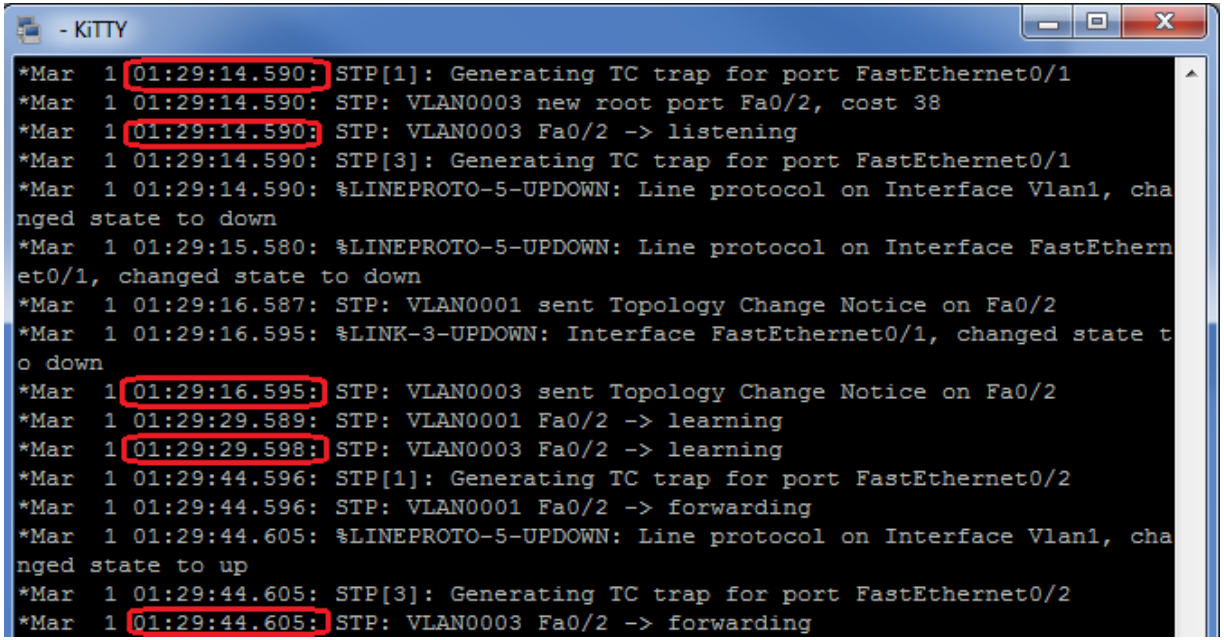
- Ugyanez a 2960-es switch nézőpontjából: a root switch a Fa 0/1 porton át érhető el
- Látható lent, hogy az RP is a Fa 0/1
- A prioritás itt is látható, hogy a default plusz a vlan ID értéke
- A lényeg pedig a Fa 0/2 port, amit ez a switch blokkolt, mint alternatív útvonalat, mert nincs rá szükség

Az STP szemléltetése – XII.

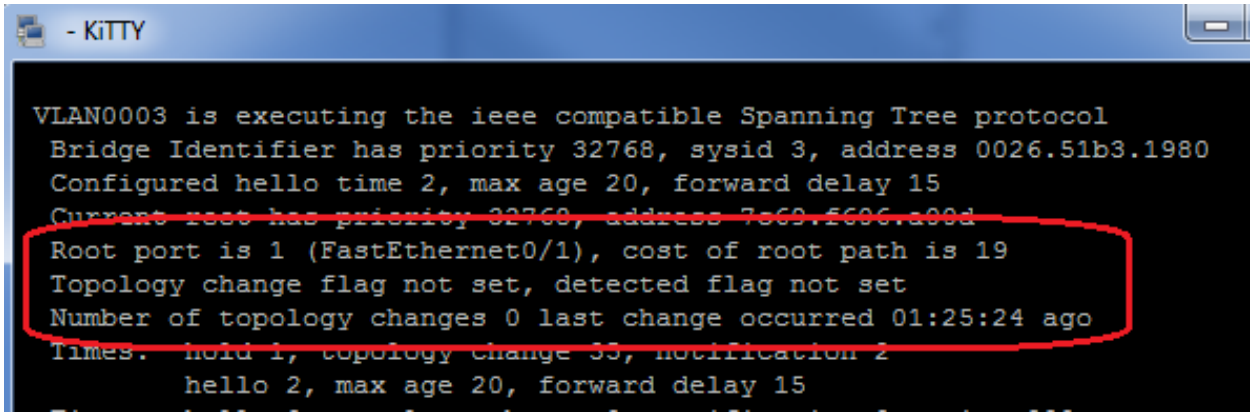
- Hibát okozunk
- A 2960-as switch 0/1 portja RP, 0/2 portja blokkolt stabilizálódott állapotban
- Fizikailag megszakítva a kábelt a 0/1 porton megnézzük mi történik
- Látható a hiba előtt, 1 órája és 25 perce nem volt topológia változás



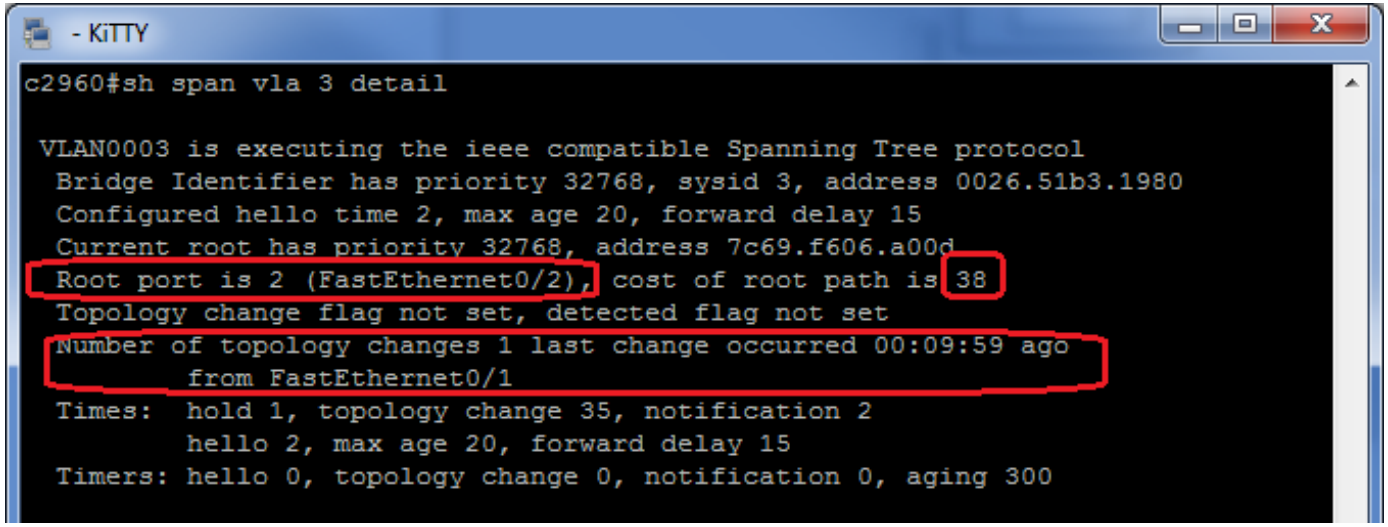
- Kábelhiba 01:29:14-kor
- Nem kell BPDU-ra várni, mivel itt helyben egy interfész állapotváltozás történt, nem kell megvárni a timeout értéket
- t+0 mp -kor a switch elkezdi hallgatni a forgalmat, BPDU-k után kutatva (listening állapot)
- t+2 mp -kor a switch értesíti a közvetlen szomszédokat a hibáról (nekik se kelljen várni)
- t+15 mp (forward delay) -kor a switch elkezdi tanulni a forgalmat (learning állapot)
- t+30 mp -kor a tartalék port üzembeállítva, mint a jelenlegi legjobb megoldás



Az STP szemléltetése – XIII.



- Érdekes összehasonlítani az előtte, utána állapotokat
- A Root Port a 0/2 lett
- A topológia váltás 9:59 azaz kb 10 perce történt, a 0/1 porton
- Látható, hogy a költség a duplájára nőtt, 19-ről 38-ra, azaz az előzőhöz képest egy szuboptimális, de amúgy remekül működő állapotra jutottunk



Smart Vision Solutions
taking you one step ahead

Az STP jellemzői

- Menet közben **folyamatos** a kommunikáció **minden porton**
- A **blocked port** csak adatforgalmat nem engedélyez, **BPDU-k jönnek-mennek** rajta
- Bármilyen kábelhiba, szakadás valahol BPDU **hiányt** idéz elő
- A BPDU hiány **20 mp**. múlva STP konvergenciát indít el
- Ekkor a blokkolt portok felengedése kezdődik el, **tanulási** folyamat mellett
- A **teljes** hálózati kiesés a felhasználóknak **kb. 50 mp**, ez a BPDU timer (20 sec) és a tanulási idő (2x15 sec)
- Üzleti környezetben ez **nem tolerálható** (= rapid STP, amely gyorsabban konvergál)
- A klasszikus STP **nem vette figyelembe** a VLANokat (látható, hogy a vlan 1 és vlan 3 topológiája megegyezik)
- A PVST, PVST+ minden VLAN-ra **külön-külön** futtat STP-t amik különbözőek lehetnek
- Sok VLAN esetén (sok száz, néhány ezer) ez **rendkívül** erőforrás-igényes
- Ez vezetett az MST-hez (nem VLAN-onként, hanem **VLAN csoportonként** van STP)

Előnyök:
- Jelentkezzen, aki **hibától számítva** kb. **30-50** mp alatt **azonosít és megjavít** egy kábelezési hibát
- **Dinamikus** alkalmazkodás **automatikusan** a mindenkori legjobb helyzethez (sebesség, stb)
- Mostantól **bármikor** ha egy kábelt ki akarsz húzni, **bátran**, legfeljebb kb. 50 mp után helyreáll minden
- Nem kell a javításokkal, átkábelezésekkel többet munkaidő utánra várni, **csökkenhet a túlóra**

Hátrányok:
- Nem triviális protokoll, **komplex hibák forrása lehet**
- A 30 másodperc kiesés is sok lehet, **a konvergencia lassú**
- **Tervezést, odafigyelést** igényel a bevezetése, elkerülendő a nemkívánt root switch választási eredményeket
- **Minden** switchport **minden** alkalommal az első 30 másodpercben tanul, **nem lehet forgalmazni** (windows boot)
- Együttműködés más gyártók switcheivel **problémás lehet**
- **Minden** eszköznek támogatnia **kell**, hogy valóban hurokmentes legyen a topológia
- Az extra kábelek és extra portok extra pénzbe kerülnek és ezek **az idő nagy részében kihasználatlanok**

Hol tartunk?

- A rétegek, rétegződés
- Megfelelő fogalmak

Hozzáférések:

- Helyi
- Távoli
- IP címzés, biztonság, best practice

Mai protokollok:

- Vlan
- CDP
- STP
- Etherchannel

Etherchannel

- Szusszanjunk egy kicsit, nehéz témán vagyunk túl
- Az STP, a különböző verziók, timerek, implementációk miatt egy bonyolult protokoll, néhány hátránnyal
- Ezeket a hátrányokat felsoroltam az előző fejezet végén
- Egy hátrányára fókuszálunk most, ez egy koncepcionális gyengeség
- Az STP de facto azt jelenti, hogy olyan kábelek vannak a rendszerben, amik (ha minden jól megy) sosem kerülnek használatba (blokkoltak)
- Ezek a kábelek pénzbe kerültek (megvenni), időbe kerültek (kiépíteni)
- A switch portok amelyekbe bele vannak dugva, szintén pénzbe kerültek
- És ott ül kihasználatlanul, miközben a működő kábel esetleg vörösen izzik a nagy forgalomtól
- **EZ PAZARLÁS**
- Milyen szuper lenne, ha a ki nem használt kábeleket is valahogy használni lehetne

Etherchannel

- Az etherchannel (esetleg port channel) lényege pontosan az, hogy több fizikai kábelt fogjunk egy marokba és kezeljük logikailag egy nagy kábelnek (nagy = kétszer, n-szer olyan gyors)
- Amennyiben két, három, akár nyolc fizikai kábelt egy logikai vastag, nagy kábelnek tekintünk, kétszer, háromszor, nyolcszor akkora forgalmat vihetünk át rajta
- ÉS! Ha egy kábel hibás lesz, megszakad – akkor a vastag kábel kevésbé lesz vastag, de még mindig üzemelni fog és nem vesztünk forgalmat
- Értelemszerűen a kábel mindkét oldalán lévő eszköznek támogatnia kell
- De támogatja is szinte mindenki: minden hálózati eszköz (switch, tűzfal), linux, windows egyaránt
- Szerver oldalról ismerős lehet: bonding, grouping, trunking (ez utóbbi félrevezető, mivel a több VLAN-t hordozó portot nevezik a hálózati világban trunk-nek)
- Természetesen itt is több protokollról beszélünk
  - LACP – Link Aggregation Control Protocol (IEEE 802.3ad)
  - PAgP – Port Aggregation Protocol (Cisco)
- Mindkettő ugyanarra való, PAgP csak Cisco eszközökben, LACP viszont bármiben van ahova implementálták
- Nyilván a kettő egymással nem kompatibilis (PAgP az egyik oldalon, LACP a másikon nem fog menni)

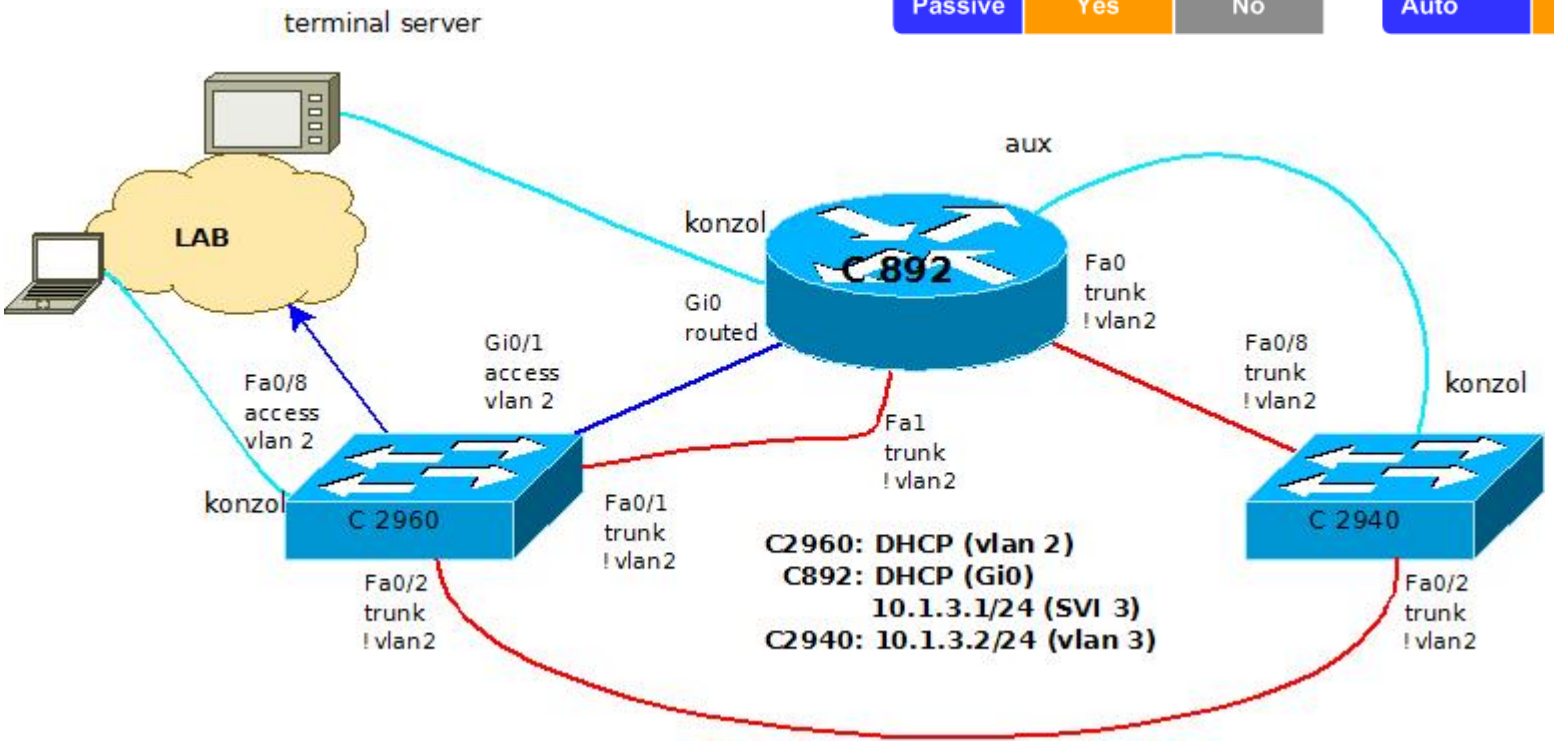
Gyakorlat - Etherchannel

- Az eddigi hálózat kiegészül egy újabb kábellel: c2940 és c2960 közé, Fa 0/3 kerül összekötésre
- Ez Fa0/2 -vel fog párban etherchannel-t képezni

Will an EtherChannel Form?

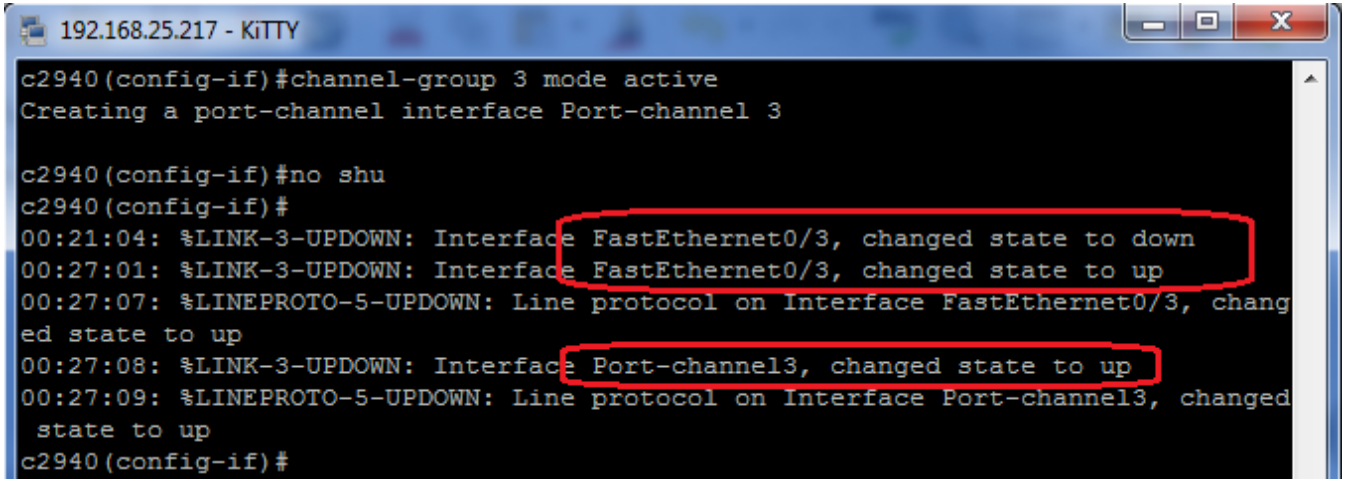
LACP	Active	Passive
Active	Yes	Yes
Passive	Yes	No

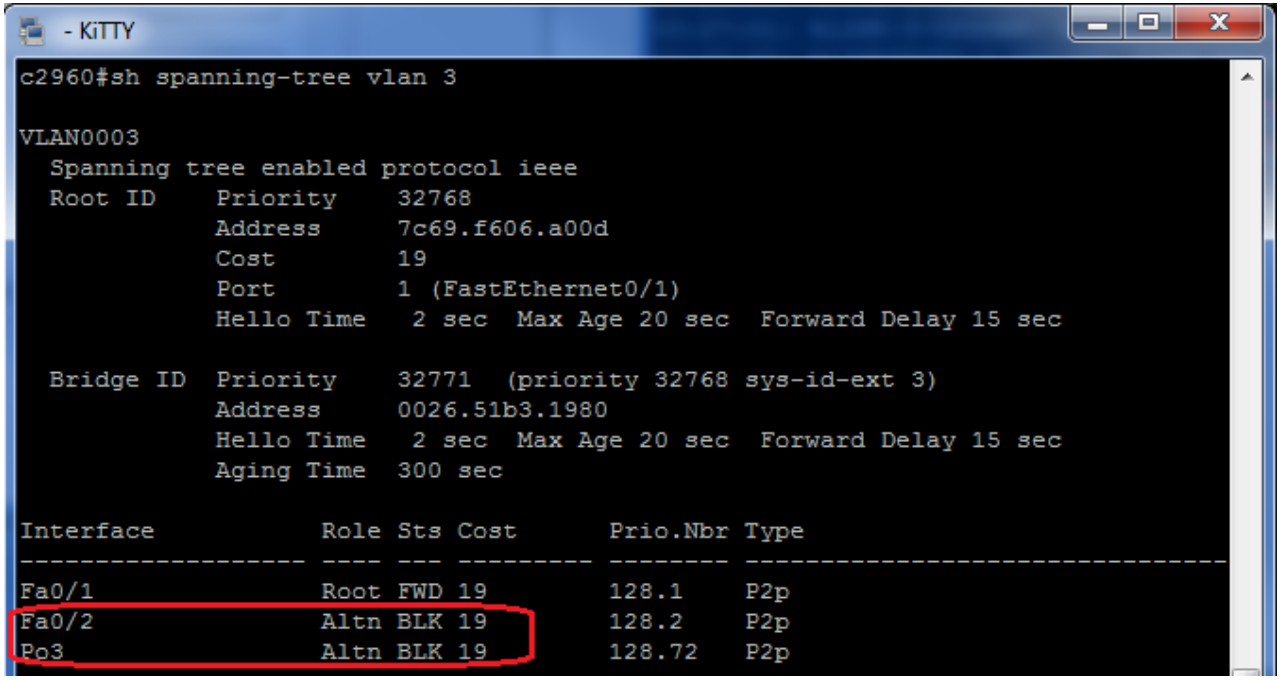
PAgP	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No



Smart Vision Solutions
taking you one step ahead

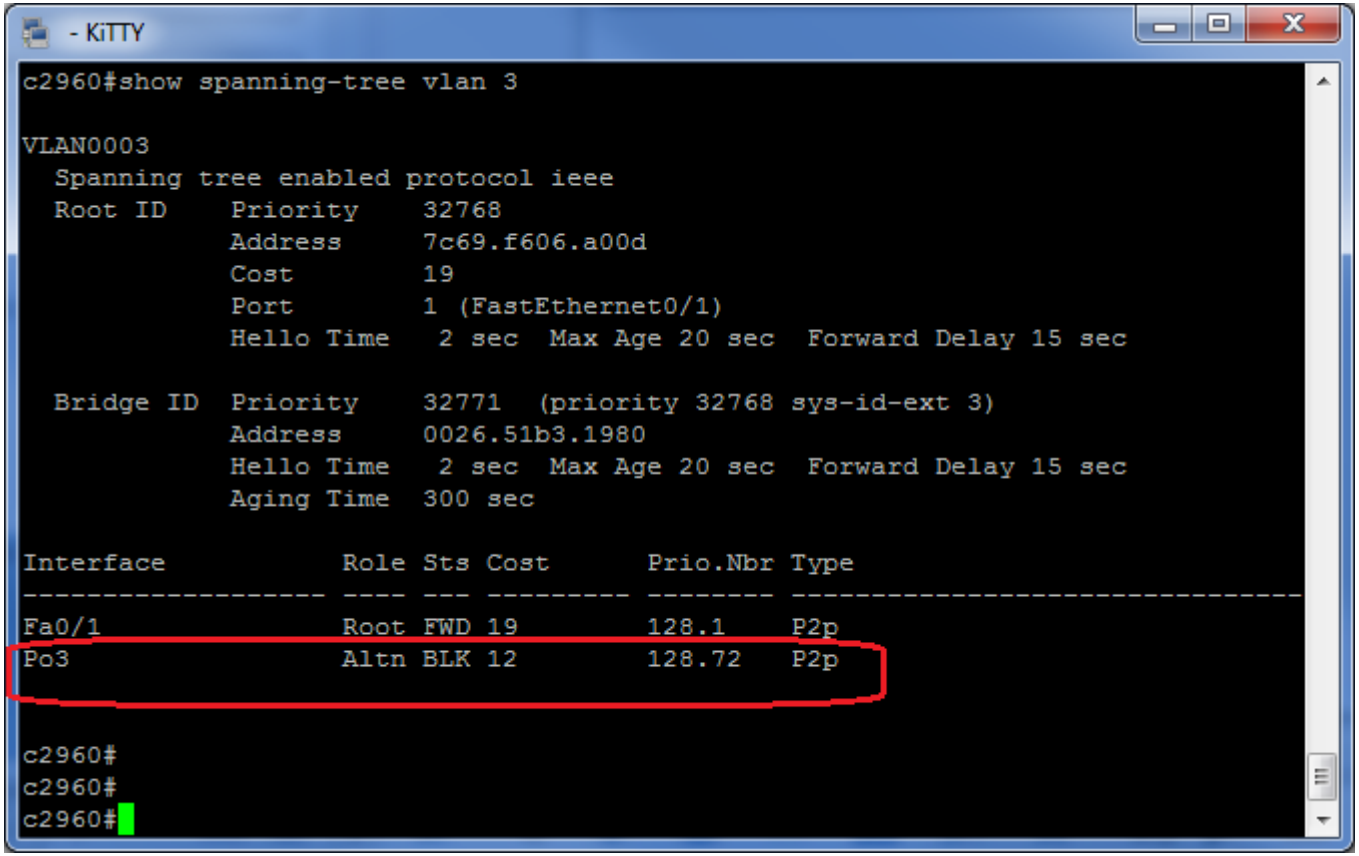
Gyakorlat - Etherchannel





Smart Vision Solutions
taking you one step ahead

Gyakorlat - Etherchannel



- Látható, hogy már csak egy link van blokkolva, nem kettő
- Az is látható, hogy a költség lecsökkent 19-ről (100 mbit/s) 12-re (200 mbit/s)
- De továbbra is blokkolva van. Ez, ha átgondoljuk, nem hiba. Miért is?
- Ha aktív lenne, akkor a root switch-ig a költség 19 + 12 lenne, ennél a 19 jobb!

Etherchannel - gondolatok

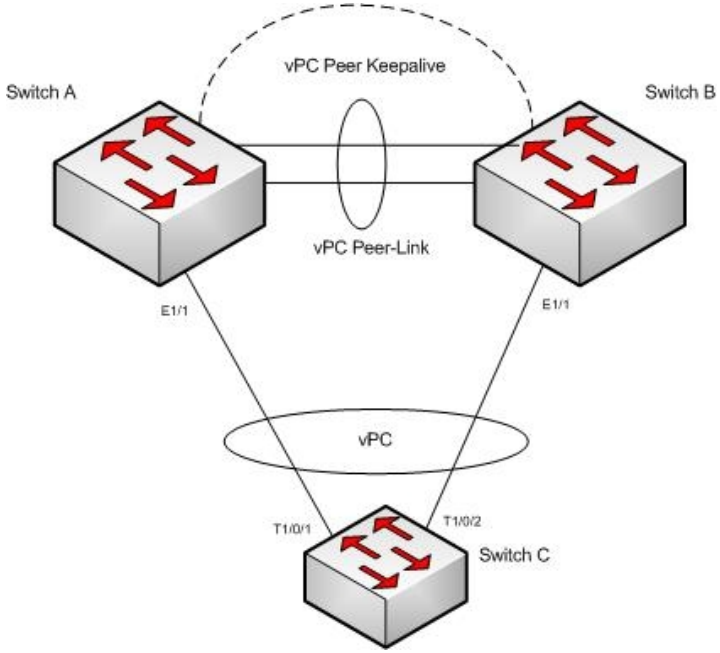
Speed	Port Cost	Comment
10 Mbps	100	Ethernet
20 Mbps	56	EtherChannel
30 Mbps	47	EtherChannel
40 Mbps	41	EtherChannel
50 Mbps	35	EtherChannel
54 Mbps	33	802.11 wireless
60 Mbps	30	EtherChannel
70 Mbps	26	EtherChannel
80 Mbps	23	EtherChannel
100 Mbps	19	Fast Ethernet
200 Mbps	12	Fast EtherChannel
300 Mbps	9	Fast EtherChannel
400 Mbps	8	Fast EtherChannel
500 Mbps	7	Fast EtherChannel
600 Mbps	6	Fast EtherChannel
700 Mbps	5	Fast EtherChannel
800 Mbps	5	Fast EtherChannel
1 Gbps	4	Gigabit Ethernet
2 Gbps	3	Gigabit EtherChannel
10 Gbps	2	10G Ethernet
20 Gbps	1	20G EtherChannel
40 Gbps	1	40G EtherChannel

- A táblázatban láthatóan az alapértelmezett STP cost értékek az egyes interfész sebességekhez
- Érdemes emlékezni rá, hogy egy szint felett már nincs eltérés, a 20Gbit és 40 Gbit linkek között nincs költség különbség
- Érdemes emlékezni arra is, hogy a sebesség nem minden – az 54 mbites wifinek a költsége jobb, mint az 50 mbites drótnak, de valóban jobb?

- Az etherchannel egyik koncepciója a rendelkezésreállás (redundancia) növelése (pl. szerverek, NASok esetén)
- Mégis hogyan növeli a redundanciát, ha az etherchannel mindkét portja ugyanabban a switchben van?
- A switch maga is SPoF

- Kézenfekvő igény lenne az etherchanneleket különböző switchekben végződtetni

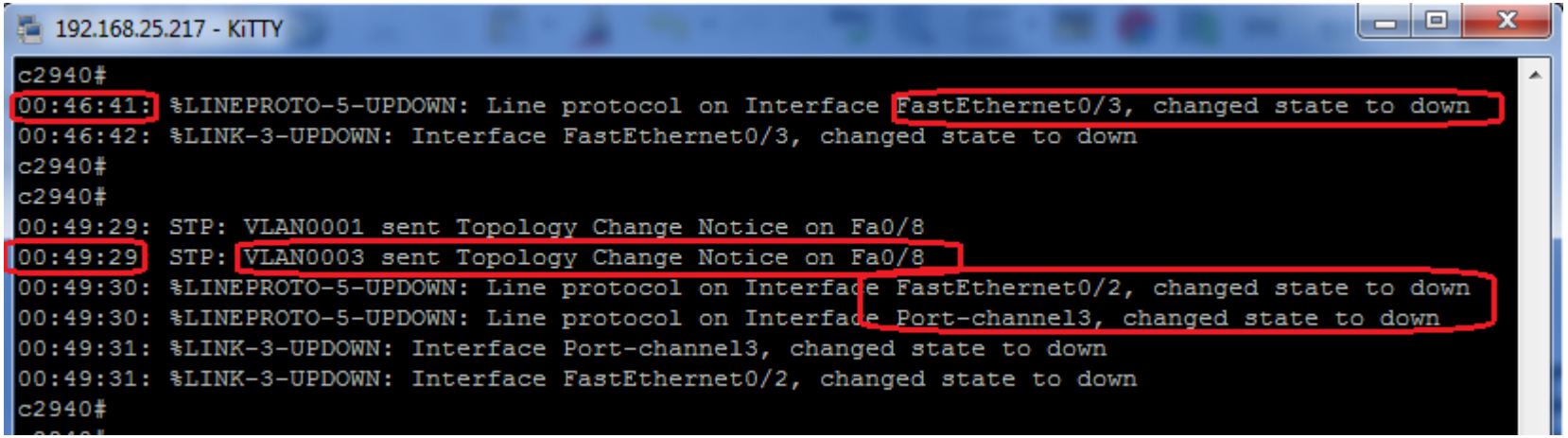
- Erre két lehetőség van:
  stack vagy VPC



Smart Vision Solutions
taking you one step ahead

Gyakorlat - Etherchannel

- Hibát okozunk a hálózaton – elsőként a 0/3 portot húzzuk ki, majd a 0/2 -t is
- Első hiba: nincs topológia változás, csak a sebesség csökken 200 mbit-ről 100 mbit-re (költség 12 → 19)
- Második hiba: itt már van topológia változás, ekkor számítunk csak STP üzenetek megjelenésére



Tanulságok, best practice:

- Az etherchannel úgy működik ahogy vártuk – addig transzparens minden hiba amíg legalább egy kábel jó
- Ez azonban nagyobb felelősséget ró a monitorozásra. Figyelni kell minden kábelszakadást, jobban, mint korábban, mert tényleges hibát már csak akkor kapunk, mikor az utolsó is megszakad.
- Monitorozni kell a kihasználtságot is – két 100 mbites kábel 150 mbit forgalma nem fog elférni egy kábelen
- Csökkent teljesítmény, csomagvesztés várható a hirtelen megjelenő 150%-os igény miatt
- A hálózati problémák detektálása komplexebbé válik (hibás kábel csak minden második csomagot érint)

Felmerülő kérdés:

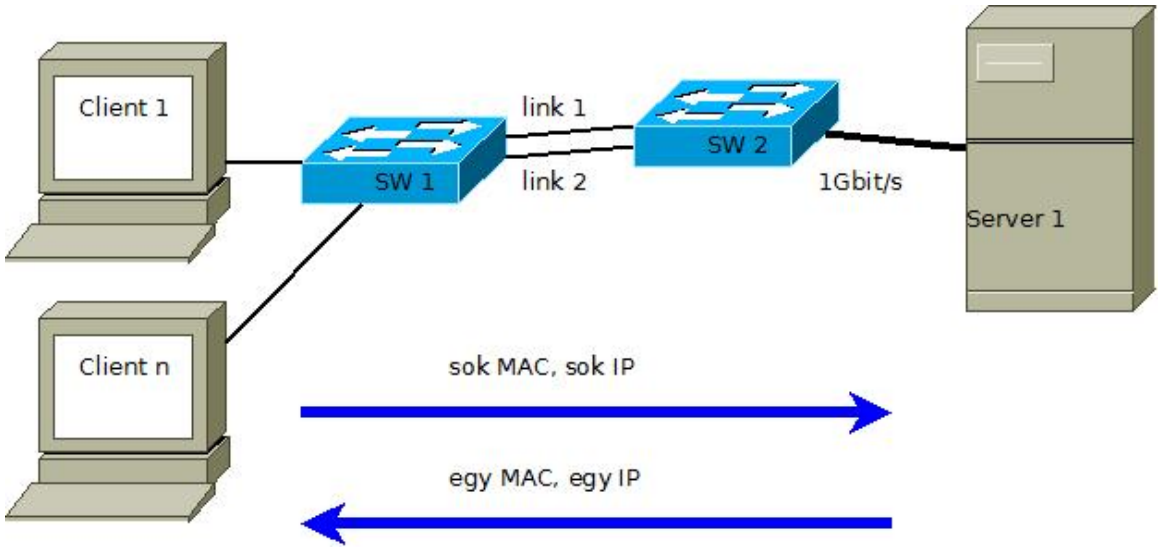
- Mitől függ, hogy mikor melyik kábelt használja a forgalom?
- Hibás, szakadozó kapcsolatot hogy lehet detektálni?

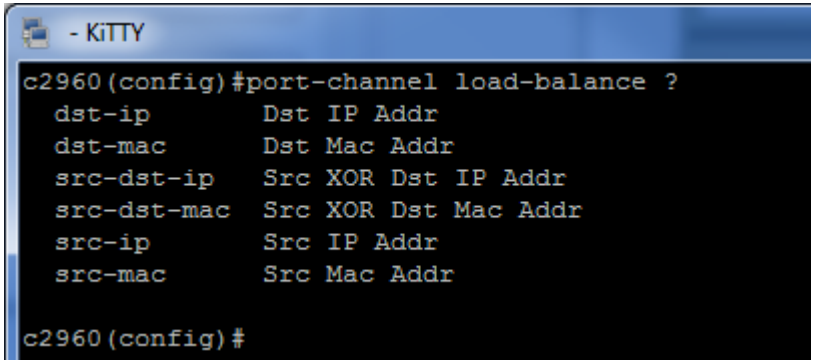
Etherchannel alkalmazása

A terhelés eloszlása:

- A lehetőségek platformtól és operációs rendszertől függnek
- Terhelés elosztás alatt azt értjük itt, hogy milyen módon osztja el a switch, melyik keret melyik porton mehet
- Még a legkisebb switch is támogat több fajta hashing algoritmust, amely eredménye egy port szám amin a keret kimehet
- A döntés alapozható: MAC címre, IP címre, esetleg TCP/UDP portszámra, valamint ezek keverékére
- Figyelembe lehet venni forrás oldalon vagy cél oldalon
- Át kell gondolni, melyik a valóban hasznos, ehhez ismerni és érteni kell a tipikus forgalmi modelleket

- Ha sok kliens forgalmaz ugyanahhoz a szerverhez (sok különböző forrás MAC, ugyanaz a cél MAC)
- A válasz pedig mindig ugyanarról a MAC címről és IP címről jön
- Akkor SW1 -en nincs értelme cél MAC alapú hash-t, SW2 -n pedig nincs értelme forrás MAC alapút választani
- Hacsak nem az aszimmetrikus terhelés a cél (de miért lenne az)





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