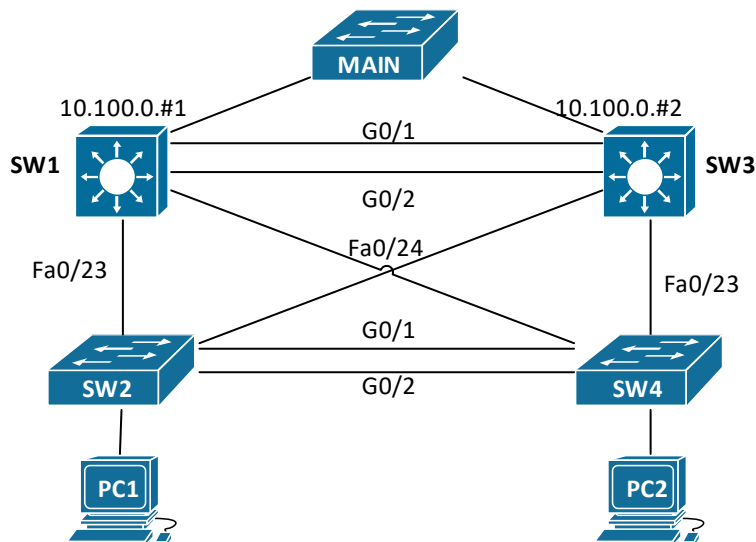


PS2 / cvičenie 06 / STP, VTP, interval routing s L3 prepínačmi

Topológia



Inštrukcie a scenár

- rieši dvojica (jeden študent DLS1 a ALS1, druhý DLS2 a ALS2), pre trojicu možno topológiu rozšíriť o ďalšie dva prepínače (DLS3, ALS3)
 - v labe RB303 je aktuálne 28 prepínačov
 - horné smerovače zvolíť 3550, aby sa v závere mohli z nich spraviť brány cez L3 switching, dolné stačia 2960, alebo 2950
 - horné je vhodné pomenovať DLS1 a DLS2 (distribution layer switch)
 - dolné ALS1 a ALS2 (access layer switch)
 - na začiatok každý iba zapne prepínač, bez kabeláže!! A cez konzolu overí, či nie je nakonfigurovaný (inak `erase startup-config`) a či má prázdnu VLAN databázu (inak `delete vlan.dat`) a `reload`, ak ste mali neprázdny startup-config alebo neprázdny vlan.dat, následne nastavte prepínače do módu transparent (`vtp mode transparent`) a až potom kabeláž a pokračovanie
- Pozn.: Všetky prepínače vedia "mdix-auto" (automatické kríženie keď je to potrebné), okrem Cisco Catalyst 3550 !
 - Preto ak zapájate dva prepínače tejto rady, tak **musíte** použiť krížový kábel
 - Pre všetky ostatné kombinácie dvoch prepojených prepínačov môžete použiť priamy kábel (aj 3550 ---- 2960)
- V postupe nižšie je **modrým vyznačený text**, kde sa niečo konfiguruje, alebo zisťuje, kde sa očakávajú vaše výsledky, ostatný čierny text (hlavne v úvodných častiach) je určený na spoločnú diskusiu a preopakovanie tém z prednášky.

Postup

Úvod a hierarchický dizajn:

1. V labe máme Cisco Catalyst switche 2960, 2950 a 3560. Ktoré z nich by boli vhodné ako prístupové/distribučné/chrbticové switche?
2. .. a na ktoré z nich sa vzťahujú tieto funkcionality?
 - Port security
 - VLANs
 - FastEthernet
 - GigaEth
 - 10GigaEth
 - PoE
 - QoS
 - L3 support, intervlan routing D, ine C
 - Redundancy
 - ACLs
 - Link Aggregation
3. Vieme už o rôznych typoch VLAN: default, native, user, management. V akej VLANe sa prenášajú rámce protokolov CDP, VTP, DTP, PAgP?
4. Aké sú možné typy enkapsulácie na trunk portoch? Aké podporujú naše switche?
5. Čo sa stane keď nastavíte natívnu VLAN na jednom a druhom konci kábla medzi switchmi odlišnú? (cdp+prelievanie)

Základná konfigurácia - nastavte:

- [hostname](#)
- [IP adresa pre vzdialené manažovanie prepínača \(pre rozhranie vlan 1\)](#)
- [zabezpečte prístup na prepínač cez SSH](#)
 - [nezabudnite login local](#)
- [otestovať konektivitu cez SSH na svoj aj susedov prepínač](#)
 - robil sa upgrade IOSov a SSH už podporuje každý prepínač (okrem dvoch – druhý prepínač v ľavom racku a tretí prepínač v pravom rack – tam použijete telnet)

Ako funguje prepínač, redundancia a STP:

Čo vieme o správaní jednoduchého prepínača...

1. Ako sa učí MAC adresy transparent bridge (štandardný switch nemenežovateľný)?
2. Keď transparent bridge nevie ktorým portom poslať daný frame, kam to pošle?
3. Ako sa dá zabezpečiť redundancia medzi switchmi, ak sú to transparent bridges? Dá sa?
4. Kedy vznikne bridging loop?
 - [nasimulujte transparent bridge = vypnite STP na všetkých prepínačoch vo vašej topológii \(defaultne je zapnuté, sh span\)](#)
 - [flapping....](#)

Čo vieme o správaní menežovateľného prepínača a STP...

5. STP vytvorí loop free topológiu switchov, koreňom je Root bridge, koľko ich je pre každú broadcastovú doménu?
6. STP funguje na výmene BPDU medzi switchmi, kam posiela switch BPDU správy?
 - [Wireshark capture: filter STP, analyzuj hlavičku STP aj Ethernet rámca](#)
 - Akú info nesie položka BridgeID? (2+6 B)
 - Čo tvorí 6B ID v BID?
 - Aká je default priorita?
 - Čo sa stane keď zmením niektorému switch prioritu? Čo všetko to môže ovplyvniť?
 - RootID – akú informáciu nesie táto položka?
 - portID – akú informáciu nesie táto položka?
 - max age, message age – akú informáciu nesú tieto položky a na čo slúžia?

7. Aké je správne poradie nasledovných parametrov, ktoré sa používajú pre porovnávanie BPDU a vyhodnotenie ktoré je lepšie?
 - Receiver Port ID
 - Sender Port ID
 - Sender Bridge ID
 - Root Path Cost
 - Root Bridge ID
8. V akých stavoch a rolách sa môže nachádzať port pri STP?

Do obrázka s jednoduchou topológiou (viď tabuľka), urči root bridge, a urči ktoré porty budú v akom stave a v akej roli (ak sa nestíha, môže sa preskočiť)

- spolu na tabuľku (náhodne zvolené MAC), neskôr sami vo svojej topológii (bude nižšie)

Zisti, pochop a ovplyvni STP:

1. Zisti svoje **BID** aj prečo je to takéto číslo a ktorý typ STP sa používa
 - na diagnostiku máme toto všetko:


```
show spanning-tree
sh sp detail
sh sp active
sh sp int fa0/4
sh sp summary (aj tu vidieť v akom móde beží.. ci PVST alebo rapid PVST, defaultne PVST)
sh sp vlan 99
```
 - ak u vás beží rapid-pvst, vypnite ho (no span mode rapid)
2. Zisti ako dopadla voľba RootBridge a ďalej zisti:
 - akú defaultnú prioritu má nastavenú každý switch
 - z informácii na svojom switchi zisti aké BID má RootBridge, nech si ktorýkoľvek switch a zdôvodni prečo sa daný switch stal RootBridge-om
 - **OBRAZOK 1:** nakresli si obrázok s topológiou (stačí 1 obrázok za skupinu, ale spoločná práca) a vyznač do neho aké role majú aktuálne jednotlivé porty na každom switchi (Root/R, Designated/D, Non-designated/Non-D) a sprav značku (krížikom) na tých portoch ktoré sú v stave Blocking (ostatné budú teda zrejme v stave Forwarding)
3. Následne zmeň voľbu tak, aby sa RootBridgom stal niektorý z ostatných switchov, použi príkazy: **root bridge primary, root bridge secondary.**
 - Over že sa zmena udiala a zisti či, a keď tak ako, sa zmenila hodnota priority na switchoch (show spanning-tree).
 - **OBRAZOK 2:** prekresli si nový obrázok s topológiou (stačí 1 obrázok za trojicu) a vyznač do neho znova aké role majú aktuálne jednotlivé porty na každom switchi (Root/R, Designated/D, Alternate/A,...) a sprav značku (krížikom) na tých portoch ktoré sú v stave Blocking (ostatné budú teda zrejme v stave Forwarding)
4. Zmeň voľbu RootBridge tak, aby sa ním stal opäť úplne iný switch, tento krát použi na zmenu parameter **priority**
 - `span vlan XXX priority YYY`
 - Koľko máme možností pre zadanie priority?
 - Prečo je priorita vždy násobkom 4096?
 - over funkčnosť a sleduj hodnoty priorít
5. Použi príkaz na **debugovanie** STP udalostí a nasimuluj výpadok niektorého portu (pozor... dohodnite sa kto čo kedy v skupine, ideálne root port)
 - Inštrukcie ešte pred tým, ako spustíš debug:
 - Budeš sledovať hlášky a vysvetlíš čo sa udialo a ako sa zmenila STP topológia
 - Nakreslíš **OBRAZOK 3:** obrázok s vyznačením stavov a rolí pre porty
 - Odsleduješ tiež, ako rýchlo sa zotaví STP topológia počas zmeny (budeš sledovať vypadnuté ICMP správy na PC)

- Uvedom si, že výstup debugovania neuvidíš, ak si na prepínači vzdialene pripojený (telnet, ssh) – riešením je zadať príkaz `terminal monitor` v privilegovanom móde, pre zobrazovanie hlášok.
- Postup ako na to:

```
na PC: ping -t IP_adresa_switcha
na SW:
debug span events
shutdown (niektorého portu)
sh span
no shut
show span
no debug span events
```

6. **Ovplyvni voľbu root portu, zmeň ju oproti aktuálnemu stavu pomocou (buď/alebo):**
 - **port priority** príkazu - ak je váš aktuálny root port f0/1
 - Kde sa mení port priority v ktorom konfiguračnom móde?
 - Priorita je v násobkoch 16, od 0 po 240. Defaultne je koľko?
 - Zmeňte root port na f0/2
 - **OBRAZOK 4:** Prekresli obrázok s topológiou + vyznačenie stavov a rolí pre porty
 - **port cost** príkazu - ak je váš root port niektorý fastethernet port
 - zabezpečte aby bol po novom root port druhý fastethernet port
7. **Ovplyvni voľbu Designated a Blocking portov na linkách medzi prepínačmi, z ktorých ani jeden nie je root bridge a sú medzi nimi 2 redundantné linky (DLS1-DLS2, alebo ALS1-ALS2)**
 - zabezpeč, aby Des. a Block. po novom bolo naopak na oboch linkách
 - odsledujte výsledok postupne najprv na jednej potom na druhej linke

Príprava na PVST - nastav VLAN a VTP:

1. Na čo slúži VTP? Ako často posiela updaty?
 2. Čo treba nastaviť pri VTP?
 3. Ako sa líšia módy server, client, transparent? Kto môže vytvárať, mazať, meniť vlany? Kto sa synchronizuje, kto preposiela ďalej?
 4. Ktorý switch je vhodne v topológii zvoliť ako server?
 5. Na čo sa používa configuration revision number pri VTP?
 6. Čo sa odporúča keď dávam nový switch do siete?
 7. Čo je to VTP pruning a kde sa nastavuje?
 8. V akej VLANe sa prenášajú VTP rámce?
 9. Čo je best practice pri zmene VLAN databázy na serveroch?
 10. Čo treba spraviť na začiatku každého labu, aby sme pracovali s čistým/nenakonfigurovaným switchom s prázdnu VLAN databázou?
- **Trunking**
 - keďže chceme použiť VTP na distribúciu VLAN databázy zo servera na klientov, je potrebné na každom switchi manuálne vytvoriť VLANu 1000 (iba tuto VLAN !), pretože vrámci nej sa budú prenášať aj VTP rámce (nastavíme ako natívnu VLANu).
 - Preto je potrebné na začiatok sa nastaviť do módu transparent a vytvoriť VLAN 1000 na každom switchi
 - Nastavte všetky aktívne porty (aktuálne sú prístupové vo VLAN 1) na **trunkové** (okrem tých k PCs) s natívnou vlan 1000
 - **VTP**
 - nastavte jeden switch ako VTP server, ostatné ako klientov
 - Hint: **Konfigurácia VTP**, alebo prednáška 5

- Doména: b303, heslo: cisco
- na serveri vytvorte všetky potrebné VLANy s číslom a menom:
10 fakulta, 20 studenti, 30 hostia, 99 manazment, 999 parkovacia
- Skontroluj na hornom aj dolnom prepínači (má správnu VLAN databázu?):
show vtp status
show vtp counters
show int trunk
- Priradíte **porty** do jednotlivých VLAN - potrebné na každom prepínači (toto mi VTP nerieši):
 - fa0/6-10 pre vlan 10
 - fa0/11-15 pre vlan 20
 - fa0/16-20 pre vlan 30
- Zistíte kto je aktuálne Root Bridge pre vlan 10, kto pre vlan 20, 30 a 99
- **Ovplyvníte voľbu Root Bridge** a nastavíte to tak, aby DLS1 bol RB pre vlan 10 a 20, DLS2 aby bol RB pre vlan 30 a 99
 - DLS1 bude default GW pre VLAN 10 a 20, a DLS2 bude default GW pre VLAN 30 a 99, preto táto voľba RB

RSTP

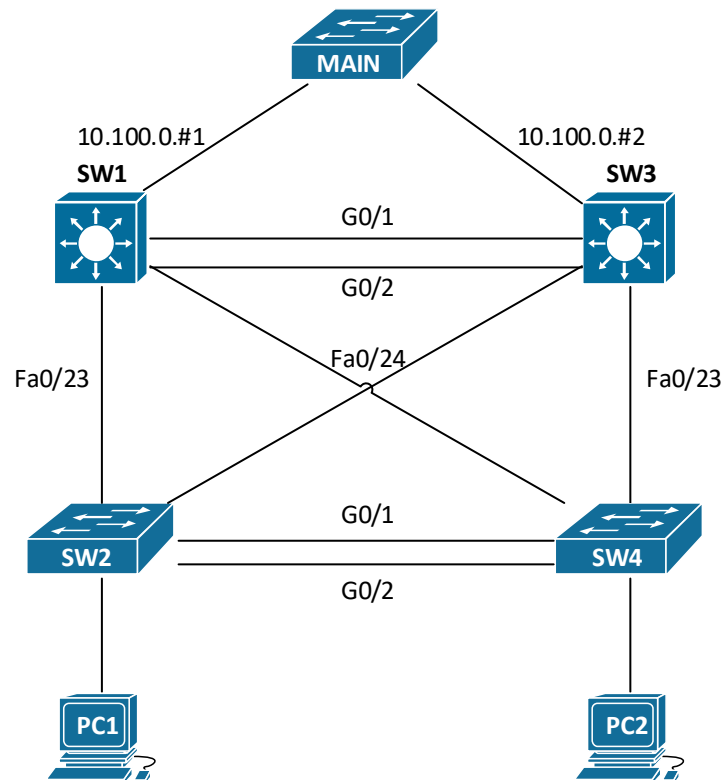
(možno preskočiť a ponechať na ďalšie cvičenie)

- Nakonfiguruj RSTP a odsleduj aj tu rýchlosť konvergencie rovnakým postupom ako predtým:

```
show span
debug span events
spanning-tree mode rapid-pvst
show span
z PC: ping -t IP_adresa_switcha
shutdown (niektorého portu)
no shut
no debug span events
```

L3 switching

(na toto už nebude priestor na ďalšom cvičení, bolo by fajn stihnúť teraz, ak sa nestíha, tak vyriešiť DÚ v PT – už bez experimentov s STP)



- Zapni na vrchných prepínačoch L3 a nastav SVI pre každú VLANu tak, že ľavý horný prepínač bude default GW pre VLAN 10 a 20 (vytvor 2x SVI), a pravý horný prepínač bude default GW pre VLAN 30 a 99 (192.#G.#VLAN.0/24)
 - ip routing
 - int vlan 10
 - Ip add
 - int vlan 20, 30, 99 – podobne
 - otestuj či ide interVLAN routing medzi VLAN 10 a 20
 - otestuj či ide interVLAN routing medzi VLAN 30 a 99
 - ostatné kombinácie až keď rozbehneme RIPv2 v ďalšom kroku
- Napoj sa na hlavný prepínač (stredný rack, HLAVNY) a nastav si na toto rozhranie IP adresu 10.100.0.#1/24, alebo 10.100.0.#2/24, ak si pravý prepínač (prepojíme vaše topológie)
 - nastav toto rozhranie ako L3 smerované (routed)
 - int f0/x
 - No switchport
 - ip add
 - Zapni RIPv2
 - Oznamuj svoje VLANy, pre ktoré je tvoj L3 switch ako default GW a samozrejme spusti RIPv2 aj na spoločnom segmente 10.100.0.0
 - Sleduj záznamy v smerovacej tabuľke, over konektivitu kdekoľvek, do susedných VLAN o kolegu, aj do niektorej VLAN v inej skupine

Diagnostika:

```
show interfaces fa0/18
show ip interface (info o vlanách či sú UP/DOWN)
show ip int brief
```

```
show flash:

show version
show history (to iste čo príkaz show ip arp)
show ip http

show arp
show mac-address-table
show port-security int fa0/18
show port-security address

show vlan
show vlan brief
show vlan id 99
show vlan name management
show vlan summary

show int switchport
show int fa0/18 switchport
```