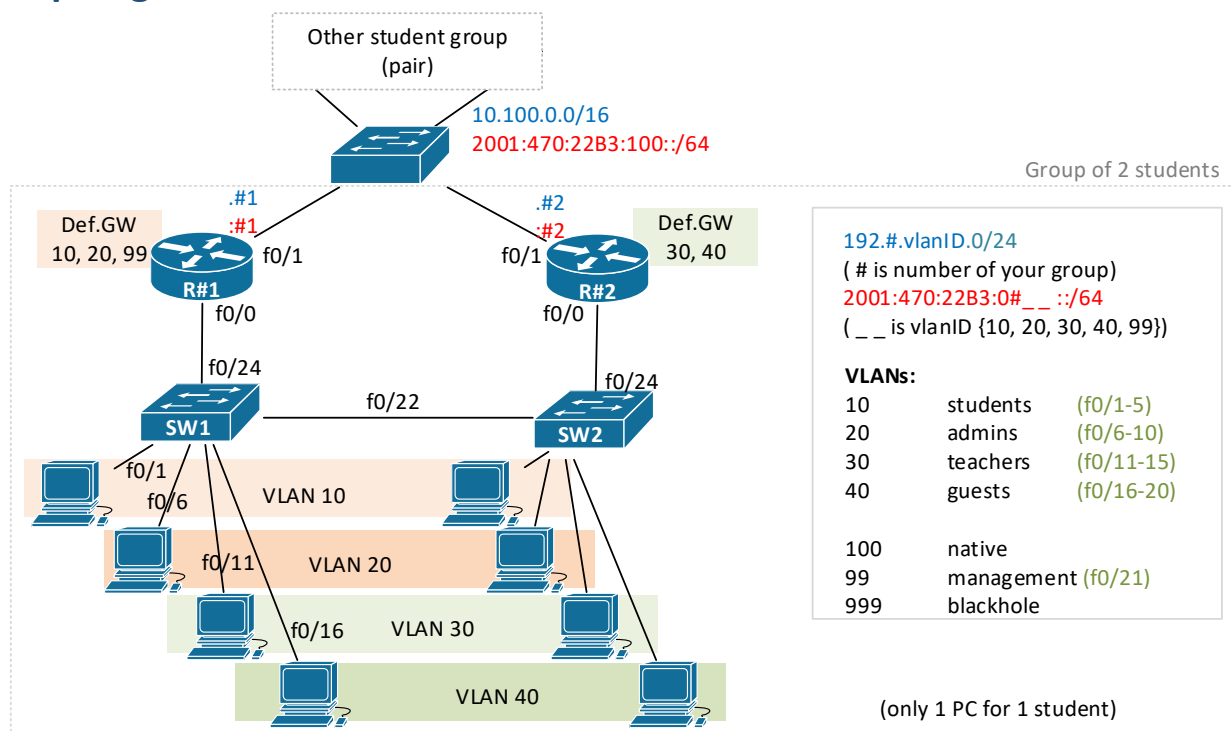


## PS1 / Cvičenie 05 / VLANs, trunks a interVLAN routing

### Topológia



### Inštrukcie a scenár

- o riešime vo dvojiciach, vo dvojici má každý jeden prepínač a jeden smerovač, prepínače sú medzi sebou prepojené
- o neskôr sa cez tretí prepínač pripojíte na jednu vybranú inú dvojicu (ideálne tá vo vašom rade)
- o ak máte možnosť si vybrať, prioritne si vyberte prepínače Catalyst rady 2960 (nie 3550),

### Postup

#### 1. Nakreslite si topológiu

- vyznačte si IP adresy, čísla rozhraní, VLANy, subint, ....

#### 2. Zapojte si topológiu (začínáme iba s prepínačmi)

- Pred káblowaním** si iba nabootujte svoj prepínač (nezapájajte do neho zatiaľ žiadne káble okrem konzoly), overte či nemá uložený config v NVRAM (ak áno, tak `erase startup-config`), a či nemá už vytvorené nejaké VLANy (`show vlan`, `delete vlan.dat`).
  - Ak ste museli niečo mazať, tak **reload**.
- Následne nastavte VTP na prepínači na VTP mode transparent, VLANy si na tomto cvičení budeme vytvárať manuálne na každom prepínači (VTP až na budúcom cvičení).
- Priebežne si konfiguráciu ukladajte (`copy run start`)
  - Po skončení cvičenia nezabudnite po sebe upratať (na SW: `erase startup`, `delete vlan.dat`, na R: `erase startup`)
- Nastavte si hostname: SW1, SW2
- Pre efektívnosť práce nastavte:

- i. `line con 0, login synchronous`
- ii. `no ip domain-lookup`

### 3. Testy ešte pred vytváraním VLAN:

- a. Pripojte PC1 a PC2 do portov f0/1 na prepínačoch SW1, SW2 a nastavte počítačom PC1 a PC2 IPv4 adresy (a príslušné masky) z **VLAN 10**, a otestujte konektivitu – ping PC1-PC2
  - i. Overtite si aktuálnu príslušnosť portov do VLAN  
`sh vlan brief, show vlan summary, show interfaces`
  - ii. Overti si v akom režime funguje linka medzi SW1 a SW2  
`show int trunk, show int f0/xy switchport, show dtp interfaces`
    - Prečo je to tak?
- b. Nastavte počítačom PC1 a PC2 IP adresy (a príslušné masky) z **VLAN 20**, a otestujte teraz konektivitu (stále sú v portoch f0/1)
  - i. Ide to? Zdôvodnite prečo?

### 4. Všetky porty na oboch prepínačoch priradíte do záložnej VLAN 999

- a. `interface range f0/1-24`  
`switchport mode access`  
`switchport access vlan 999`
  - i. VLAN 999 netreba vytvárať (príkazom: `vlan 999`), prečo? (mohli by sme ale nemusíme..)
- Pozrite si teraz výpisy z: `show interface, show vlan brief, Show vlan id 999, show vlan summary`
- Pridajte pre VLAN 999: `state suspend` (prepínač nebude potom prepínať žiadne rámce, ktoré prídu vrámci tejto VLAN), a nastavte jej meno `blackhole` (`name blackhole`)
  - Overtite `show vlan brief, show vlan 999`
  - Pozn.: Na vytvorenie záložnej VLAN môžeme použiť príkaz v konfigurácii danej VLAN: `state suspend`, alebo `shutdown`. Rozdiel je v tom, že `suspend` VLAN sa šíri aj cez VTP, `shutdown` má lokálny význam iba na danom prepínači.

### 5. Vytvorte VLAN 10 na oboch prepínačoch (`vlan 10, name students`)

- a. Priradíte porty f0/1-5 do VLAN10 (`switchport access vlan 10`) a overte výpisy  
`sh vlan brief, sh vlan summary, sh int f0/1 vlan 10, sh vlan id 10`
  - i. Otestujte konektivitu z PC1 na PC2 (nemalo by ísť)
    - Prečo to nejde? - pozrite si v akom režime funguje port medzi prepínačmi? (keď sme odkladali porty do záložnej VLAN 999, "pokazili" sme aj porty medzi prepínačmi)  
Overti si v akom režime funguje linka medzi SW1 a SW2: `show int trunk, show int f0/22 switchport, show dtp interfaces, sh vlan`
      - Prečo je to tak?
  - Vyriešte situáciu, použite DTP protokol, a použite mód `dynamic desirable` na oboch koncoch linky medzi prepínačmi, aby si prepínače dohodli trunk automaticky (na rozhraní f0/22: `switchport mode dynamic desirable`, ale ešte pred tým treba zrušiť príslušnosť daného portu do suspendovanej VLAN 999 príkazom: `no switchport access vlan 999`)
  - Ako si overiť, či je DTP zapnuté (defaultne by malo byť):
    - Buď v `running-config` na porte hľadám `switchport negotiate pre` daný port
    - Alebo pozriem výpis  
`show interfaces trunk,`

`show dtp` (hľadaj: `x` interfaces using DTP – namiesto X budete mať počet rozhraní)

`show int switchport` (hľadaj Negotiation of Trunking: `On`)

`show dtp interfaces`

## 6. Otestujte zmazanie VLAN

- a. Zmažte VLAN 10 (no vlan 10)

- i. Čo sa stalo s portami f0/1-5? Do akej vlan teraz prislúchajú?

`sh vlan brief`, `show run` – pozrite konfiguráciu portov f0/1-5

- b. Znovu vytvorte VLAN 10

- i. Čo sa stalo s portami f0/1-5? Do akej vlan teraz prislúchajú?

`sh vlan brief`, `show run` – pozrite konfiguráciu portov f0/1-5

- ii. Dajte situáciu do pôvodného stavu, aby porty f0/1-5 boli opäť korektne vo VLAN 10

## 7. Priradte príslušné porty do VLAN 20 (admins), 30 (teachers), 40 (guests), 99 (management)

Pozn.: Už nemusíte vytvárať VLANy, keďže viete že sa vytvoria automaticky pri tom, keď priradíte porty do príslušných VLAN. Dodatočne im ale treba nakonfigurovať meno.

- a. Otestujte konektivitu z PC1 vo VLAN 10 na PC2 vo VLAN 10 (IP adresy musia byť zo subnetu ktorý sme si stanovili pre túto VLAN)
- b. Zopakujte predošlé pre VLAN 20, 30, 40, 99 – t.j. prepnem PC1 a PC2 do iných portov a test pingom (testujeme iba intraVLAN konektivitu – t.j. vrámci 1 VLAN)

## 8. Nastavte prepínačom IP adresu z VLAN 99

- a. Menežmentovú VLAN sme zvolili VLAN 99, preto interface vlan 99, ip add...
- b. Nastavte aj default gateway (viď návrh IP dizajnu na tabuli) a heslo pre VTY
  - i. IP rozhrania smerovača - viď tabuľa - konfigurovať to rozhranie na smerovači budeme neskôr, tu si len pripravíme všetko potrebné na prepínači
- c. Pokúste sa z vášho PC telnetnúť na váš prepínač
  - i. Ide/nejde? Zdôvodnite prečo?
    - Elegantné riešenie príde neskôr, keď nakonfigurujeme rozhranie smerovača (bod 10), dovtedy:
    - Vieme to ale vyriešiť aj inak - vyhradiť jeden port na prepínači - z tých dvoch ešte voľných portov, ktorý pridáme do VLAN 99 a tam zapojíme náš PC (dočasne), treba mu potom aj prideliť IP adresu z VLAN 99
      - Otestujte teraz telnet pripojenie na váš prepínač
      - Ide/nejde? Zdôvodnite prečo?
- d. Telnetnite sa z vášho prepínača na susedov prepínač
  - i. Ide/nejde? Zdôvodnite prečo?

## 9. Znížte bezpečnostné riziko - vypnite DTP protokol a nastavte napevno trunk medzi SW1 a SW2

- a. Nastavte teraz f0/22 medzi prepínačmi SW1 a SW2 napevno aby bol trunk, a zmeňte natívnu VLAN na 100

- i. `interface f0/22`

`switchport trunk encapsulation dot1q` ! iba ak mám na výber z ISL a dot1q. Ak na damon IOSe je podporovaný iba 1 typ, tak netreba tento príkaz.

`switchport mode trunk`

`switchport trunk native vlan 100` ! pozor, tu neplatí, že vlan 100 sa týmto príkazom aj automaticky vytvorí, ak ešte nie je. Treba ju manuálne vytvoriť a pomenovať (vlan 100, name native)

- ii. Over nastavenia linky medzi SW1 a SW2? (`sh int trunk`, `sh int f0/22 switchport`)

- b. Pozrite vo výpisoch, či je DTP on alebo off
  - i. Použi: `sh dtp`, `sh int f0/22 switchport`
    - Hľadaj: ... interfaces using DTP
    - Hľadaj: Negotiation of Trunking...
  - ii. Následne DTP vypnite (`int f0/22, switchport nonegotiate`), a sledujte výsledok:
    - `show dtp` (hľadaj: 0 interfaces using DTP – ak ale na niektorých rozhraniach ostalo DTP zapnuté, nebudete mať 0, overenie ale spravíte ešte druhým príkazom nižšie)
    - `show int switchport` (hľadaj Negotiation of Trunking: **Off**)
    - `show dtp int f0/22`
- c. Otestujte teraz konektivitu medzi PC1 a PC2 (obom dajte IP adresu z rovnakej VLAN) – malo by fungovať

## 10. Nakonfigurujeme subinterfejsy na smerovači pre smerovanie medzi VLANami

Podľa dohody v tomto kroku nastavíme:

R1 bude default GW pre VLAN 10, 20, a 99

R2 bude default GW pre VLAN 30, 40

Zatiaľ teda vyriešime iba smerovanie medzi VLANami 10, 20 a 30, a oddelene medzi 30 a 40. V bode 11 doriešime celkovú konektivitu každý z každým, pomocou RIP.

- a. Nastavte si hostname: R#G1, R#G2
- b. Nakonfigurujte subrozhrania na smerovačoch - podobne ako fyzické rozhrania, ale pridať treba, že sa bude značkovať a aj pre akú VLAN, t.j. aké značky budeme pridávať rámcom, keď ich pošleme daným trunkom k prepínaču:
  - i. Na smerovači R1:
 

```
interface f0/1.10
  encapsulation dot1q 10
  ip address ... (IP z VLAN 10)
```

(no shutdown nie je potrebný, je to subinterface, zadáme ho neskôr pre fyzický interface f0/1)

```
interface f0/1.20
  encapsulation dot1q 20
  ip address ... (IP z VLAN 20)
```

(no shutdown nie je potrebný, je to subinterface, zadáme ho neskôr pre fyzický interface f0/1)
  - ii. Podobne f0/1.99 na R1 a f0/1.30, f0/1.40 na R2
  - iii. Vzbudíte fyzické rozhranie f0/1 (`no shut`). Toto rozhranie nebude mať pridelenú žiadnu IP adresu.
- c. Rozhrania na prepínačoch vedúce k smerovačom nastavte napevno na trunk tak, že povolíte iba existujúce VLANy.
  - i. Z týchto trunkových rozhraní odstráňte tie VLANy, ktoré sa cez tento trunk určite nebudú prenášať.
    - Na SW1 majú byť vo finale povolené iba VLAN 10,20,99, na SW2 iba VLANs 30 a 40
- d. Otestujte konektivitu
  - i. Iba medzi **vybranými** dvojicami VLAN
    - Najjednoduchší test je, keď z prepínača (ktorého manažmentový virtuálny interfejs je vo VLAN99) skúsime ping na PC vo VLAN 10, a na PC vo VLAN 20

- Pozn.: Zvykom študentov je zabudnúť nastaviť na počítačoch okrem IP adresy a masky aj **default GW**, čo je kritické, ak chceme robiť test aj k iným subsietiam (iným VLANs).
- Ďalej sa dá testovať...
  - PC1 dám do portu vo VLAN30, pridelím mu príslušnú IP, PC2 dám do portu vo VLAN 40, pridelím správnu IP z VLAN 40 a test pingom
  - PC1 dám do portu vo VLAN10, pridelím mu príslušnú IP, PC2 dám do portu vo VLAN 20, pridelím správnu IP z VLAN 20 a test pingom
- Testy z VLAN 10 do 30 alebo 40, a z VLAN 20 do VLAN 30 a 40 pôjdu až keď zrealizujete nasledujúci bod 11. – cez hornú časť siete cez RIP.

**11. Použite RIPv2 pre spojenie so susednom dvojicou, aj pre smerovanie medzi VLANs na R1 a VLANs na R2**

- a. R1 oznamuje iba svoje priamo pripojené siete VLAN 10 a 20
- b. R2 oznamuje iba VLAN 30 a 40
- c. VLAN 99 v RIP neohlasujeme
- d. Otestujte konektivitu k susednej dvojici k počítačom v rôznych VLANs v IPv4

**12. Nakonfigurujte interVLAN routing aj pre IPv6**

Pozn.: Zopakovať treba bod 10, ale pre IPv6 adresy

**13. Použite RIPv6 pre spojenie so susednom dvojicou**

- a. R1 oznamuje iba svoje priamo pripojené siete VLAN 10 a 20
- b. R2 oznamuje iba VLAN 30 a 40
- c. VLAN 99 v RIP neohlasujeme
- d. Otestujte konektivitu k susednej dvojici k počítačom v rôznych VLANs v IPv6