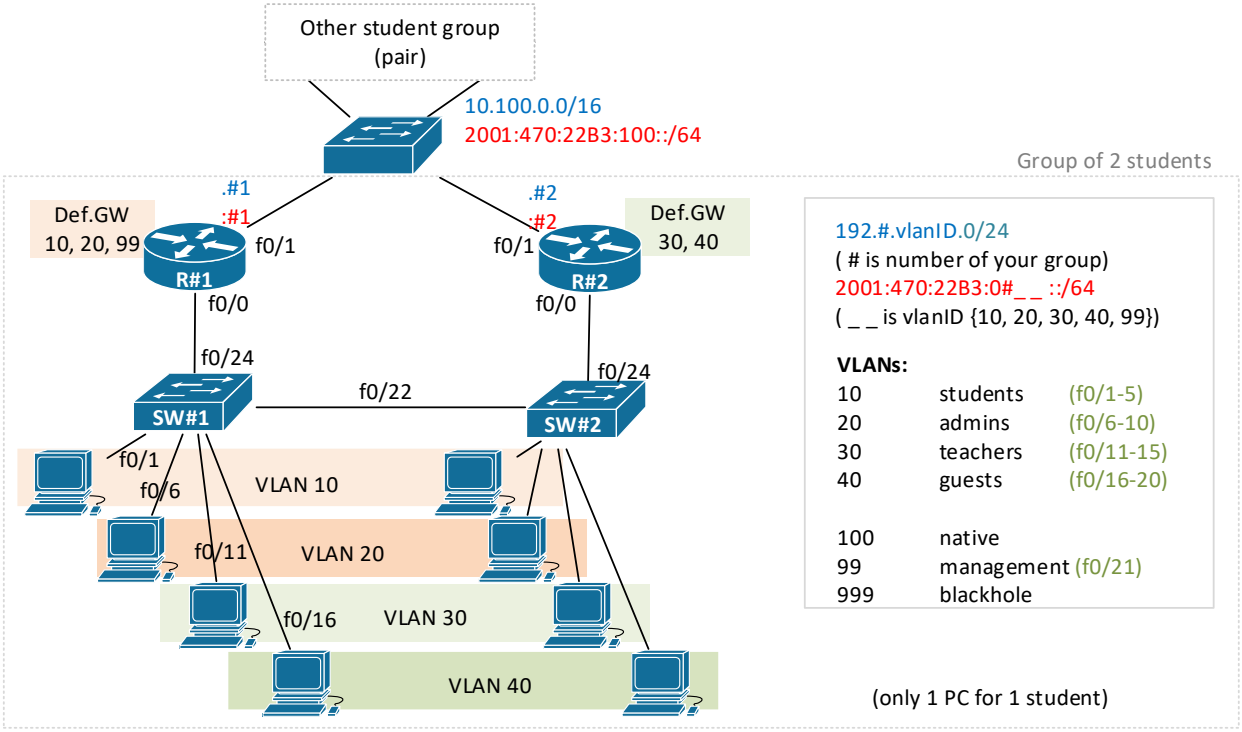
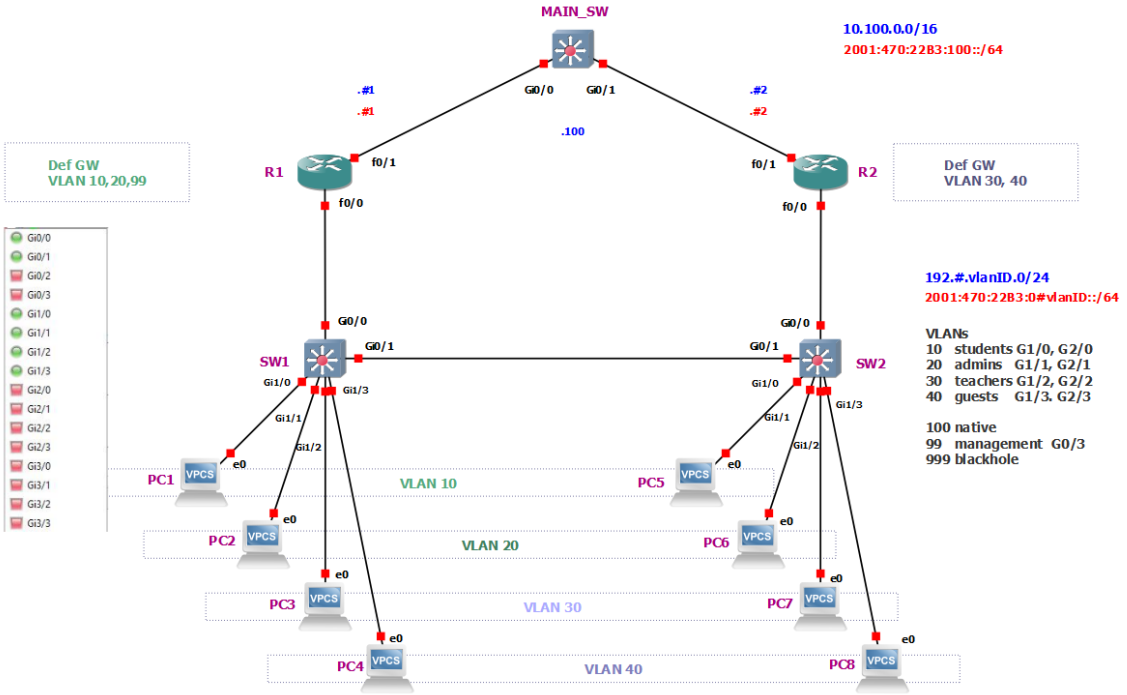
PS1 / Cvičenie 05 / **VLANs, trunks a interVLAN routing**

Topológia

Ver. A – pre prácu na reálnych zariadeniach v laboratóriu (nekáblujte skôr ako spravíte krok 1 a 2 z postupu):



Ver. B – pre prácu na emulovaných zariadeniach vo virtuálnom prostredí GNS3 (topológia je pripravená pod názvom: PS1-cv05-VLANs—TEMPLATE, ktorú vyučujúci nakopíruje pre všetky skupiny):



Inštrukcie a scenár

- riešime vo **dvojiciach**, vo dvojici má každý jeden prepínač a jeden smerovač, prepínače sú medzi sebou prepojené
- body zvýraznené **modrým** v postupe zadania je potrebné **ukázať** vyučujúcemu – kontrola
- špecificky pre prácu v **laboratóriu**:
  - neskôr sa cez tretí prepínač pripojíte na jednu vybranú inú dvojicu (ideálne tá vo vašom rade) – toto teda nie je prepínač MAIN ako sme používali doteraz, ale len nejaký tretí prepínač, ktorý bude prepájať vašu skupinu, s jednou inou dvojicou
  - ak máte možnosť si vybrať, prioritne si vyberte prepínače Catalyst rady **2960** (nie 3750) – z tých štvoríc prepínačov v našich rackoch sú to vždy tie spodné dva
- pre prácu v **GNS3**:
  - potrebná je VPN, a prístup buď cez prehliadač: 158.193.152.63, alebo cez nainštalovaného GNS3 klienta ver. 2.2.25 (nie žiadna iná) – info máme v Moodle
  - v zozname projektov hľadajte tento názov: **PS1-cv05-VLANs-**str15-JU-skupina01 (str15 – nájdite deň a čas vášho cvičenia, JU – nájdite iniciály vášho cvičiaceho, skupina0X – skupinu vám pridelí vyučujúci, pracuje sa v dvojiciach)
  - po otvorení projektu, si naštartujete všetky zariadenia stlačením tlačidla Start/Play – hore v menu trojuholník v obdĺžniku
  - Na CLI daných zariadení vojdete takto – pravým tlačidlom na zariadenie a:
    - V GNS3 klientovi: Console
    - V prehliadači vo web GUI: Web console in new tab
  - IP adresy na počítačoch nastavte takto:
    - Pravým tlačidlom na PC a Edit config a odkomentovať riadok:
      - ip TUdajADRESU/TUdajMASKU TUdajIPdefaultGATEWAY, napr: `ip 192.1.10.3/24 192.1.10.1`, a pod to neskôr pripíšeš: `ip 2001:470:22B3:10::3/64 auto` (auto - automaticky nastaví bránu, viď SLAAC proces, a vidieť ju budete vo výpise: show ipv6)
      - Potvrdíte: Apply
    - Vojdite do CLI daného zariadenia (Console, alebo Web console in new tab) a zadajte príkaz (týmto sa daný config aplikuje/použije):
      load startup.vpc
    - Overenie nastavení zistíte príkazmy: `show ip, show ipv6`
  - keďže v GNS3 používame iný typ prepínača ako máme v reálnom laboratóriu, prosím berte do úvahy tieto zmeny, a podľa nich konfigurujte kroky v postupe:
    - Prepínač v GNS3 má 4 karty s Ethernet portami, pričom na každom sú po 4 porty (v obrázku ver. B s topológiou vidieť vľavo zoznam portov), preto **názvy týchto rozhraní sa budú odlišovať**
    - Vpravo v obrázku ver. B máte zoznam portov, ktoré majú patriť do ktorej VLAN. Budete pridávať práve dva porty do každej access VLAN na každom prepínači, akurát názvy tých rozhraní budú iné.

Obsah

Postup

1. **Pri práci v labe: nakreslite si topológiu na papier**
    a. vyznačte si IP adresy, čísla rozhraní, VLANy, subint, ….
2. **Zapojte si topológiu (začíname iba s prepínačmi)**
    a. Pre prácu v GNS3: topológiu máte hotovú.
    b. **Pre topológiu v labe: Pred káblovaním** si iba nabootujte svoj prepínač (nezapájajte do neho zatiaľ žiadne káble okrem konzoly), overte či nemá uložený config v NVRAM
        i. `show running-config`, ak má uloženú konfiguráciu, tak `erase startup-config`
        ii. a či nemá už vytvorené nejaké VLANy: `show flash:`, hľadaj súbor `vlan.dat` - nemal by tam byť žiadny, `show vlan` - nemali by tam byť žiadne iné vlany okrem VLAN 1, vyššie ako 1000 nerátame, tam je niekoľko VLANs vždy prítomných a „nezmazateľných“, `ak` ak ste niečo našli, tak je potrebné zmazať súbor s VLAN databázou `delete vlan.dat`
        iii. Ak ste museli niečo z predošlého mazať, tak **reload**
            - Na otázku typu: `Would you like to save configuration...?` odpovedzte: No (inak by ste boli znova v rovnakom stave, a config naloadovaný v RAM by sa znova uložil do NVRAM)
    c. 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).
    d. Priebežne si konfiguráciu ukladajte (`copy run start`)
        i. Pri práci v GNS3:
            - Ukladajte si priebežne konfiguráciu, lebo ak vy alebo váš kolega okno GNS3 klienta alebo okno prehliadača zavrie, tak prídete o všetko neuložené.
            - Pokiaľ chcete po zavretí okna GNS3 aby vám ostal projekt bežať na pozadí, a neskôr sa k nemu vrátiť, tak v menu vyberte File – Edit Project (alebo cez

web GUI: Projects setings – Edit project) – a tam zaškrtnite možnosť: Leave this project running in the background when closing GNS3.
- Upozorňujeme, aby ste toto nerobili vždy a paušálne, ale len vtedy, keď naozaj chcete na tom robiť po krátkej prestávke, pretože zahlcujete zdroje servera, na ktorom pracujú mnohé iné skupiny študentov.

ii. Po skončení cvičenia nezabudnite po sebe upratať (na SW: `erase startup, delete vlan.dat`, na R: `erase startup`)

e. Nastavte si hostname: SW1, SW2

f. Pre efektívnosť práce nastavte:
   i. `line con 0, logging synchronous`
   ii. `no ip domain-lookup`

3. Testy ešte pred vytváraním VLAN

Pozn. pre topológiu v reálnom laboratóriu: keďže počítač máte na osobu len jeden, budete si dané PC prepínať do rôznych portov podľa potreby a meniť na ňom IP podľa potreby.
Pozn. pre topológiu v GNS3: nie sme obmedzený počtom PC na osobu, a teda máte v topológii toľko PCs koľko potrebujeme.

a. Pripojte PC1 a PC2 do portu f0/1 (v GNS3 už máte zapojené v G1/0 ako PC1 a PC5) na prepínačoch SW1, aj SW2 a nastavte počítačom PC1 a PC2 IPv4 adresy (a príslušné masky) z **VLAN 10**, a otestujte konektivitu – ping PC1-PC2
   i. Overte 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 (v GNs3: PC1 a PC5) IP adresy (a príslušné masky) z **VLAN 20**, a otestujte teraz konektivitu (stále sú v portoch f0/1, resp. v GNS3: G1/0)
   i. Zdôvodnite prečo to ide?

c. Po teste im opäť vráťte IP adresu z rozsahu pre VLAN 10.

4. Všetky porty na oboch prepínačoch priraďte do záložnej VLAN 999

a. `interface range f0/1-24` (v GNS3 pozor, je to iná množina portov, pozri obrázok, ver. B)
```
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 v rámci tejto VLAN), a nastavte jej meno blackhole (`name blackhole`)
         - Overte `show vlan brief, show vlan id 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. Priraďte 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`
Pozn. pre GNS3 topológiu: porty G1/0 do VLAN10.

i. Otestujte konektivitu z PC1 na PC2 (nemalo by ísť) (v GNS3 je to PC1 a PC5)
   - 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`
     Pozn. pre GNS3 topológiu: port Gi0/1.
     - 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`) (v GNS3: nastavujete port G0/1, a nastavte na ňom ešte navyše aj typ enkapsulácie na dot1q, z dôvodu že ISL značkovanie v GNS3 nefunguje korektne)
   - Ako si overiť, či je DTP zapnuté (defaultne by malo byť):
     - Nájdite v running-config na porte `switchport negotiate` pre daný port
     - A pozrite aj výpis
       `show interfaces trunk` (`Desirable`, alebo `Auto` – znamená, že využívame DTP, niektoré prepínače majú predvolené: `dynamic desirable`, niektoré: `dynamic auto`)
       `show dtp` - hľadaj: `X interfaces using DTP` – namiesto `X` budete mať počet rozhraní, ale nebude tam žiadne konkrétnejšie info, to nájdete tu:
       `show int f0/22 switchport`
       (hľadaj `Negotiation of Trunking: On`)
       `show dtp interface f0/22`
       (hľadaj v riadku TAS/TOS/TNS: `Trunk/Negotiate/Trunk`)
       Pozn. pre GNS3 topológiu: pracujete s portom Gi0/1.

6. Otestujte zmazanie VLAN

Pozn. pre GNS3 topológiu: pracujete s portami G1/0 a G2/0.

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. Priraďte 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)
   Pozn. pre GNS3: z PC1 vo LAN 10 na PC5 vo VLAN 10.
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. v rámci 1 VLAN)

Pozn. pre GNS3 topológiu: vy nemusíte nič nikde prepínať, pretože máte v topológií už priamo nakopírovaných viac počítačov.

8. **Nastavte prepínačom IP adresu z VLAN 99**
   a. Manažmentovú 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 telnetnúť na váš prepínač
      i. Prvý pokus spravte z vášho PC.
         Pozn. pre GNS3 topológiu: na PC nemáte k dispozícii telnet, preto spravte iba ping.
         - Zdôvodnite prečo to nejde?
      ii. Druhý pokus – prepnite si PC do portu, ktorý ste pridali do VLAN99 v kroku 7, a tam zapojíte váš PC (dočasne), treba mu potom aj prideliť IP adresu z VLAN 99
         Pozn. pre GNS3 topológiu: na PC nemáte k dispozícii telnet, preto spravte iba ping. Môžete si do topológie v GNS3 vložiť nový počítač a použiť ten (nájdete ho ako VPCS medzi koncovými zariadeniami).
         - Otestujte teraz telnet pripojenie na váš prepínač
           - Zdôvodnite prečo to ide?
      iii. Tretí pokus spravte z prepínača na prepínač - v dvojici sa pripojte cez telnet zo svojho prepínača na kolegov prepínač (ideme cez trunk)
         - Zdôvodnite prečo to ide?
      iv. Štvrtý pokus - príde neskôr, keď nakonfigurujeme rozhranie smerovača (bod 10) pre interVLAN routing.

9. **Znížte bezpečnostné riziko - vypnite DTP protokol a nastavte napevno trunk medzi SW1 a SW2**
   Pozn. pre GNS3 topológiu: pracujete s portom G0/1.
   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 danom IOSe je podporovaný iba 1 typ, tak netreba tento príkaz.
         Pozn. pre GNS3: tento príkaz je nutné zadať, ISL enkapsulácia nefunguje na prepínačoch v GNS3 korektne.
         `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 a dokonfigurujte aj rozhranie na prepínačoch vedúce k smerovaču

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 na smerovačoch 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 f0/0.10
      encapsulation dot1q 10
      ip address ...
   ```
   (IP z VLAN 10)
   (no shutdown nie je potrebný, je to subinterface, zadáme ho neskôr pre fyzický interface f0/0)
   ```
   interface f0/0.20
      encapsulation dot1q 20
      ip address ...
   ```
   (IP z VLAN 20)
   (no shutdown nie je potrebný, je to subinterface, zadáme ho neskôr pre fyzický interface f0/0)
   ii. Podobne f0/0.99 na R1 a f0/0.30, f0/0.40 na R2
   iii. Vzbuďte fyzické rozhranie f0/0 `(no shut)`. Toto rozhranie nebude mať pridelenú žiadnu IP adresu.
   iv. Skontrolujte stav rozhraní aj subrozhraní `(sh ip int br)`
c. Rozhrania na **prepínačoch (SW1, SW2)** vedúce k smerovačom nastavte napevno na trunk tak, že povolíte iba existujúce VLANy (v labe: f0/24, v GNS3: G0/0).
   i. Z týchto trunkových rozhraní odstráňte tie VLANy, ktoré sa cez tento trunk určite nebudú prenášať.
      - Na SW1 majú byť vo finále povolené iba VLAN 10, 20, 99, na SW2 iba VLANs 30 a 40
         - Pozn.: V príkaze pri vymenovaní VLANs **nesmie byť** medzi nimi **medzera**, t.j. za čiarkou. (správne je: vlans 10,20,99 alebo: vlans 30,40)
   ii. Pri práci v GNS3: na rozhraní G0/0 vám začnú chodiť správy *CDP duplex mismatch...*, riešením je:
      - `G0/0: no negotiate auto, duplex auto`
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 subsieťam (iným VLANs).

- Ďalej sa dá testovať...
  Pozn. pre GNS3 topológiu: netreba prekladať PC do iných portov, vy už máte v každom porte zapojený počítač, a ping môžete robiť z daných PC (v labe nemôže mať študent viac ako 1 PC, v GNS3 týmto nie sme limitovaní).
  - 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
    Pozn. pre GNS3 topológiu: ping z PC3 na PC8
  - 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
    Pozn. pre GNS3 topológiu: ping z PC1 na PC6.
- 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 svoje priamo pripojené siete VLAN 10 a 20
   i. Nezabudnite aké všetky siete zapísať do príkazu `network`
   ii. Skontrolujte si konfiguráciu cez `sh ip protocols`
b. R2 oznamuje VLAN 30 a 40
   i. Nezabudnite aké všetky siete zapísať do príkazu `network`
   ii. Skontrolujte si konfiguráciu cez `sh ip protocols`
c. VLAN 99 v RIP neohlasujeme
d. Skontrolujte obsah smerovacích tabuliek na R1 aj R2
e. Otestujte konektivitu k susednej dvojici k počítačom v rôznych VLANs v IPv4
   Pozn. pre GNS3 topológiu: máte viac možností – buď si pridať do MAIN_SW jedno PC, a dať mu IP adresu z rozsahu ktorý v danom segmente používate arobiť ping voči nemu, alebo budete robiť ping voči IP adresám ktorá majú smerovače na vonkajších rozhraniach f0/1.
   i. Zisti cez traceroute, kadiaľ ide komunikácia
      - z PC vo VLAN10 na PC vo VLAN20, z PC vo VLAN 30 na PC vo VLAN40
      - z PC vo VLAN10 na PC vo VLAN 30, z PC vo VLAN 40 na PC vo VLAN 20

12. Nakonfigurujte interVLAN routing aj pre IPv6 (pokiaľ zvýši čas)

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

13. Použite RIPng pre spojenie so susednom dvojicou (pokiaľ zvýši čas)

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