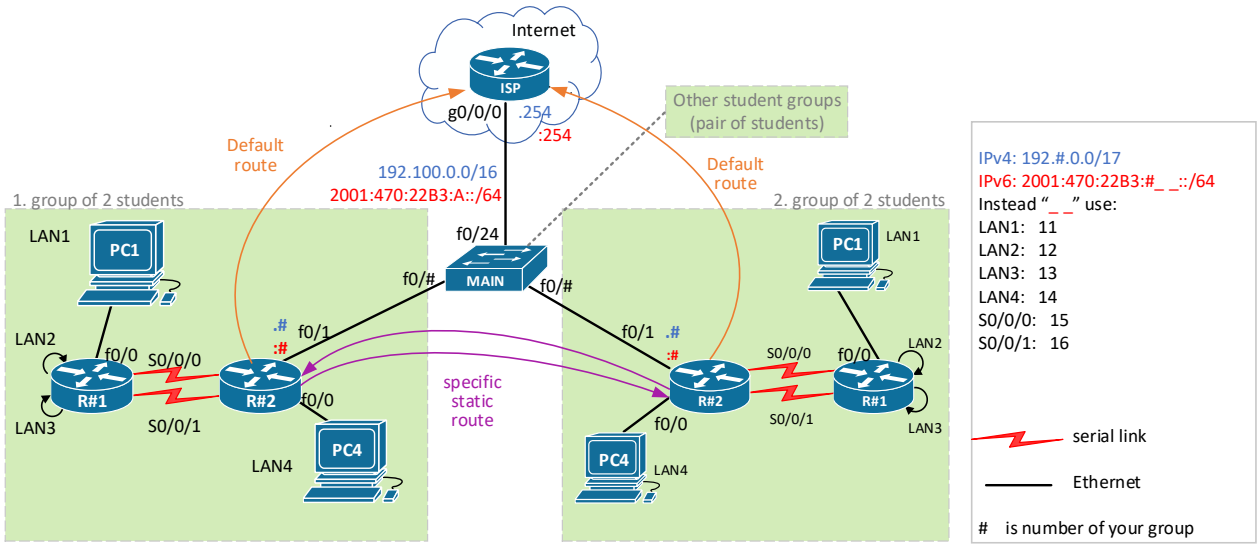
# **PS1** / Cvičenie 02 / Statické cesty

(špecifické, default, sumarizované, plávajúce)

## Topológia




## Scenár

Topológiu s 2 smerovačmi rieši **dvojica** – tvoria jednu skupinu, pričom:

- učiteľ priradí každej skupine číslo skupiny, v zadaní ďalej ako **#**
- @ bude značka pre číslo smerovača {1 alebo 2}
- Ohraničené šípky na smerovačoch označené ako LAN 2, 3 budú simulované virtuálnym rozhraním Loopback 2 a 3 (`interface loopback 2, int lo 3`)
- Modré časti v texte nižšie je potrebné ukázať inštruktorovi pre kontrolu.
  - KONTROLA 1 až 8

## Postup

1. **Pripojenie sa na konzolu prepínača a smerovača a kontrola default stavu**
   **Pozn.:** Pokiaľ vidíte, že pri stojanoch je príliš veľa ľudí naraz, robte zatiaľ bod 3, a 4, a akonáhle sa uvoľní priestor, pokračujte v tomto bode 1.
   a. **Pred káblovaním** si iba nabootujte svoj prepínač, potom aj smerovač (nezapájajte do neho zatiaľ žiadne iné káble okrem konzoly), overte či nemá uložený config v NVRAM nasledovne:
      i. Pozn.: Prepínače sa zapínajú automaticky, nemajú tlačidlo pre zapnutie, smerovač treba manuálne zapnúť
      ii. Nenakonfigurovaný smerovač a prepínač po nabootovaní vypíše hláškou: „*Would you like to enter initial configuration dialog?*“
      - Ak vám táto hláška vyskočila, tak:
        - Odpovedzte „No“, pretože by vám spustilo dialóg, a nie CLI.
        - Ak sa zobrazí ešte potvrdzujúca otázka: „*Would you like terminate autoinstal*?“ tak potvrďte „Yes“, že naozaj chcete ukončiť dialóg/autoinštaláciu.

- Pokiaľ tá hláška nevyskočí, tak:
  - overte príkazom `show startup-config`, že je tam uložená konfigurácia a zmažte ju: `erase startup-config`
  - Následne reštartujte smerovač/prepínač príkazom: `reload`
  - Na otázku: `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)

2. **Zapojte si topológiu**

   **Pozn.:** Pokiaľ vidíte, že pri stojanoch je príliš veľa ľudí naraz, robte zatiaľ bod 3, a 4, a akonáhle sa uvoľní priestor, pokračujte v tomto bode 2. Ideálny počet ľudí je jedna dvojica pri každom stojane.
   a. Zapojte zariadenia podľa obrázku s topológiou, dodržte rozhrania pokiaľ je to možné.
      i. Pri niektorých rozhraniach môže byť krížik vyznačený fixkou, čo znamená, že dané rozhranie nie je funkčné, vtedy použite iné rozhranie, alebo si vymeňte zariadenie.
3. **Subsieťujte pridelený IPv4 rozsah pre svoju topológiu s 2 smerovačmi a 2 PCs:**
   a. Subsieťujte pridelený IPv4 rozsah: 192.#.0.0/17
      i. Veľkosti sieti LAN 1, 2, 3, 4 sú takéto: 60, 20, 25, 120
      ii. Veľkosti WAN sietí – sú jasné (sériové linky medzi smerovačmi)
   b. Zakreslite si IPv4 adresy sietí a rozhraní do obrázka, pričom:
      i. Počítačom prideľte najvyššiu IPv4 adresu, smerovačom najnižšiu IPv4.
      ii. Na linkách medzi smerovačmi (sériové linky) dajte smerovaču s nižším číslom v jeho hostname nižšiu IP adresu z rozsahu, a smerovaču s vyšším číslom vyššiu IP adresu.
4. **Nakreslite si topológiu na papier** (pokiaľ ju nemáte vytlačenú)
   a. vyznačte si IP adresy, čísla rozhraní, číslo vašich zariadení v racku, ktoré ste si obsadili, atď.
5. **Základná konfigurácia**
   a. Nastavte smerovačom hostname R#1, R#2
   b. Pre efektívnosť práce nastavte:
      i. Zabráňte na prepínačoch výpis hlášok do písaného textu na konzole (zmiešavanie vstupu a výstupu CMD) `(line console 0, logging synchronous)`
      ii. Vypnite prekladanie doménových mien na IP adresy `(no ip domain-lookup)`
      iii. Nakonfigurujte si SSH prístup na svoj smerovač
   c. Podľa plánu v bode 1 tohto zadania nakonfigurujte IP adresy pre všetky rozhrania vašich smerovačov aj počítačov
   d. Skontrolujte stavy rozhraní (`sh ip int br`), aj obsah smerovacích tabuliek (`sh ip ro`) – skontrolujte zatiaľ iba priamo pripojené siete.
6. **Nahrajte konfiguračný súbor na ISP smerovač**
   a. Na konci tohto zadania nájdete config súbor, ktorý stačí vložiť do CLI na ISP smerovači (nastavení musíte byť v globálnom konfiguračnom móde). Zrealizuje najrýchlejšia dvojica študentov, ktorí sa ako prví dostanú na riešenie tohto bodu. Učiteľ pomôže, stačí si prehodiť konzolu na ISP.
      i. Overte na ISP stav jeho rozhraní, obsah smerovacej tabuľky aj ping do internetu (ping 8.8.8.8)
   b. V obsahu konfiguračného súboru si každá dvojica skontroluje, je na konci tohto zadania, či tam vidí pre svoju topológiu spiatočné cesty, pomocou ktorých bude vedieť ISP smerovať pakety do siete vašej dvojice. Zvyšok configu analyzovať nemusíte, budeme sa učiť v ďalších týždňoch.
7. **Test IPv4 konektivity každý dvaja priami susedia**
   a. PC v LAN2 – R1

b. R1 – R2
c. R2 – PC v LAN 4
d. R2 – ISP

8. **IPv4 smerovanie na R1** (po každom kroku pozri `sh ip route`)
   a. Nastav špecifickú statickú cestu do LAN 4 cez R2
      i. Prioritne cez vrchnú trasu
      ii. Záložne cez dolnú trasu (floating....)
      iii. Po pridaní ciest over obsah smerovacej tabuľky `(sh ip ro)`
   b. Nastavte default static route pre všetku ostatnú prevádzku cez R2, ale:
      i. Prioritne cez dolnú linku
      ii. Záložne cez vrchnú trasu (floating)
      iii. Po pridaní ciest over obsah smerovacej tabuľky `(sh ip ro)`
9. **IPv4 smerovanie na R2** (zase... sh ip route)
   a. Nastav **default** static route do internetu cez ISP
   b. Skontroluj obsah smerovacej tabuľky
   c. Nastav **sumárny** statický záznam do všetkých sietí za R1 (LAN1, 2, 3) cez R1 najtesnejšie ako sa dá, a zamysli sa ktoré všetky siete do tohto sumárneho záznamu spadajú (maj na papieri), a nastav:
      i. Primárne cez hornú linku
      ii. Záložne cez dolnú linku (floating...)
      iii. Skontroluj obsah smerovacej tabuľky, a uvedom si prečo do nej pribudla iba jedna cesta.
   d. Nastav sumárny statický záznam do siete vybranej jednej susednej dvojice
      i. Cez ich R2
      ii. Skontroluj obsah smerovacej tabuľky
10. **Zrealizujte testy IPv4 konektivity v dobrej situácii**
   a. Overenie smerovacej tabuľky na vašom PC:
      i. Ak máte zapnuté obidve sieťové karty, tak si overte nasledovné (ak nemáte, tak si ich teraz obe zapnite):
      ii. Overte že v smerovacej tabuľke počítača máte dve default route (`route print`, alebo `netstat -r`)
      iii. Všimnite si že jedna má výhodnejšiu (menšiu metriku), a tá sa bude využívať
         - Ak si nie ste istý, komu patrí IP adresa, ktorá je uvedená v tej prvej default route, použite príkaz `ipconfig –all`, a nájdite tam IP adresu, ktorú ste videli pri danej default route v stĺpci Interface.
            - Mala by to byť IP adresa vašej NIC Internet (ethernet 5)
         - Mravné ponaučenie:
            - ak by sme teraz spravili test konektivity voči akejkoľvek IP adrese v internete, tak pakety budú odchádzať cez NIC Internet. S kľudom si preverte, ideálne je použiť tracert, aby ste videli kadiaľ dáta prechádzajú, cez aké IP adresy. Kúzlo/zádrhel budete vidieť hneď v tej IP adrese pri prvom skoku/hop-e.
            - My samozrejme chceme využiť NIC Cisco (ethernet 4), aby sme otestovali vašu cvičnú topológiu a konfiguráciu v nej.

- Riešenie: odteraz a navždy ... na cvičeniach, akonáhle idete robiť nejaké testy konektivity (hlavne keď už idete vyliezť z vašej LAN), tak treba NIC Internet vypnúť.

b. Pozrite na začiatok smerovaciu tabuľku na R1, aj R2 (zamyslite sa prečo tam nie sú floating static routes ? kedy budú?
c. Ping PC v LAN1 – PC v LAN4, keď OK, tak tracert na ten istý cieľ, musí ísť prvou linkou (KONTROLA 1)
d. Ping PC v LAN1: v prehliadači vzdelavanie.uniza.sk, plus tracert na daný cieľ, musí ísť druhou linkou (KONTROLA 2)
e. Ping PC v LAN 4 – PC v LAN1, keď OK, tak tracert na ten istý cieľ, musí ísť prvou linkou smerom tam (KONTROLA 3)
f. PC v LAN4: spusti hocijaký web v Internete v prehliadači (KONTROLA 4)
g. PC v LAN4: ping na vnútornú IP na R2 susednej dvojice (ak už majú aspoň default route do Inetu – toto si určite najprv preverte), tracert na ten istý cieľ, a dokáž, že nejdeš cez ISP, ale priamo na ich R2 (KONTROLA 5)

**11. Zrealizujte testy IPv4 konektivity v situácii, keď si zrušíte 1 linku**

(na jednom aj druhom konci shutdown na sériovom int.)

a. Shutdown 1. linky:
   i. pozri smerovaciu tabuľku (RT) na R1, aj R2, over že floating static route nabehla do RT na R1, R2
   ii. Ping PC v LAN1 – PC v LAN4, keď OK, tak tracert na ten istý cieľ, musí ísť druhou linkou tam (KONTROLA 6)
   iii. Ping z PC v LAN4 do PC v LAN1, keď OK, , tak tracert na ten istý cieľ, musí ísť druhou linkou tam (KONTROLA 7)
   iv. Vzbuďte naspäť vypnuté rozhranie
b. Shutdown 2. linky
   i. pozri smerovaciu tabuľku (RT) na R1, aj R2, over že floating static route nabehla do RT na R1, R2
   ii. Ping PC v LAN1 do Internetu, tracert do Internetu, musí ísť OK, pôjde prvou linkou (KONTROLA 8)
   iii. Musí chodiť aj všetko ostatné

**12. Úloha za 1 bonusový bod (dobrovoľná, ak zvýši čas na cvičení): konfigurácia rozhraní a smerovania pre IPv6**

a. zrealizujte body 5c, 5d, a body 7 až 11 pre IPv6 a ukážke výsledok (KONTROLA 1-8 pre IPv6) vyučujúcemu.

**13. Záverečné upratovanie**

a. Po skončení cvičenia nezabudnite po sebe upratať:
   i. `erase startup` (ak ste ukladali konfiguráciu do NVRAM)
   ii. Odkáblujte si svoju časť topológie a vypnite smerovače

## Konfigurácia ISP smerovača (pre učiteľa, alebo šikovného študenta):

Ak neostala na smerovači pôvodná/základná konfigurácia (IPv6 tunel a pod.), treba ju nakopírovať z flash: config-2801.txt príkazom v privilegovanom móde:

```
config replace flash:config-2801.txt
```

A k tejto základnej konfigurácii pridať toto (ctrl+c, a pravé tlačidlo myši v globálnom config móde na smerovači):

```
!
hostname ISP
!
ipv6 unicast-routing
!
interface g0/0/0
 no shut
 ip address 192.100.0.254 255.255.255.0
 ip nat inside
 no ipv6 address 2001:470:22B3::1/64
 ipv6 address 2001:470:22B3:A::254/64
!
interface g0/0/1
 no shut
 ip add dhcp
 ip nat outside
!
ip nat inside source list 1 interface g0/0/1 overload
!
access-list 1 permit 192.0.0.0 0.255.255.255
!
ip route 192.1.0.0 255.255.0.0 192.100.0.1
ip route 192.2.0.0 255.255.0.0 192.100.0.2
ip route 192.3.0.0 255.255.0.0 192.100.0.3
ip route 192.4.0.0 255.255.0.0 192.100.0.4
ip route 192.5.0.0 255.255.0.0 192.100.0.5
ip route 192.6.0.0 255.255.0.0 192.100.0.6
ip route 192.6.0.0 255.255.0.0 192.100.0.6
ip route 192.7.0.0 255.255.0.0 192.100.0.7
ip route 192.8.0.0 255.255.0.0 192.100.0.8
ip route 192.9.0.0 255.255.0.0 192.100.0.9
ip route 192.10.0.0 255.255.0.0 192.100.0.10
!
ipv6 route 2001:470:22B3:100::/56 2001:470:22B3:A::1
ipv6 route 2001:470:22B3:200::/56 2001:470:22B3:A::2
ipv6 route 2001:470:22B3:300::/56 2001:470:22B3:A::3
ipv6 route 2001:470:22B3:400::/56 2001:470:22B3:A::4
ipv6 route 2001:470:22B3:500::/56 2001:470:22B3:A::5
ipv6 route 2001:470:22B3:600::/56 2001:470:22B3:A::6
ipv6 route 2001:470:22B3:700::/56 2001:470:22B3:A::7
ipv6 route 2001:470:22B3:800::/56 2001:470:22B3:A::8
ipv6 route 2001:470:22B3:900::/56 2001:470:22B3:A::9
ipv6 route 2001:470:22B3:1000::/56 2001:470:22B3:A::10
```