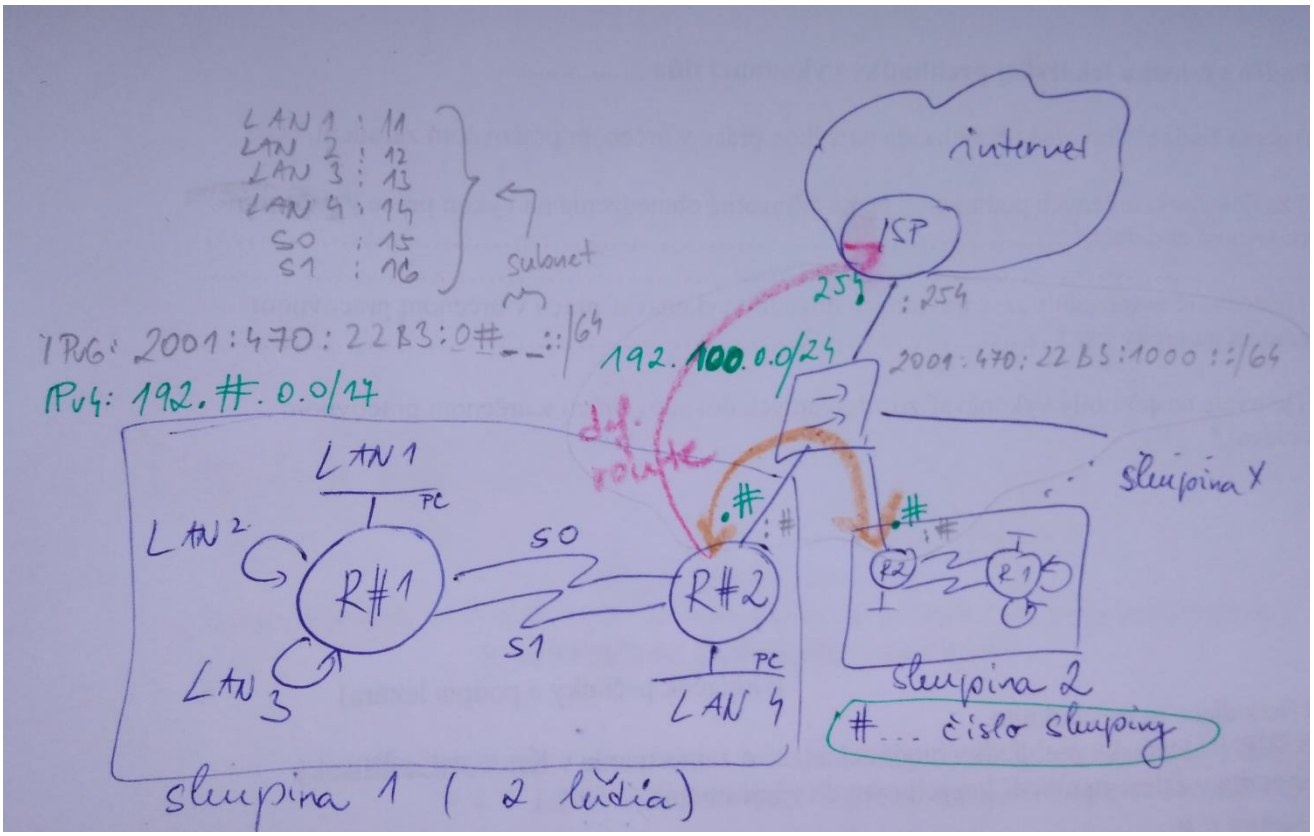
# **PS1** / Cvičenie 02 / Statické cesty

(špecifické, default, sumarizované, plávajúce)

## Topológia




## Scenár

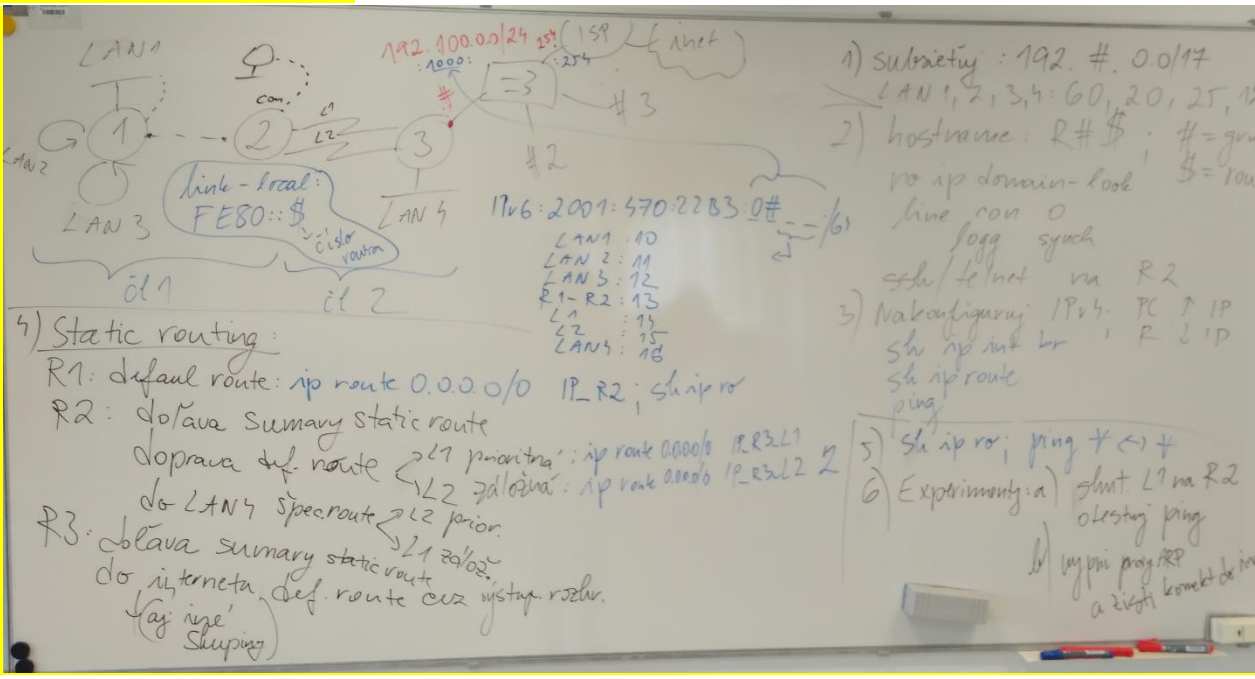
Topológiu s 2 smerovačmi rieši **dvojica** – tvoria jednu skupinu, pričom:

- 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`)

## Postup

1. **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
   b. Zakreslite si IP adresy sietí a rozhraní do obrázka, pričom počítačom prideľte najvyššiu IP adresu, smerovačom najnižšiu IP.
2. **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. Otestujte konektivitu medzi sebou aj do Internetu.
d. Tu som skoncila.... dorobit.....
e. 


## 3. Štandardný číslovaný ACL – zákaz vstupu celej LAN

a. Zakážte celej susednej LAN (v dvojici) prístup do svojej LAN, všetko ostatné povoľte. Použite číslovaný štandardný ACL, č. 3.
b. Nasaďte a otestujte vytvorené ACL, že funguje
   i. Host zo susednej LAN sa nevie pingnúť do vašej LAN.
   ii. Host zo susednej LAN môže ísť do Internetu

## 4. Štandardný pomenovaný ACL – zákaz vstupu celej LAN, okrem admina

a. Zakážte celej susedovej LAN (v dvojici) prístup do svojej LAN, iba adminovi zo susednej LAN prístup povoľ. Všetko ostatné nech je povolené. Použi štandardný ACL s menom: U4_BLOKUJ_LANx_OKREM_ADMINA
b. Nasaďte a otestuj vytvorený ACL, že funguje:
   i. Admin sa vie pingnúť do danej LAN
   ii. Host sa nevie pingnúť do danej LAN (využi Wireshark a pozri sa čo príde ako odpoveď cez ICMP - hľadaj... Communication Administratively Filtered...) , ale ide mu konektivita do Internetu
c. Uprav daný ACL tak, aby povolenie platilo aj pre druhého admina (o 1 vyššia IP adresa). Nemaž celý ACL, iba doplň pravidlo na správne miesto do súčasného ACL.
d. Otestuj vytvorený ACL, že funguje
   i. Obaja adminovia sa vedia pingnúť do vašej LAN, aj do Inetu
   ii. Host sa nevie pingnúť do vašej LAN, ale ide mu konektivita do Inetu

## 5. Štandardný pomenovaný ACL – zákaz vstupu pre jedného hosta

a. Zistili ste, že jedna zo staníc v susednej podsieti (Host), ktorá je pod správou iného administrátora (váš spolužiak z dvojice) je zdrojom mnohých problémov, ktoré ste museli v poslednej dobe vo vašej lokálnej podsieti odstraňovať. Zakážte tomuto hostovi akýkoľvek

vstup do vašej siete (zakážte všetky porty). Všetko ostatné má byť povolené. Použi štandardný ACL s menom: U5_BLOKUJ_1HOSTA

b. Otestuj vytvorený ACL
   i. susedov host sa nevie pingnúť do vašej siete.
   ii. susedov admin má plný prístup... otestuj ping
   iii. susedov smerovač má plný prístup do vašej siete, otestuj ping.

6. **Štandardný pomenovaný ACL – zakáž telnet aj SSH na svoj smerovač pre prvú polovicu**
   a. Vytvorte ACL, ktorý zakáže iba klientským staniciam TELNET prístup na router, ktorý je ich bránou do internetu, t.j. adminom prístup povolí.
      i. Použite štandardný ACL aplikovaný na rozhranie vty s menom: U6_ZAKAZ_TELNETaSSH_NA_BRANU
      ii. Uvažujte, že klienti majú IP adresy z prvej polovice a admini z druhej polovice.
   b. Otestujte funkčnosť ACL
      i. Klient (=host) sa nevie pripojiť na svoj smerovač cez telnet ani ssh.
      ii. Admin sa pripojí cez telnet aj ssh.
7. **Rozšírený číslovaný ACL – zakáž prístup na WWW a TFTP servery v LAN**
   a. Zistili ste, že niektorí klienti vo vašej LAN sieti si nainštalovali WWW a TFTP server. Z hľadiska bezpečnosti vašej sieti je to neprípustné. Aby ste predišli riziku, zakážete prístup **zvonku** do vašej siete na tieto služby.
      i. Použite rozšírený číslovaný ACL s č. 7
   b. Otestujte funkčnosť ACL:
      i. ping z PC v susednej LAN na niektorý PC vo vašej LAN – prejde OK
      ii. PC v susednej LAN sa nevie pripojiť na TFTP server na počítači vo vašej LAN (použite TFTPd utilitu na ploche vášho PC)
   c. Uprav daný ACL tak, že prístup na WWW a TFTP bude povolený iba na jednu vyhradenú IP adresu vo vašej LAN. Následne otestuj funkčnosť.
8. **Rozšírený pomenovaný ACL – zakáž 1 hostovi prístup do Inetu.. povoľ mu len http**
   a. Nové použitie jednej zo staníc (**Host**) vo vašej sieti, vás prinútilo nastaviť prísnejšie obmedzenia. Vytvorte také pravidlo, ktoré bude povoľovať danej stanici prístup na Internet len cez HTTP a HTTPs a všetky ostatné porty zakáže. ACL: U8_POVOL_IBA_WEB_1HOSTOVI
   b. Otestujte funkčnosť ACL:
      i. Admin z vašej podsiete môže pristupovať do Internetu cez FTP (nájdite si akýkoľvek otvorený FTP server na Internete, pre testovanie)
      ii. Host z vašej podsiete nemôže pristupovať cez FTP do Internetu
      iii. Host z vašej podsiete môže browsovať po Internete
9. **Riešte nasledovný firewall pomocou ACLs:**
   a. Smer VON z vašej lokálnej siete:
      i. Povoľte prístup na službu Remote Desktop Protocol (TCP/3389) v rámci celej topológie
      ii. Povoľte odpovede na službu Remote Desktop Protocol odchádzajúce z LAN siete
      iii. Prístup na službu http (TCP/80) povoľte len na susedný smerovač
      iv. Službu PING (ICMP echo) do celej topológie povoľte len stanici s poslednou použiteľnou IP adresou v LAN sieti
      v. Voľte politiku – čo nie je povolené, je zakázané
   b. Smer DO lokálnej siete:
      i. Povoľte vstup odpovedí na TCP spojenia vychádzajúce zvnútra LAN siete (nápoveda: ... established)

ii. Povoľte prístup na službu Remote Desktop Protocol na počítače v LAN sieti
iii. Povoľte zodpovedajúce prichádzajúce ICMP odpovede
iv. Voľte politiku – čo nie je povolené, je zakázané

10. **Zvýšte bezpečnosť RIP protokolu blokovaním RIP updatov na rozhraní zo svojej LAN**
    a. Ak ešte nemáte, nastavte vhodné rozhrania na smerovači ako pasívne. To vás ale neochráni proti útokom, pri ktorých by útočník z LAN generoval falošné smerovacie informácie. Preto vytvorte ACL, ktorý bude blokovať RIP updates prichádzajúce na ethernetové rozhranie z vašej LAN (UDP/520).
11. **ACL pre filtrovanie paketov v príkaze debug (možno ponechať na budúce cvičenie, kedy sa bude robiť DHCP)**
    a. Predpokladajte, že vo vašej lokálnej sieti nemáte IP adresy pre hostov pridelené staticky, ale žiadate ich od DHCP servera, ktorým je smerovač, ktorý je zároveň ich bránou do internetu. Chcete si nechať zobrazovať správy o všetkých paketoch, ktoré si vymieňajú DHCP server s ľubovoľným klientom (hostom).

       Vytvorte preto ACL pre filtrovanie IP paketov pre príkaz:
       **debug ip packet <cislo_vaseho_ACL>**

       Príkaz **debug ip packet** vám zobrazí všetky pakety prichádzajúce alebo odchádzajúce z vašeho smerovača. Vašou úlohou je ale nechať si vypisovať informácie iba o IP paketoch, ktoré sa prenášajú medzi DHCP serverom a ľubovoľným DHCP klientom (správy DHCP Discovery, Offer, Request, Acknowledgment - viac bude na prednáške o DHCP a na budúcom cvičení). DHCP komunikácia medzi serverom a klientmi sú nespojovo orientované, t.j. používajú UDP ako transportný protokol, pričom pre posielanie dát od klienta na server sa používa **UDP port 67**, a pre posielanie dát zo servera ku klientovi sa používa **UDP port 68**. (pozn.: DHCP používa rovnaké dve čísla portov, ktoré sú pridelené organizáciou IANA pre protokol bootp)