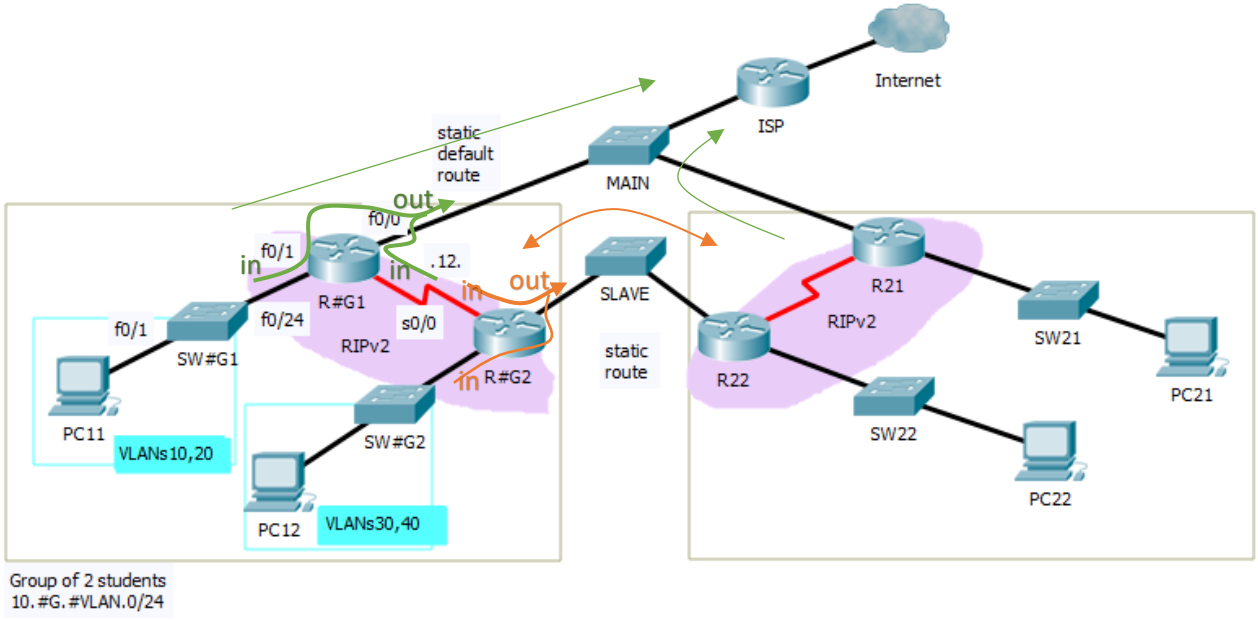
PS2 / Cvičenie 2 – typ B / **Opakovanie RIPv2, NAT, DHCPv4, ACL**

Topológia



Postup:

1. **Základná konfigurácia:**
   a. Nakreslite si topológiu na papier (aspoň jeden za dvojicu) a rozdeľte si pridelený IPv4 rozsah 10.#G.#VLAN.0/24 pre 4 VLANs (10, 20 na R1, 30, 40 na R2) a pre WAN linku medzi R1 a R2 použite ako tretí oktet číslo „***12***“. Smerovačom (subrozhraniam do VLAN) prideľte najnižšiu IP z rozsahu, prepínaču (SVI) druhú najnižšiu. Všetko si zaznačte to obrázku s topológiou.
   b. Na rozhraní smerovača R1 smerom k hlavnému prepínaču MAIN nastavte získanie adresy z DHCP servera od ISP – katedrový smerovač `(ip address dhcp)`
      i. Overte si získanú adresu, aj obsah smerovacej tabuľky - pribudne vám jedna statická cesta a default route – tú budete chcieť neskôr redistribuovať v RIPv2.
   c. Na rozhraní k susednej skupine pripojenej cez SLAVE prepínač použite rozsah 100.0.0.0/24 a pre rozhranie smerovača použite IPv4 adresu s posledným oktetom podľa čísla skupiny (100.0.0.G)
   d. Nastavte hostnames RG1, RG2, SWG1, SWG2, za G dajte číslo skupiny.
   e. 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)`
2. **VLANs a interVLAN routing**
   a. Nastavte vhodne trunk porty a access porty na prepínači
      i. Trunk 1x (fa0/24), over: `sh int trunk`
      ii. Access porty – po 5 portov do každej VLAN (na SW1 sú iba VLANy 10 a 20, na SW2 iba VLANy 30 a 40), over: `sh vlan`
   b. Vyriešte interVLAN routing na smerovačoch

i. Každý smerovač bude mať 2 subrozhrania (R1 pre VLAN 10 a 20, R2 pre VLAN 30 a 40)
ii. Počítaču dajte IPv4 adresu z prvej VLAN a prepínaču dajte IPv4 adresu z druhej VLAN (nezabudnite preň nastaviť aj default gateway – subrozhranie smerovača pre danú VLAN) a overte intraVLAN routing.

3. RIPv2

a. Nastavte RIPv2, aby ste mali konektivitu k VLANs na susednom smerovači v dvojici, neaktivujte RIP pre rozhranie vedúce k ISP, ani na rozhraní k susednej dvojici (!) pripojenej cez SLAVE prepínač, iba vo vašej vnútornej časti topológie. Do internetu máte statickú default route a k susednej skupine budete neskôr riešiť špecifickú statickú cestu.
   i. Otestujte konektivitu medzi počítačmi – s vašim kolegom v dvojici ako aj prístup (ping) na prepínač
   ii. Zabezpečte posielanie updates medzi R1 a R2 MD5 autentifikáciou cez kľúčenku s názvom KLUCENKA s kľúčom číslo 1 a heslom „*HesloHeslovate*“.
   iii. Overte funkčnosť, t.j. smerovače musia mať platné smerovacie tabuľky.
   iv. Redistribuujte z R1 default smerovaciu cestu na R2 cez RIP.

4. DHCPv4

a. Nastavte DHCP server na vašom smerovači
   i. R1: Vytvorte pool pre svoju VLAN10 a extra pool pre počítače zo susedovej VLAN40
   ii. R2: Vytvorte pool v obrátenom garde, t.j. pre svoju VLAN 30 a susedovu VLAN 20.
      - Pri oboch konfiguráciách uvažujte a nepomýľte sa s IP adresou default brány
      - Ako adresu DNS servera použite 8.8.8.8
   iii. Zabezpečte funkčnosť, t.j. pre VLAN, ktorá má DHCP konfiguráciu na susedovom smerovači aktivujte na danom VLAN subrozhraní DHCP relay agenta
   iv. Overte prideľovanie adries
      - Na PC aj na prepínači (v SVI rozhraní príkazom ip address dhcp)
      - Výpisom show ip dhcp server na dhcp servery

5. NAT

a. Na **R1** nastavte **NAT** pre odchádzajúce pakety **do Internetu – PAT s preťažením rozhrania**
   i. Na R1 nastavte preklad všetkých privátnych adries vo vašej topológii (10.#G.0.0/16) na verejnú IPv4 adresu vášho ethernetového rozhrania f0/0 vedúceho k hlavnému prepínaču a ISP
   ii. Overte prístup na internet prístupom na nejaký verejný web server: napr. www.fri.uniza.sk

b. Na **R2** nastavte **NAT** pre pakety idúce **k susednej dvojici**
   i. **Dynamické PAT (NAT overloading)**
      - Na R2 nastavte preklad všetkých privátnych adries vo vašej topológii (10.#G.0.0/16) na rozsah IPv4 adries 20G.0.0.0/24 (G je číslo vašej skupiny).
      - Nastavte na R2 statickú cestu k susednej dvojici k ich verejnému rozsahu IPv4 adries (20G.0.0.0/24) a oznamujte ju v RIPv2 `(redistribute static)` smerom dovnútra na R1. Redistribuujte aj priamo pripojené siete v RIPv2 `(redistribute connected)` – aby R1 videl aj sieť 100.0.0.0/24.
        - Overte záznamy v smerovacej tabuľke R1
        - Skontrolujte susednú dvojicu, či už má nastavenú statickú cestu k vám a či ju redistribuuje v RIPv2
      - Z vašich počítačov otestujte konektivitu cez ping na rozhranie smerovača R2 v susednej dvojici vedúce k vášmu spoločnému prepínaču SLAVE, následne pozrite záznamy cez show ip nat translations (alebo debug ip nat) – mali by tam byť viditeľné, ak nie, troubleshootuj!

ii. **Statické NAT**
- Konfiguruj na R2 statické NAT pre 2. IPv4 adresu z VLAN 10, ktoré ju bude mapovať na verejnú IPv4 adresu 20G.0.0.253
  - Nastav PC vo vlan 10 staticky druhú IPv4 adresu, s maskou, def. Gw a DNS serverom 8.8.8.8, spusti si na PC TFTP server
  - Popros kolegu v susednej dvojici, aby ti nahral na TFTP server nejaký svoj súbor, over nahranie.
    - Kolega sa musí pripájať na tvoju IPv4 adresu 20G.0.0.253. Rovnako by mal fungovať aj ping v poriadku.
  - Over záznamy v show ip nat translations!

iii. **Port forwarding**
- Konfiguruj na R2 statický port forwarding pre 2. IPv4 adresu z VLAN 40, ktorý bude mapovať túto privátnu IP adresu na verejnú IPv4 adresu 20G.0.0.254. Zároveň bude záznam mapovať vnútorný TCP port port 23 služby **TELNET** na vonkajší port 2222
  - Nastav prepínaču pre jeho SVI rozhranie vlan 40 staticky druhú IPv4 adresu z rozsahu pre VLAN 40, s maskou, def. gw a DNS serverom 8.8.8.8,
  - Konfiguruj na prepínači VTY manažment s telnet prístupom s lokálnou autentifikáciou na meno admin a heslo admin s privileg levelom 15
  - Popros kolegu v susednej dvojici, aby sa pokúsil pripojiť zo svojho počítača cez Putty Telnet na verejnú IPv4 adresu 20G.0.0.254, port 2222 na tvoj prepínač
  - over záznamy v show ip nat translations. Ping by ísť nemal, keďže port forwardingom riešite iba prístup na službu Telnet

6. **ACL**
   Každý na svojom smerovači premyslite a aplikujte ACL na subrozhrani pre VLAN s PC (VLAN 10 resp. 30) tak, aby:
   a. Smerom von z VLAN boli povolené iba:
      i. HTTPS kamkoľvek
      ii. ICMP
      iii. DNS len na 8.8.8.8
      iv. Nezabudni zvážiť, čo všetko ti v sieti okrem toho ešte beží, a je nutné, aby to ACL neblokoval, ale povoľoval:
          - Hints:
            - Klienti dostávajú IPv4 adresy dynamicky
            - Beží vám nejaký smerovací protokol
            - Chcete využívať pri browsovaní aj doménové mená
            - Prípadne iné...?
            - Čo sieťové služby ako telnet či TFP z nat časti
   b. Smerom dnu do VLANs zakáž všetko čo netreba, t.j. aby sa do vlan dostali len pakety patiace k vracajúcim sa podla ACL z bodu a)

7. **Kontrola vyučujúcim – test vytvorených ACL a celkovej konektivity v sieti bude** priebežne