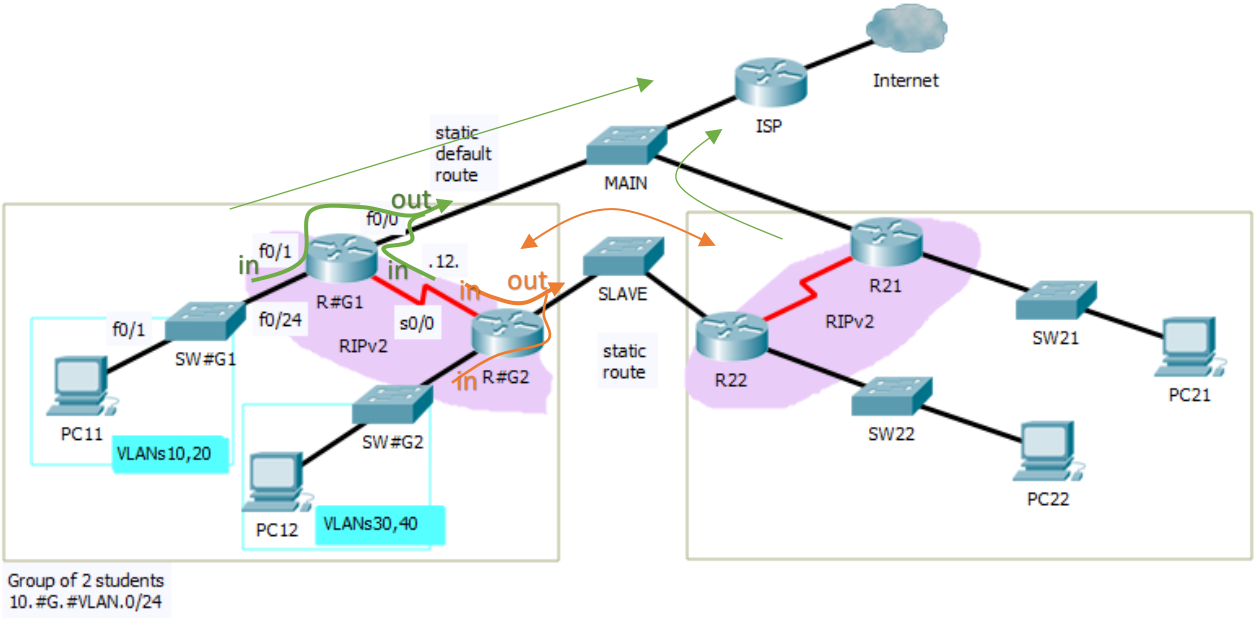
PS2 / Cvičenie 2 / **Opakovanie RIPv2, NAT, DHCPv4, ACL**

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 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
4. **DHCPv4**
   a. Nastavte DHCP server na vašom smerovači
      i. R1 – vytvorte pool pre VLAN10 a VLAN40 pre počítače zo susedovej VLAN (aby sme si vyskúšali aj relay agentov)
      ii. R2: Nezabudnite na subrozhraní pre VLAN40 nastaviť relay agenta (DHCP pool pre VLAN40 je na susednom smerovači!, takže requesty by ste mali preposielať na IP adresu R1)
      iii. R2 – vytvorte pool pre VLAN30 a VLAN20 pre počítače zo susedovej VLAN (aby sme si vyskúšali aj relay agentov)
      iv. R1: Nezabudnite na subrozhraní pre VLAN20 nastaviť relay agenta (DHCP pool pre VLAN20 je na susednom smerovači, takže requesty by ste mali preposielať na IP adresu R2)
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
   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, okrem druhej a tretej IPv4 adresy z VLAN 30, tie budeš riešiť v statickom NAT v bode ii aj iii, preto premysli ako má vyzerať ACL pre NAT) na zakúpený rozsah verejných IPv4 adries 20G.0.0.0/24 (G je číslo vašej skupiny), pričom začni od tretej použiteľnej IPv4 adresy z tohto rozsahu (prvé dve si vyhraď na adresy pre servery, ktoré budete riešiť v bode ii. Statickým NAT)
         - Nastavte na R2 statickú cestu k susednej dvojici k ich verejnému rozsahu IPv4 adries (20G.0.0.0/24) a oznamujte ju v RIPv2, redistribuujte aj priamo pripojené siete v RIPv2 `(redistribute connected)` – aby R1 videl aj sieť 100.#G.0.0.
            - Overte záznamy v smerovacej tabuľke
            - 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 vašemu spoločnému prepínaču, následne pozrite záznamy cez show ip nat translations – mali by tam byť viditeľné, ak nie, troubleshootuj!
      ii. **Statické NAT** pre 3. IPv4 adresu z VLAN 30 na verejnú IPv4 adresu 20G.0.0.1

- Popros kolegu v susednej dvojici, aby sa pokúsil pripojiť na TFTP server, ktorý si spustíš na počítači, ktorý bude mať tuto 3. privátnu IPv4 adresu, pre ktorú robíš na R2 statický NAT preklad
  - Kolega sa musí pripájať na tvoju verejnú IPv4 adresu. Rovnako by mal fungovať aj ping v poriadku.
  - Over záznamy v show ip nat translations!
    - Ak susedná dvojica zaostáva, a nemá ešte krok 5bi, použi ich smerovač R2 a z neho spravte copy run tftp – na vašu verejnú IPv4 adresu 20G.0.0.1

iii. **Port forwarding** pre 2. privátnu IPv4 adresu z VLAN 30 (IPv4 adresa prepínača) na verejnú IPv4 adresu 20G.0.0.2, so špecifikovaním protokolu TCP pre služby **SSH**, t.j. použi vnútorný port 22 a vonkajší port 2222 (ak si netrúfaš na SSH, sprav telnet, potom porty 23 a 2323)

- Popros kolegu v susednej dvojici, aby sa pokúsil pripojiť zo svojeho počítača cez SSH (alebo telnet) na verejnú IPv4 adresu 20G.0.0.2 (použi putty a zmeň port na 2222, resp. 2323), malo by ísť, a over záznamy v show ip nat translations. Ping by ísť nemal, keďže port forwardingom riešite iba prístup na službu SSH
  - Ak susedná dvojica zaostáva, pripoj sa cez SSH (resp. TELNET) z ich smerovača R2

6. ACL

Každý na svojom smerovači premyslite ACL (koľko, kde, aké, s akými pravidlami) tak, aby:

a. Smerom von z VLANs boli povolené z aplikačných služieb iba:
   i. HTTPs kamkoľvek
   ii. SSH
   iii. TFTP
   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...?

b. Smerom dnu do VLANs:
   Upozornenie: tu treba rozlišovať čo ide z Internetu a čo zo susednej skupiny, zrejme sa to nedá riešiť úplne rovnakým ACL len na inom rozhraní:
   i. http, ale iba komunikáciu, ktorá je odpoveďou na žiadosti iniciované zvnútra siete
   ii. TFTP a SSH iba od susednej skupiny, z Internetu nie
   iii. Nezabudni zvážiť, čo všetko ti v sieti okrem toho ešte beží, a je nutné, aby to ACL neblokoval, ale povoľoval:
   - Hints:
     - Niektorý klienti dostávajú IPv4 adresy dynamicky ale zo susedného smerovača
     - Beží vám nejaký smerovací protokol
     - Chcete využívať pri browsovaní aj doménové mená
     - Prípadne iné...?

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

a. Oba vaše PCs sa vedia dostať do internetu – otvor prehliadač a ukáž
b. Funguje pripojenie cez SSH na prepínač do vedľajšej skupiny
c. Funguje prenos súboru na TFTP server k susednej dvojici

d. Nefunguje TFTP ani FTP smerom do Internetu