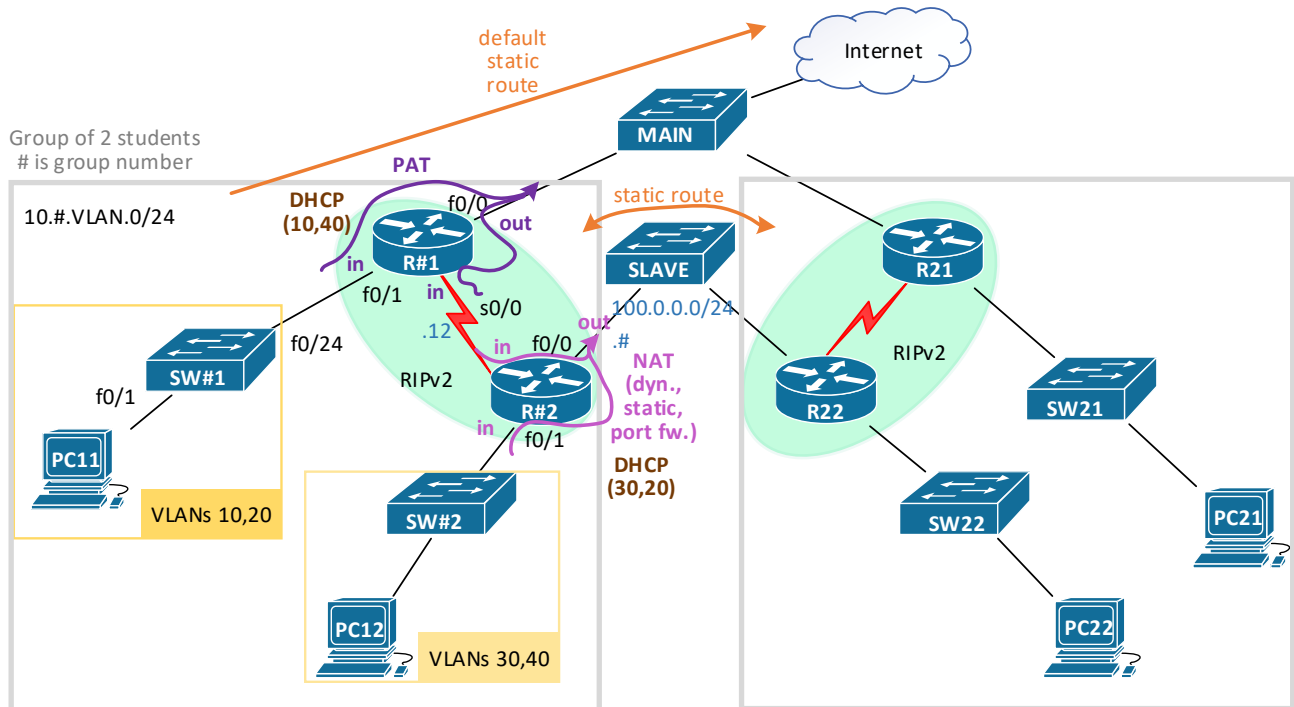


PS1 / Cvičenie 10 / NAT,DHCPv4

Topológia



Postup

1. Základná konfigurácia:

- Rozdeľte si pridelený IPv4 rozsah 10.#.VLAN.0/24 pre 4 VLANs (10, 20 na R1, 30, 40 na R2) a pre WAN linku medzi R1 a R2 použite tretí oktet .12.**
- Na prepínačoch:**
 - Nastavte hostnames SW#1, SW#2
 - Zabráňte na prepínačoch výpis hlášok do písaného textu na konzole (zmiešavanie vstupu a výstupu CMD) (line console 0, logging synchronous)
 - Vypnite prekladanie doménových mien na IP adresy (no ip domain-lookup)
 - Nastavte vhodné trunk porty a access porty na prepínači
 - Trunk 1x (fa0/24), over: `sh int trunk`
 - Access porty – po 5 portov do každej VLAN (10,20 na R1, alebo 30,40 na R2), over: `sh vlan`
 - Zapni RSTP na svojom prepínači
 - Skupina, ktorá bude popredu, overí konfiguráciu prepínačov MAIN a SLAVE (SLAVE bude prvý vyšší prepínač nad prepínačom MAIN v strednom racku): Či je `vlan.dat` prázdna, či nie je prítomný `startup-config`
 - Kvôli vzdialenému prístupu pridajte prepínaču najvyššiu IPv4 adresu (.254) z VLAN 10 ak ste na SW1 alebo z VLAN 30 ak ste na SW2. (Už vieme, že je lepšie oddeliť manažmentovú VLAN od user VLANs, v tomto zadání to ale spravíme jednoduchšie, aj keď menej bezpečne).
 - Počítaču dajte druhú najvyššiu IP z VLAN 10 ak je to PC1, alebo z VLAN20 ak je to PC2, pripojte ich do správnych portov na prepínačoch

- Overte intraVLAN routing, ping na svoj prepínač, a vzdialene sa naň prihláste
- c. **Na smerovačoch:**
- i. Nastavte hostnames R#1, R#2
 - ii. Vyriešte **interVLAN routing** na oboch smerovačoch
 - Každý smerovač bude mať 2 subrozhrania (R1 pre VLAN 10 a 20, R2 pre VLAN 30 a 40)
 - Smerovačom pridelte najnižšiu IP z rozsahu.
 - Overte **intraVLAN** routing, ping z PC na router (subrozhranie pre VLAN 10).
 - Na prepínači dokonfigurujte default gateway – IPv4 adresa subrozhrania smerovača pre danú VLAN (10 ak ste na SW1, 30 ak ste na SW2)
 - Overte **interVLAN** routing:
 - Počítaču zmeníte IPv4 adresu z VLAN 20 ak ste na PC1 a z VLAN 40 ak ste na PC2, zapojte počítače do správnych portov, a ping z PC na SW (sú teraz v iných VLAN). Musí ísť. Overte aj či sa viete vzdialene prihlásiť z PC na svoj prepínač.
 - iii. Na **R1** na rozhraní k hlavnému prepínaču nastavte získanie adresy z DHCP servera od ISP – katedrový smerovač (`ip address dhcp`)
 - Overte si získanú adresu, aj obsah smerovacej tabuľky - pribudne vám jedna statická cesta a default route – tú budete chcieť neskôr redistribuovať v RIPv2 (v bode d.)
 - Overte z R1 ping do internetu (napr. ping 8.8.8.8)
 - iv. Na **R2** na rozhraní k susednej skupine použite rozsah 100.0.0.0/24 a pre svoje rozhranie použite IPv4 adresu s posledným oktetom podľa čísla skupiny (100.0.0.#)
 - Overte stav rozhraní `sh ip int br`, pozrite čo vidieť v smerovacej tabuľke `sh ip route`
- d. **RIPv2**
- i. Na oboch smerovačoch nastavte RIPv2, aby ste mali konektivitu k VLANs na kolegovom smerovači, s ktorým ste spolu v dvojici, **nespúšťajte RIP pre rozhranie vedúce k ISP, ani k susednej dvojici (smerom na SLAVE)**, iba vo vašej časti topológie.
 - ii. Na **R1** oznamujte default static route v RIPv2 updatoch (`default-information originate`)
 - iii. Skontrolujte obsah smerovacích tabuliek a otestujte konektivitu medzi počítačmi PC1 a PC2 vo vašej dvojici
 - Teraz sú vo VLAN 20 a 40
 - iv. Na R2 overte, či v smerovacej tabuľke vidíte redistribuovanú default route z R1 (riadok **R***)

2. DHCPv4

- a. Nastavte DHCP server na vašom smerovači
 - i. **R1** – vytvorte pool pre svoju VLAN10 a pool pre VLAN40 pre počítače zo susedovej VLAN (aby sme si vyskúšali aj relay agenta)
 - **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 – ktorúkoľvek jeho IP, ale zvyčajne sa definuje IP toho rozhrania, ktoré je najbližšie k DHCP serveru (t.j. susednému smerovaču))
 - ii. **R2** – vytvorte pool pre svoju VLAN30 a pool pre VLAN20 pre počítače zo susedovej VLAN (aby sme si vyskúšali aj relay agenta)

- **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 – ktorúkoľvek jeho IP, ale zvyčajne sa definuje IP toho rozhrania, ktoré je najbližšie k DHCP serveru (t.j. susednému smerovaču))
- iii. Over funkčnosť:
 - Svoj PC daj do portu v prvej VLAN (10 ak si na PC1, 30 ak si na PC2) a nastav dynamické získanie IPv4 adresy, over či si ju dostal, a testni ping ku kolegovmu smerovaču, alebo PC. Ak je všetko OK, pokračuj:
 - Svoj PC potom daj do portu v druhej VLAN (20 ak si na PC1, 40 ak si na PC2), a over či si dostal správnu IPv4 adresu, a testni ping ku kolegovmu smerovaču, alebo PC.

3. NAT

- a. Na **R1** nastavte **NAT** pre odchádzajúce pakety **do Internetu – PAT s preťažением rozhrania**
 - i. Na R1 nastavte preklad všetkých privátnych adries vo vašej topológii (10.#.0.0/16) na verejnú IPv4 adresu vášho ethernetového rozhrania f0/0 vedúceho k hlavnému prepínaču a ISP
 - ii. Overte funkčnosť:
 - ping 8.8.8.8 v internete z PCs
 - ak na PC nastavíš aj DNS server, tak si zobraz nejaký web v prehliadači
- b. Na **R2** nastavte **NAT** pre pakety idúce **k susednej dvojici** (aby sme si vyskúšali ďalší typ NATka)
 - i. **Dynamické PAT (NAT overloading) na R2:**
 - Na **R2** nastavte preklad všetkých privátnych adries vo vašej topológii (10.#.0.0/16, okrem posledných dvoch IPv4 adries z VLAN 30, tie budete riešiť v statickom NAT v bode ii a iii, preto premysli ako má vyzeráť ACL, ktorý špecifikuje tieto privátne IPv6 adresy pre NAT) na zakúpený rozsah verejných IPv4 adries 20#.0.0.0/24 (kde # je číslo vašej skupiny), pričom vynechajte posledné dve IPv4 adresy z rozsahu (.253, .254 si vyhradte ako verejné adresy pre servery, ktoré budete riešiť v bode ii a iii pri statickom NAT a port forwarding)
 - Nastavte na **R2** statickú cestu k susednej dvojici k **ich verejnému rozsahu** IPv4 adries (20#.0.0.0/24) a oznamujte ju v RIPv2 (`redistribute static`), redistribuuje aj priamo pripojené siete v RIPv2 (`redistribute connected`) – aby R1 videl aj sieť 100.#.0.0.
 - Overte záznamy v smerovacej tabuľke **oboch** smerovačov
 - Skontrolujte susednú dvojicu, či už má nastavenú statickú cestu k vám a či ju redistribuuje v RIPv2 (t.j. či má tiež vyriešený tento bod i.)
 - Z vašich **oboch počítačov** otestujte konektivitu cez ping na rozhranie f0/0 smerovača R2 v susednej dvojici vedúce k prepínaču SLAVE, následne pozrite záznamy cez `show ip nat translations` – mali by tam byť viditeľné, ak nie, troubleshootuj!
 - Poznámka: Nemá význam skúšať ping z vašich PC na PC v susednej skupine, pretože neviete akú verejnú IPv4 dostali v dynamickom NAT, ktoré majú nakonfigurované na ich R2, smerom k vám.
 - Kto sa ale nebojí experimentov, môže dynamicky pridelenú verejnú IP pre počítač zistiť v NAT prekladovej tabuľke (`sh ip nat translations`) a pokúsiť sa spraviť ping na ňu k susedom (zistiť treba na R2).

- ii. **Statické NAT** (stále na R2) pre predposlednú IPv4 adresu z VLAN 30 (.253) na verejnú IPv4 adresu 20#.0.0.253
- Následne to otestuj:
 - Svoj **PC2** daj do portu pre VLAN 30 a nastav statickú IPv4 adresu (.253)
 - Spusti na PC2 TFTP server cez utilitu TFTPd, nastav priečinok kde máš práva zápisu (niečo typu: ..Student\Documents)
 - Najprv otestuj funkčnosť svojho TFTP servera na PC2, a z R1 vo vašej topológii ulož konfiguráciu na TFTP server bežiaci na vašom PC2 (použi jeho privátnu IP) (`copy runn tftp`)
 - Potom popros kolegu v **susednej** dvojici, aby najprv pingol verejnú IP tvojho TFTP servera, a potom sa pokúsil uložiť na TFTP server napr. konfiguráciu z ich R1 alebo R2 (`copy run tftp`, a zadať treba verejnú IPv4 adresu daného TFTP servera)
 - Upozornenie: vyber si ale takú susednú dvojicu, ktorá už má otestovaný a funkčný bod 3.b.i. tohto zadania.
 - Over záznamy v `show ip nat translations`!
- iii. **Port forwarding** (stále na R2) pre IPv4 adresu prepínača **SW2** (posledná privátna IPv4 adresa z VLAN 30, .254) na verejnú IPv4 adresu 20#.0.0.254, so špecifikovaním protokolu TCP pre službu **SSH**, t.j. použi vnútorný port 22 a vonkajší port napr. 2222 (ak si netrúfaš na SSH, sprav telnet, potom porty 23 a 2323)
- Popros kolegu v susednej dvojici, aby sa pokúsil pripojiť zo svojho počítača cez SSH (alebo telnet) na verejnú IPv4 adresu 20#.0.0.254 (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 (a všetky ostatné služby na danú IP nie sú zvonku NATkom povolené)
 - Ak susedná dvojica zaostáva, pripoj sa cez SSH (resp. TELNET) z ich smerovača R2 na svoj prepínač SW2