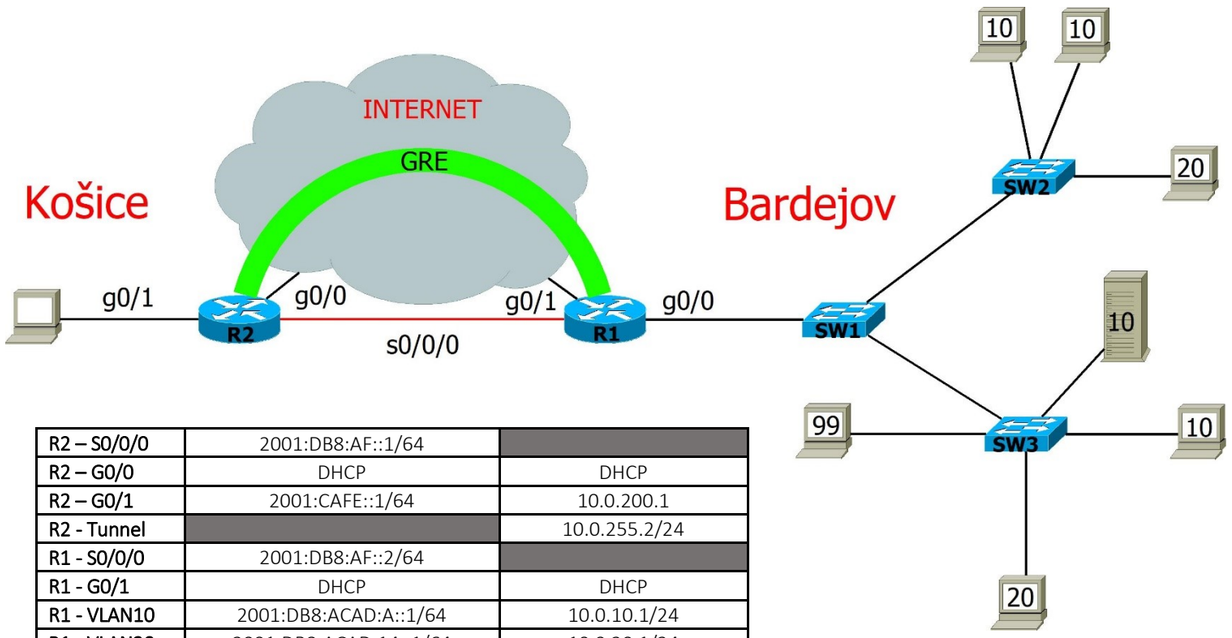

R2 – S0/0/0	2001:DB8:AF::1/64	
R2 – G0/0	DHCP	DHCP
R2 – G0/1	2001:CAFE::1/64	10.0.200.1
R2 - Tunnel		10.0.255.2/24
R1 - S0/0/0	2001:DB8:AF::2/64	
R1 - G0/1	DHCP	DHCP
R1 - VLAN10	2001:DB8:ACAD:A::1/64	10.0.10.1/24
R1 - VLAN20	2001:DB8:ACAD:14::1/64	10.0.20.1/24
R1 - VLAN99	2001:DB8:ACAD:63::1/64	10.0.99.1/24
R1 - Tunnel		10.0.255.1/24
ISP -> R1	2001:DB8:F::F	190.37.25.1
ISP -> R2	2001:DB8:A::BAD	25.0.0.1

Predkonfigurácia, dôležité informácie a troubleshooting

Ste sieťovým inžinierom v rozvíjajúcej sa národnej spoločnosti. V nedávnej minulosti pribudla do Vašej siete nová pobočka v Bardejove (Lokálna sieť na pravej strane), ktorú predkonfiguroval Váš kolega, ktorý Vám zanechal neúplne popísanú topológiu a tabuľku adries (na obrázku hore). Jeho úlohou bolo nakonfigurovať nasledovné:

- V pobočke Košice
  - Konfiguráciu súkromnej adresy na PC
  - Konfiguráciu IPv6 adries na PC a rozhraniach smerovača s0/0/0 a g0/1

Do dnešného dňa táto konfigurácia ide bezchybne.

- V pobočke Bardejov
  - Konfiguráciu VLAN na prepínačoch – rozdelenie portov na access/trunk
  - Konfiguráciu IPv6 adries na PC, sériovom rozhraní S0/0/0 a podrozhraniach g0/0.X
  - Konfiguráciu IPv4 adries na podrozhraniach g0/0.X
  - Konfiguráciu DHCP servera pre prideľovanie všetkých adries v súkromnej sieti
  - Staticky priradenú IP adresu pre PC vo VLAN 99
  - Konfiguráciu inter VLAN smerovania v IPv4 a IPv6
  - Konfiguráciu port-security na prepínači SW1 pre limitovanie maximálneho počtu MAC adries na **20** prichádzajúcich cez porty spájajúce SW1 s prepínačmi access vrstvy (SW2 a SW3).

Pri overovaní konfigurácie však boli zaznamenané **3 samostatné nezrovnalosti**, **ktoré je vašou úlohou nájsť a odstrániť.** Konfigurácia musí spĺňať body pôvodného zadania, ktoré mal Váš kolega. Zistené chyby boli nasledovné:

- Pri spustení počítačov a priraďovaní DHCP adries sme si všimli, že DHCP adresy sú priraďované iba počítačom vo VLAN 10. Nedokázali sme však identifikovať zdroj problému, avšak vieme, že DHCP server je nastavený bezchybne.
- Po niekoľkých sekundách od zapnutia počítačov sme stratili spojenie s prepínačom SW2 ako aj všetkými k nemu pripojenými počítačmi.
- Počítač vo VLAN 99 nie je schopný komunikácie s nikým v sieti ako pri použití IPv4, tak pri použití IPv6.

Poznámka: Možno Vás zaujme skutočnosť, že ping v IPv6 medzi počítačmi vo VLAN 10 a 20 pripojených k SW3, ide bezchybne.

V prípade, že sa Vám nepodarí identifikovať a opraviť chyby, nezúfajte – **každá ďalšia úloha môže byť vypracovaná nezávisle od vyriešenia problému.** IPv4 riešenia bude možné aj bez vyriešenia problémov overovať voči serveru, a PC vo VLAN 10 na prepínači SW3. IPv6 riešenia bude možné overovať voči rovnakým zariadeniam + počítaču vo VLAN 20 na prepínači SW3. **Pri konfigurácii smerovania, NAT a podobne však zahrňujte aj siete, ktoré Vám nefungujú!**

Rozvoj siete a komunikácie medzi pobočkami

1. Prvou úlohou pri rozvoji siete je nakonfigurovať pripojenie k internetu v protokole IPv6 na oboch smerovačoch (R1 aj R2).
   a. Pri konfigurácii smerovačov, získajte IPv6 adresy na rozhrania pripájajúce sa k ISP v internete prostredníctvom DHCP
   b. Na výmenu adries s ISP použite OSPF nasledovne:
      i. Používajte OSPF s číslom 1
      ii. Siete spájajúce Vás a ISP majú byť na oboch smerovačoch v oblasti 0
      iii. Všetky vnútorné siete v Bardejovskej pobočky majú byť v oblasti 10
      iv. Vnútorná sieť Košickej pobočky má byť v oblasti 20
      v. Ak budete potrebovať pri konfigurácii akýkoľvek iný paramater, použite ľubovoľný.
      vi. Po tomto bode by sa mali všetky Vaše zariadenia pingnúť

2. Druhou úlohou je konfigurácia floating statickej cesty v IPv6, ktorá bude využívaná na komunikáciu prostredníctvom pomalých sériových rozhraní, v prípade, že by sa v OSPF vyskytol problém.
   a. Na smerovači R2 vytvorte 3 statické cesty (jednu pre každú používanú IPv6 sieť v Bardejove), pričom pri výbere AD použite AD ktorú používa RIPv2.
   b. Na smerovači R1 vytvorte 1 statickú cestu smerujúcu k dosiaľ jedinej vnútornej IPv6 sieti v Košiciach. Použite presnú masku a rovnakú AD ako v predchádzajúcom kroku.
   c. Pri konfigurácii statických ciest **používajte IP adresy**, nie východzie rozhrania smerovača.

   Po tejto konfigurácii je naša IPv6 plne funkčná a môžete ju považovať za plne nakonfigurovanú.

3. Konfigurácia pripojenia do internetu prostredníctvom IPv4.
   a. Pri konfigurácii smerovačov, získajte IPv4 adresy na rozhrania pripájajúce sa k ISP v internete prostredníctvom DHCP
   b. Okrem toho, na smerovač R2 nakonfigurujte IP adresu 10.0.200.1/24 na rozhranie G0/1
   c. Pre informácie o IP adresách v internete použite BGP nakonfigurované nasledovne:
      i. Na smerovači R2 používajte číslo autonómneho systému 20
      ii. Na smerovači R1 používajte číslo autonómneho systému 10
      iii. ISP, prepájajúci naše autonómne systémy má číslo autonómneho systému 1111
      iv. V žiadnom prípade do internetu neoznamujte siete so súkromnými adresami
      v. Po úspešnej konfigurácii by sa mali pingnúť Vaše smerovače medzi sebou

4. Konfigurácia PAT a statického NAT
   a. Na smerovači R1 nakonfigurujte NAT nasledovne:
      i. Povoľte preklad akejkoľvek IP adrese vo VLAN sieťach 10,20 a 99. Žiadným iným IP adresám nesmie byť preklad umožnený. Pre vytvorenie pravidiel použite štandardný ACL s menom ***10_20_99***
      ii. IP adresy musia byť prekladané za verejnú IP adresu získanú od ISP cez DHCP v predchádzajúcom kroku
      iii. Umožnite prístup na webový server pre protokoly HTTP a HTTPS, pričom na prístup k HTTP užívateľ v internete použije adresu 190.37.250.101:50000 a na prístup k HTTPS použije adresu 190.37.250.101:50001
   b. Na smerovači R2 nakonfigurujte PAT nasledovne:
      i. Povoľte preklad iba IP adrese patriacej počítaču a žiadnej inej - Pre vytvorenie pravidiel použite štandardný ACL s menom ***POVOL_PC***
      ii. IP adresa musí byť prekladaná za verejnú IP adresu získanú od ISP cez DHCP v predchádzajúcom kroku

   Po tomto kroku si musí vedieť počítač z Košíc prehliadať WEB na serveri v Bardejove. Okrem toho musí každý z počítačov vedieť pingnúť verejné adresy v internete.

5. Konfigurácia VPN
   a. Využite výhodu technológie VPN a zabezpečte, aby komunikácia medzi Bardejovskou a Košickou pobočkou nemusela nutne využívať NAT pri prechode internetom a aby sa koncovým používateľom aj pri použití traceroutu javilo, že neopúšťajú sieť 10.0.0.0/8. Na zabezpečenie takého správania využite GRE tunel, pričom konfiguráciu vykonajte nasledovne:
      i. Číslo tunel rozhrania má byť 0.
      ii. Začiatok a koniec tunela vytvorte medzi verejnými rozhraniami smerovačov R1 a R2
      iii. Na smerovači R2 nastavte IP 10.0.255.2/24
      iv. Na smerovači R1 nastavte IP 10.0.255.1/24
   b. Následne zabezpečte statické smerovanie súkromných adries cez GRE tunel nasledovne:
      i. Na smerovači R2 vytvore 3 statické cesty – Jednu pre každú z Bardejovských VLAN 10,20,99
      ii. Na smerovači R1 vytvorte 1 statickú cestu s presnou maskou jedinej vnútornej siete v Košiciach
      iii. Pri konfigurácii statických ciest **používajte IP adresy**, nie východzie rozhrania smerovača.

   Po tomto kroku by malo byť možné pingnúť akýkoľvek PC a tiež prístup na web z Košíc využitím adresy http://10.0.10.2 resp. https://10.0.10.2