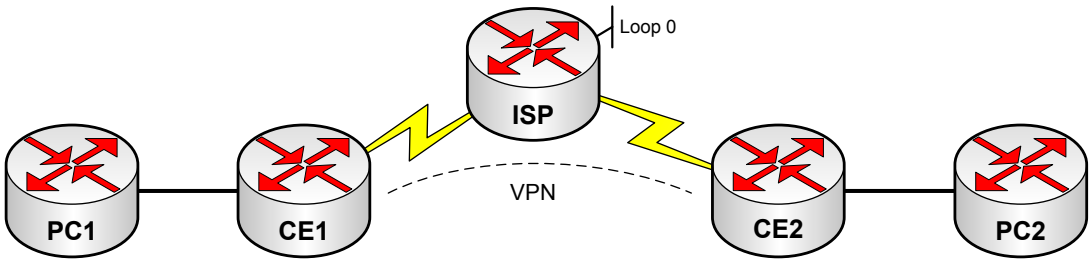
Point-to-point GRE VPN tunel a preklad adries pomocou NAT



Úlohy:

1. Ubezpečte sa, že sú zariadenia čisté, prípadne ich vyčistite. Nakonfigurujte zariadeniam hostname a zapojte ich podľa zobrazenej topológie.
2. Nakonfigurujte zariadeniam IP adresy, clock rate na sériových linkách a zapnite rozhrania.
   - Lokálne siete (PC-CE) budú mať adresy X0.X0.X0.0 /24, kde X je číslo smerovača.
   - Loop 0 rozhranie ISP bude mať IP adresu 1.2.3.4 /32 (simuluje Internet).
   - Pre siete medzi CE a ISP použite ľubovoľné /28 podsiete z rozsahu 172.16.0.0 /24.
   - Pre sieť VPN použijete adresu 192.168.0.0 /24.
3. Pomocou ping overte komunikáciu medzi priamo pripojenými zariadeniami.
4. Na smerovačoch PC (simulujúcich koncové stanice) nakonfigurujte predvolenú statickú cestu cez IP adresu príslušného CE smerovača. Na smerovačoch CE (customer edge) nastavte predvolenú statickú cestu cez sériové rozhranie. Komunikácia medzi CE smerovačmi by už mala fungovať.
5. Medzi CE smerovačmi vytvorte GRE tunel, ktorý predstavuje sieť VPN.
   - Vytvorte tunelové rozhranie a prideľte mu IP adresu z rozsahu pre VPN.
   - Ako zdroj tunelu nastavte lokálne sériové rozhranie.
   - Ako cieľ tunelu nastavte IP adresu sériového rozhrania vzdialeného CE smerovača.
6. Pomocou ping z CE na adresu pridelenú druhej strane tunela overte jeho úspešné vytvorenie.
7. Nakonfigurujte smerovanie medzi CE smerovačmi v rámci VPN pomocou OSPF. Do smerovacieho procesu zahrňte len lokálnu sieť a tunel (nie sériové linky).
8. Overte zobrazením smerovacej tabuľky a pomocou ping medzi PC1 a PC2.
9. Skontrolujte či ISP vie smerovať do koncových (lokálnych) sietí. V smerovacej tabuľke by sa nemali nachádzať. Ping medzi PC a 1.2.3.4 by nemal fungovať.
10. Na CE nastavte lokálnu sieť ako vnútornú a sériovú linku ako vonkajšiu z hľadiska NAT.
11. Na CE1 nakonfigurujte statický preklad IP adresy PC1 na poslednú použiteľnú adresu príslušnej sériovej linky. Overte pomocou ping z PC1 na 1.2.3.4 a zobrazte tabuľku prekladov na CE1.
12. Na CE2 vytvorte ACL, ktorý povolí príslušnú lokálnu sieť vstúpiť do prekladacieho procesu a nakonfigurujte PAT, ktorý bude prekladať adresy identifikované týmto ACL na adresu sériového rozhrania. Overte pomocou ping z PC2 na 1.2.3.4 a zobrazte tabuľku prekladov na CE2.
13. Na PC2 umožnite vzdialený prístup cez telnet. Na smerovači CE2 nakonfigurujte preposielanie TCP komunikácie prichádzajúcej na sériové rozhranie na port 8000 na IP PC2 na port 23. Overte vytvorením telnet spojenia na adresu sériového rozhrania CE2 cez port 8000.
14. Na CE2 vytvorte rozsah 10 nepoužitých adries (NAT pool) zo siete VPN a nakonfigurujte dynamický NAT, ktorý bude prekladať adresy identifikované ACL z úlohy 12 na adresy vytvoreného poolu. Na CE2 nastavte tunelové rozhranie ako vonkajšiu sieť pre NAT.
15. Overte funkčnosť dynamického NAT pomocou ping medzi z PC2 na PC1, pričom na PC1 aktivujte debug ip icmp a sledujte, na akú IP adresu PC1 odpovedá. Overte taktiež zmeny v tabuľke prekladov na CE2.

Doplnkové úlohy:

16. Na smerovačoch PC zobrazte tabuľku CDP susedov.
17. Na PC2 nastavte IP adresu z podsiete PC1 a na CE lokálnych rozhraniach (ethernetových) odstráňte nakonfigurované IP adresy.

18. Na CE smerovačoch vytvorte tzv. pseudowire tunel tak, aby smerovače PC boli prepojené v rámci VPN na druhej vrstve.
    - Vytvorte pseudowire triedu, ktorá bude použitá vo VPN na odvodenie konfiguračných parametrov spojenia. V tejto triede nastavte tunelovací protokol L2TPv3 a zdroj signalizačných správ nech je sériové rozhranie.
    - Na rozhraniach smerom k PC vytvorte xconnect spojenie k cieľu špecifikovanému IP adresou sériového rozhrania na opačnom CE smerovači. Konfiguračné parametre spojenia odvoďte od vytvorenej pseudowire triedy.
19. Overte vytvorenie VPN zobrazením relačných informácií pre L2 tunely. Overte L2 konektivitu smerovačov CE v rovnakej VPN zobrazením CDP susedov. Pomocou ping overte, či vedia spolu komunikovať a pomocou traceroute skontrolujte cez aké smerovače L3 komunikácia prechádza.

Command summary

```
  !konfigurácia GRE tunela
Router(config)# interface tunnel <number>
Router(config-if)# ip address <ip-address> <subnet-mask>
Router(config-if)# tunnel source { <interface> | <local-ip-address> }
Router(config-if)# tunnel destination <remote-ip-address>
Router(config-if)# tunnel mode gre ip
  !overenie konfigurácie tunelového rozhrania
Router# show interfaces tunnel <number>

  !vytvorenie ACL na identifikáciu adries, ktoré sa majú prekladať
Router(config)# access-list <num> permit <lan-network> <wildcard-mask>
  !identifikácia rozsahu adries, na ktoré bude NAT prekladať
Router(config)# ip nat pool <name> <first-ip> <last-ip> netmask <mask>
  !mapovanie ACL na POOL pre dynamické NAT (s preťažením)
Router(config)# ip nat inside source list <acl> pool <pool> [overload]
  !mapovanie ACL na adresu konkrétneho rozhrania pre PAT
Router(config)# ip nat inside source list <acl> interface <int> overload
  !statický preklad adries
Router(config)# ip nat inside source static <local-IP> <global-IP>
  !port forwarding – preposielanie komunikácie na určitý port
Router(config)# ip nat inside source static <protocol> <local-IP> <local-port>
{<global-IP> | interface <int>} <global-port>
  !označenie ktoré rozhranie patrí do vnútornej siete a ktoré do vonkajšej
Router(config-if)# ip nat {inside | outside}

  !verifikácia NAT
Router# show ip nat translations
Router# show ip nat statistics
Router# clear ip nat translations *
Router# clear ip nat statistics
Router# debug ip nat

  !konfigurácia triedy pseudowire
Router(config)# pseudowire-class <pw-class-name>
Router(config-pw-class)# encapsulation l2tpv3
Router(config-pw-class)# ip local interface <interface>
  !konfigurácia pseudowire na rozhraní
Router(config-if)# xconnect <peer-IP-address> <virtual-circuit-number> [pw-class
<pw-class-name>]
  !verifikácia vytvorenia L2 tunela
Router# show l2tun tunnel
Router# show l2tun session
```