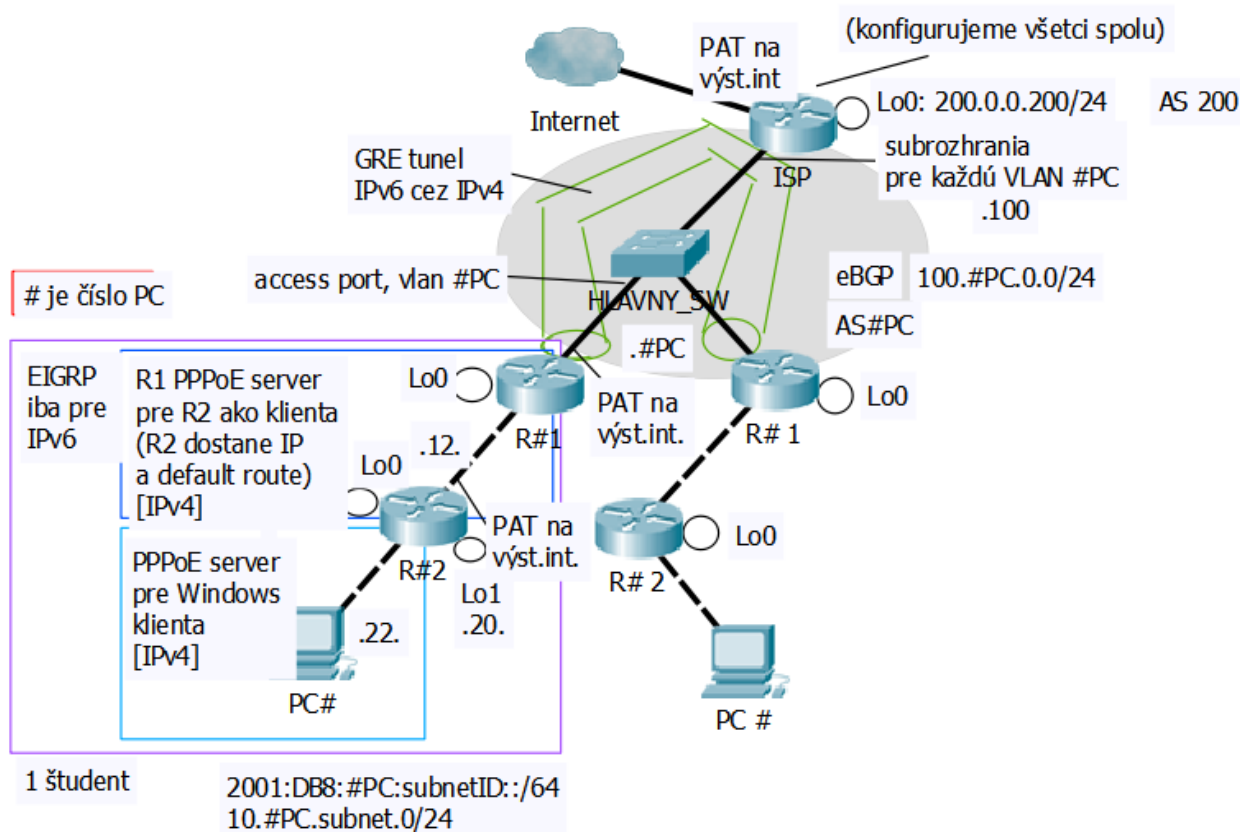


PS2 / Cvičenie 10 / Opakovanie

PPPoE, eBGP, GRE tunel IPv6 cez IPv4, EIGRP, VLANs

Topológia

Každý študent má dvojicu smerovačov. Všetci sú napojení na spoločný prepínač HLAVNY_SW, ktorý je spojený s ISP smerovačom, ktorý má uplink do Internetu. HLAVNY_SW aj ISP smerovač konfigurujú študenti, spoločne, nie učiteľ.



Scenár

Spoločnú sieť medzi ISP a smerovačmi R#1 od študentov chceme oddeliť do odlišných IPv4 adresných rozsahov. Keďže ale ISP smerovač nemá 16 fastethernet rozhraní pre pripojenie 16 študentských topológií, tak využijeme iba jedno rozhranie a spravíme na ňom subrozhrania. Prepínač HLAVNY bude mať preto rozhrania vedúce k topológiám študentov ako access vo VLAN #PC, rozhranie k ISP bude trunk.

Nad touto časťou topológie, vyznačené šedým oválom, rozbehneme eBGP protokol, študenti nebudú oznamovať ISP nič, všetko budú NATovať na svoju vonkajšiu IPv4 adresu. Na ISP treba zabezpečiť, aby ISP posielala cez eBGP default route.

Keď je eBGP funkčné, cieľom je cez túto IPv4 časť mať konektivitu do Internetu – vyriešiť NAT smerom do Internetu.

Následne svoju topológiu s 2 smerovačmi a 1 PC nakonfigurujete s IPv6 adresami, a rozbehnete EIGRP pre IPv6. Keď budete mať IPv6 konektivitu vo svojej topo koniec-koniec, cieľom je prepojiť sa s kolegom v dvojici (dá sa riešiť aj trojica, ale treba premyslieť) tak, že sa vždy dve študentské IPv6 topológie prepoja GRE tunelom cez IPv4 sieť (vedie cez ISP). Smerovanie sa vyrieši zapojením tunelovacieho rozhrania s IPv6 adresami do EIGRP procesu. Overí sa konektivita v dvojici z PC na PC v IPv6.

Na záver sa zopakuje PPPoE, ale budete riešiť všetko u seba vo svojej topo, teraz už len pre IPv4. R1 bude server pre R2, ktorý získa IPv4 adresu z poolu na R1 aj default gateway, R2 bude server pre PC, ktoré

dostane IPv4 adresu z R2 aj default gateway. Doriešite NAT na R2 aby všetky IPv4 adresy z LAN s daným PC smerovač prekladal na IPv4 adresu výstupného rozhrania, doriešite aj NAT na R1 tak, aby prekladal IPv4 adresy 10.#PC.12.0 na IPv4 adresu výstupného rozhrania k ISP. Overíte konektivitu z PC do Internetu, mala by ísť.

IP adresovanie

Celkový adresový plán predpokladá univerzálne adresovanie, z ktorého sa budú tvoriť subsiete. Aby sa odstránili duplicity, predpokladáme (# je číslo počítača):

1. Keď budete konfigurovať IPv6 adresy, nastavte aj link-local adresy, na R1 všetky rozhrania fe80::1, na R2 všetky fe80::2
2. Smerom k učiteľskému smerovaču ISP použite 100.#PC.0.0/24
 - a. Na R#1: 100.#PC.0.#PC/24
 - b. Na ISP: 100.#PC.0.100/24 na subrozhraní f0/0.#PC
(dokonfiguruje si každý sám na ISP, alebo jeden študent pre všetkých)
3. Vo vašej časti topológii
 - a. Medzi vašimi smerovačmi použite verejný IPv4 adresný rozsah:
 - i. medzi R1-R2:
 - 10.#.12.0/24, (.1 na Lo0 na R1, R2 dostane IP od R1, keď sa autentifikuje neskôr v PPPoE)
 - 2001:DB8:#PC:12::/64 (:1 na R1, :2 na R2)
 - ii. LAN s PC:
 - 10.#.22.0/24, (.1 na Lo0 na R2, PC získa IP adresu od R2, keď sa autentifikuje neskôr v PPPoE)
 - 2001:DB8:#PC:22::/64 (:1 na R2, :2 na PC)
 - b. Na každom smerovači navyše loopback rozhranie:
 - i. loopback Lo1 na R#1: 10.#PC.10.1/24, 2001:DB8:#PC:10::1/64
 - ii. loopback Lo1 na R#2: 10.#PC.20.1/24, 2001:DB8:#PC:20::1/64
 - c. IPv6 rozsah pre rozhrania v GRE tuneli:
 - i. 2001:DB8:100::/64, :#PC posledný hexet na rozhraniach
(budete konfigurovať neskôr pri riešení GRE tunela v postupe)

Postup

1. Základná konfigurácia:

- a. Hostname na všetkých smerovačoch zvolte #R@ (# je číslo PC, @ je číslo smerovača)
 - i. 1R1, 1R2
 - ii. 2R1, 2R2
 - iii. ...atď.
- b. Pre synchronizáciu hlášok posielaných smerovačom (napr. výstup debugovania) s príkazmi, ktoré zadávate do konzoly ako admin, nastavte: logging synchronous, pre konzolovú linku: line con 0
- c. Nastavte si heslo pre vty aj do privilegovaného módu
- d. Nakonfigurujte IPv4 adresy a IPv6 adresy vo vašej topológii pre sérové rozhrania na smerovačoch, aj loopbacky podľa IP adresného plánu vyššie (2.a, 2.b)
- e. Teraz aj priebežne po každom kroku si zálohujte konfiguráciu (`copy run start`)

2. Konfigurácia ISP smerovača a prepínača HLAVNY

Nakonfiguruje ich najrýchlejšia dvojica študentov, ostatní sa vzdialene prihlásia na ISP aj HLAVNY

a skontrolujú si konfiguráciu pre pripojenie svojej topológie, a overia funkčnosť. Pozor, ak je na ISP nejaká konfigurácia, tak ju zmažte.

a. HLAVNY_SW

- i. Nakonfigurujte vzdialené prihlásenie na prepínač (line vty 0 15 !!!, heslo aj na vty aj do privileg. levelu)
- ii. Rozhranie vedúce k študentským smerovačom nakonfigurujte ako access vo VLAN #PC
- iii. Rozhranie k ISP ako trunk

b. ISP

- i. Nakonfigurujte vzdialené prihlásenie na smerovač (line vty 0 15 !!!, heslo aj na vty aj do privileg. levelu)
- ii. Rozhranie k prepínaču HLAVNY aktivuje a nakonfiguruje subrozhrania f0/0.#PC s IP adresami 100.#PC.0.100/24, so značkováním dot1q pre VLAN #PC
- iii. Nakonfigurujte NAT tak, aby sa prekladali všetky vnútorné IPv4 adresy 100.#PC.0.0/24 na IPv4 adresu vonkajšieho rozhrania f0/1, ktorú ISP získa cez DHCP od katedrového servera. Overte aj získanú default route.

c. Overte funkčnosť

- i. Ping z ISP do internetu
- ii. Ping R#1 na subrozhranie pre svoju VLAN na ISP
- iii. Ping z R#1 do Internetu ešte nepôjde, default route potrebujete získať cez eBGP (ďalší krok)

3. eBGP smerovanie medzi ISP a skupinami študentov (single homed)

a. nakonfigurujte peering svojho smerovača R1 s ISP cez eBGP

- i. ako vaše číslo AS použite číslo vášho PC
- ii. v sieti ISP je AS číslo 200
 - vzdialene sa pripojte na ISP a nastavte na ňom peering so svojím R#1
 - skontroluj, či má v smerovacej tabuľke default route a či ju oznamuje cez eBGP, ak nie, zabezpeč to konfiguráciou (network 0.0.0.0 mask 0.0.0.0) a over na svojom R#1 či ju dostal cez eBGP
- iii. R1 nebude oznamovať nič, ale potrebujete nastaviť NATovanie celej svojej IPv4 siete na svoje výstupné rozhranie k ISP
 - Nastavte NAT na R1

b. skontrolujte:

- i. BGP peering (sh ip bgp neighbor)
- ii. smerovacie tabuľku (sh ip ro bgp)
- iii. BGP tabuľku (sh ip bgp, sh ip bgp summary)
- iv. Konektivitu k topológiám ostatných študentov – k ich smerovaču R#1

4. IPv6 topo s EIGRP

- a. IPv6 bude iba vo vašej časti topológie, nie k ISP !
- b. Nakonfigurujte IPv6 adresy pre sériové rozhrania smerovačov, aj loopbacky Lo 1 podľa IP adresného plánu vyššie, aj PC, ak ešte nemáte.
- c. Rozbehnite EIGRP pre IPv6
 - i. Skontrolujte
 - smerovaciu tabuľku
 - konektivitu z PC k Lo1 na R1

5. Vytvorte IPv6 GRE tunel cez IPv4 sieť ISP

- a. Overte že aktuálne neexistuje konektivita medzi vašimi PC v dvojici v IPv6
 - i. Ping medzi PCs v skupine v IPv6
- b. Nakonfigurujte začiatok a koniec tunela medzi hornými smerovačmi R#1, pričom použite:
 - i. číslo tunel rozhrania 0
 - ii. **IPv6** adresy v tunely z rozsahu – 2001:DB8:100::/64, :#PC posledný hexet na rozhraniach
 - iii. Zadefinuj začiatok a koniec tunela – verejné **IPv4** adresy!
 - iv. Zahrňte tunelovacie rozhrania do EIGRP dynamického smerovania pre IPv6
- c. Overte
 - i. Stav rozhraní (sh ip int br)
 - ii. Stav GRE tunel rozhrania (sh int tunnel 0)
 - iii. Smerovaci tabuľku
 - iv. Konektivitu medzi PC v dvojici

6. Smerovač R1 ako PPPoE access koncentrátor (server)pre R2

- a. Nakonfiguruj PPPoE server

```

int lo 0
  ip address 10.#PC.12.1 255.255.255.0
username #R2 password #R2pass
username #R2 autocommand logout
! Pool adries pre klientov
ip local pool PPPoE-POOL 10.1.13.2 10.1.13.20
! Virtual template (pozor, pri NATku sa sem dava ip nat inside!!!)
interface virtual-template 1
  ip unnumbered loop 0
  mtu 1492
  ppp mtu adaptive
  peer default ip address pool PPPoE-POOL
  ppp authentication chap
  ppp ipcp dns 158.193.152.2
  ip nat inside
! Asociuj template s PPPoE grupou
bba-group pppoe global
  virtual-template 1
! Nastav template na rozhranie
interface f0/0
  pppoe enable group global
  no shut

```

7. Doriešite aj NAT na R1

- a. tak, aby prekladal IPv4 adresy 10.#PC.12.0 na IPv4 adresu výstupného rozhrania k ISP.

8. Smerovač R2 ako PPPoE dialer (klient/customer)

- a. Zapnite debug ppp negotiation, debug ppp authentication
- b. Nastavte rozhranie Dialer 1 na svojom smerovači

```

int dialer 1
  mtu 1492
  ip address negotiated
  encapsulation ppp
  dialer pool 1
  ppp chap hostname #R2
  ppp chap password #R2pass
  ppp ipcp route default

```

- c. Priradte Dialer na fyzické rozhranie

```

interface f0/1

```

```
pppoe enable
pppoe-client dial-pool-number 1
no shut
```

d. Skontrolujte:

i. Na vašom smerovači:

- prezrite výpisy debugov (už by malo byť niečo vidieť), následne debug vypnite
- pridelenie IP adresy na rozhraní Dialer 1 (sh ip int br)
- default route v smerovacej tabuľke
- show pppoe session, show int dialer (pozri MTU a enkapsuláciu, ...)
- konektivitu z R2 na R1
- konektivitu z R2 do Internetu (predpokladom je funkčné NAT na R1 aj na ISP – už ste riešili vyššie)
 - debuguj ak je problém, sh ip nat translations

9. Doriešte NAT na vašom spodnom smerovači R2

a. tak, aby všetky IPv4 adresy z LAN s daným PC smerovač prekladal na IPv4 adresu výstupného rozhrania

- i. Pozn.: Toto je potrebné na to, že vám pribudla IPv4 default route R2, ale R1 nemá žiadne statické cesty smerom k vám – bol by problém nastaviť takéto statické cesty, keďže IP adresu na rozhraní vašeho smerovača R2 vedúceho k R1 získavate z local pool-u od R1, čo je náhodný proces, a IP adresa môže byť vždy iná.

ii. Čo treba:

- ip nat inside – pozor toto ide pri PPPoE na virtual template rozhranie !
- ip nat outside – pozor toto ide na dialer 1 !
- ACL – jasné
- ip nat inside source list 1 interface dialer 1 overload

b. Overte že funguje:

- i. z R2 ping 8.8.8.8 source 10. #.22.1

- ak toto ide, určite pôjde aj ping z PC neskôr v nasledovnom bode

10. Smerovač ako PPPoE access koncentrátor (server) + Windows ako PPPoE klient

a. Nastavte váš smerovač ako PPPoE server pre Windows klientov vo vašej LAN.

- i. Nastavte username a heslo pre Windows klientov pre PPPoE autentifikáciu na R2:

```
username PC password cisco
username PC autocommand logout
```

- Logout slúži na to, aby sa daný človek s daným kontom nemohol prihlásiť napr. na konzolu, ak je na nej zadané login local

- ii. Nastavte IP adresu pre Lo rozhranie (použije sa ako IP pre virtual template neskôr) ak ešte nemáte

```
int Lo 0
ip add 10.#.22.1 255.255.255.0
```

- iii. Nastavte lokálny pool adries pre PPPoE klientov

```
ip local pool POOL_KLIENTI 10.#.22.2 10.#.22.250
```

- iv. Vytvorte Virtual-template 1 s parametrami:

```
interface Virtual-Template 1
ip unnumbered Loopback0
peer default ip address pool POOL_KLIENTI
mtu 1492
```

```

ppp mtu adaptive
ip tcp adjust-mss 1452
ppp authentication ms-chap-v2 ms-chap chap
ppp ipcp dns 158.193.152.2

```

v. Vytvorte bba-group

```

bba-group pppoe global
virtual-template 1
sessions per-mac throttle 1000 2 1

```

- Throttle je tam na zmiernenie requestov, ktoré neustále generuje Windows:

- Ak príde 1000 requestov vrámci 2 sekund, smerovač zablokuje danú MAC na 1 minútu, t.j nebude spracovávať správy prichádzajúce od nej.

vi. Priradíte bba-group na fyzické rozhranie

```

interface FastEthernet 0/0
pppoe enable group global
no shutdown

```

b. Zapnite debugovanie PPP správ

```

debug ppp authentication
debug pppoe event

```

c. Nastavte váš počítač s OS Windows ako PPPoE klienta

i. Ovládací panel > Sieť/Network center:

- Internet NIC vypni, Cisco NIC zapni
- Set up new internet connection > Connect to Internet (anyway) > Broadband PPPoE (skip)

ii. Výsledkom bude nové rozhranie, ktoré treba zapnúť a zadať dohodnuté Meno/Heslo

d. Skontrolujte:

i. Na smerovači:

- prezrite výpisy debugov (už by malo byť niečo vidieť), následne debug vypnite
- `show pppoe session`
- `show ip int brief` – pozrite nové rozhrania, stavy a IP

ii. Na počítači:

- pridelenie IP adresy (`ipconfig /all`)
- default route v smerovacej tabuľke (`netstat -r`)
- konektivitu z PC ku Lo0 na svojom smerovači
- konektivitu z PC ku R2, do Internetu

11. Záverečné upratovanie

- Zmaž uloženú konfiguráciu na všetkých svojich smerovačoch (`erase startup`)
- Odkábluj, vypni zariadenia