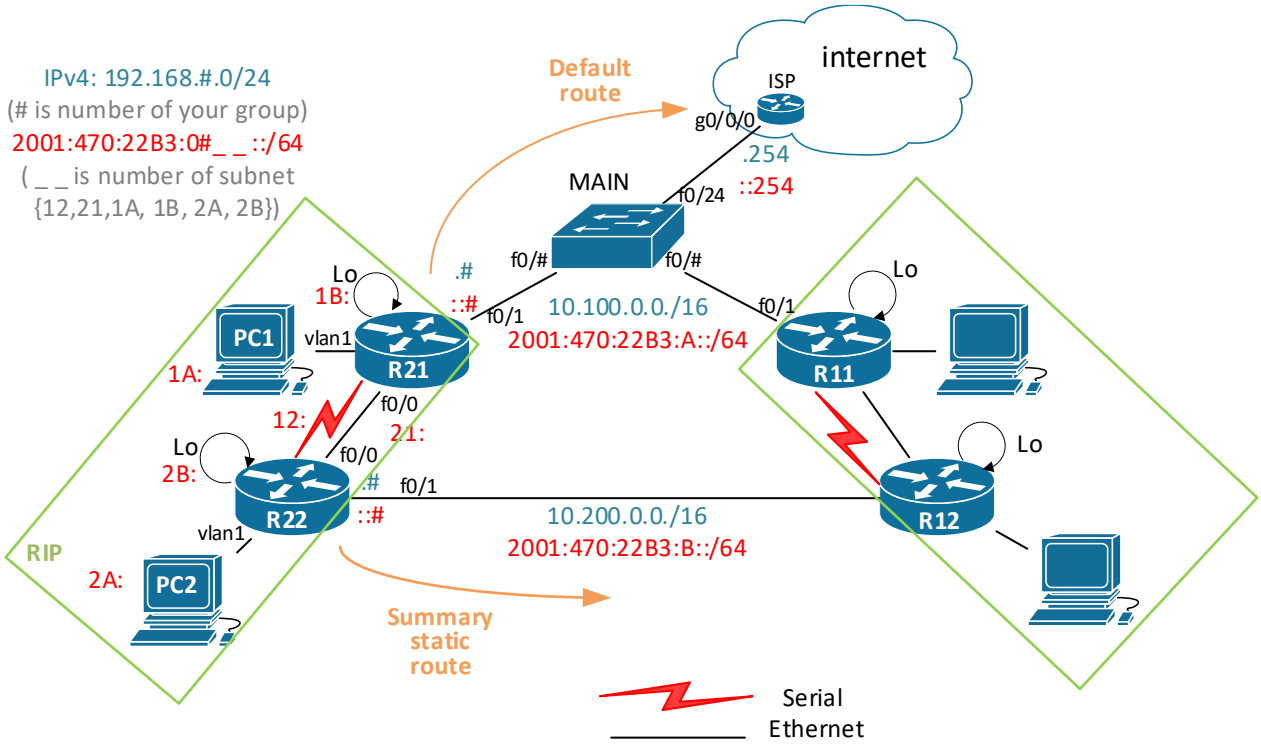
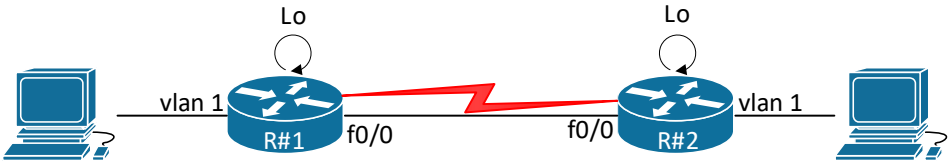
PS1 / Cvičenie 03 / **RIPv2, RIPng**

Topológia



Inštrukcie

- pracuje sa v dvojiciach, jeden človek má jeden smerovač, a spolupracujú vždy dve dvojice študentov spolu v topológii vyššie (ideálne rady stolov v labe)
- všetky dvojice sú pripojené na MAIN prepínač
- oba vaše smerovače potrebujú 3 ethernetové rozhrania, preto využite dve fastethernet rozhrania (f0/0, f0/1), a jeden port z karty Cisco HWIC-4ESW (4 portový modul, konfigurovať sa bude ako `int vlan 1`)
    - v labe RB303 máme viac ako 20 smerovačov ktoré majú aj Cisco HWIC-4ESW !
- ISP smerovač nakonfiguruje najrýchlejšia dvojica študentov, pripojí topológiu do internetu, konfiguračný súbor je na konci tohto zadania. Nezabudnite overiť funkčnosť po nahratí súboru (`sh ip int br, sh ip ro, ping 8.8.8.8`)
- kroky, ktoré sú v postupe tohto zadania zvýraznené modrým, je potrebné si zdokumentovať (to ukážete na koniec vyučujúcemu), poväčšine pôjde o:
    - **screenshot** smerovacej tabuľky a výstupu `sh ip protocols`, cez snipping tool vo Windowse, vyznačte čo je v danom výpise zaujímavé a sledované v danom kroku, obrázky ukladajte do priečinka, alebo do wordu
    - kde sa robí s **Wiresharkom**, spravíte **screenshot** aj z pohľadu na hlavičky pri odchytení RIP update, a zvýrazníte dôležité veci
- **začnite v takejto topológii:**



RIPv2

1. **Pripojenie sa na konzolu prepínača a smerovača a kontrola default stavu**
   Pozn.: Pokiaľ vidíte, že pri stojanoch je príliš veľa ľudí naraz, robte zatiaľ bod 3.a., 3.b., a akonáhle sa uvoľní priestor, pokračujte v tomto bode 1.
   a. **Pred káblovaním** si iba nabootujte svoj smerovač (nezapájajte do neho zatiaľ žiadne iné káble okrem konzoly), overte či nemá uložený config v NVRAM, a pokiaľ je tam nejaká konfigurácia, zmažte ju a spravte reload smerovača.
2. **Zapojte si topológiu**
   Pozn.: Pokiaľ vidíte, že pri stojanoch je príliš veľa ľudí naraz, robte zatiaľ bod 3.a, 3.b., a akonáhle sa uvoľní priestor, pokračujte v tomto bode 2. Ideálny počet ľudí je jedna dvojica pri každom stojane.
   a. Zapojte zariadenia podľa obrázku s topológiou, dodržte rozhrania pokiaľ je to možné.
      i. Pri niektorých rozhraniach môže byť krížik vyznačený fixkou, čo znamená, že dané rozhranie nie je funkčné, vtedy použite iné rozhranie, alebo si vymeňte zariadenie.
3. **Základná konfigurácia:**
   a. Spravte **VLSM subsieťovanie** z prideleného rozsahu: 192.168.#.0/24, pre siete LAN s počítačom a siete s Lo rozhraním s týmito požiadavkami:
      i. Veľkosť LAN aj virtuálnej Lo0 siete je 8 IP adries (8 už je vrátane adresy siete aj broadcast adresy)
      ii. Prideľte subsiete od najnižšej v tomto poradí pre tieto siete (aby sme boli konzistentný aj s inými skupinami):
         - 1. LAN/PC1, 2. R1/Lo0, 3. LAN/PC2, 4. R2/Lo0
   b. Pre linky **medzi smerovačmi** použite tieto IPv4 subsiete (pozn.: chceme tam mať inú major network, aby sme mohli neskôr robiť experimenty s automatickou sumarizáciou):
      i. Serial: 192.168.#1.0/30 (napr. pre skupinu 5 je to: 192.168.51.0/30)
      ii. Ethernet: 192.168. #2.0/30 (napr. pre skupinu 5 je to: 192.168.52.0/30)
   c. Nastavte **hostname** R#1, R#2 (pre skupinu/grupu 5 je to R51, R52)
   d. Overte čo máte (resp. nemáte :-) na začiatku v smerovacej tabuľke `sh ip route`
      i. Nemalo by tu byť teraz nič
   e. Nakonfigurujte IPv4 adresy na smerovačoch (4x) aj na počítačoch podľa svojho VLSM návrhu
      i. Smerovačom dajte najnižšiu IP, počítačom najvyššiu z daného rozsahu
   f. Overte stav rozhraní `sh ip int br`, pozrite čo vidieť v smerovacej tabuľke `sh ip route`
      i. Vidíte všetky priamo pripojené siete?
         - Na každom smerovači musia byť 4 priamo prepojené siete, a vo výpise o rozhraniach 4 rozhrania v stave up up – ak nie ste v tomto stave, nepokračujte ďalej, ale vyriešte problém so stavom rozhraní !
      ii. Vzdialené siete zatiaľ nie je vidieť, čo je v poriadku, viete prečo?

4. **Spustite RIPv1 a odsledujte správanie**
   a. Spustite RIP na oboch smerovačoch, s týmito požiadavkami:
      i. Nekonfigurujte zatiaľ version 2 (ostane predvolená version 1)

ii. Pridajte siete cez `network` príkaz (3x):
- Pre siete vedúcu k vašemu PC a sieť na Lo stačí jeden príkaz – major network, v našom prípade triedy C
  - Pozn.: z prednášky vieme, že tieto siete musíme zaradiť do network príkazu, pretože „O tejto sieti chcem informovať svojich susedov."
- A rovnako treba pridať aj siete medzi smerovačmi – obe linky, aj serial, aj ethernet – obe major networks
  - Pozn.: z prednášky vieme, že tieto siete musíme zaradiť do network príkazu, pretože „Do týchto sietí chcem a budem posielať RIP updates."
- Pozor ! nepridávaj sieť 10.0.0.0 ! Nemá byť súčasťou RIP!

b. Skontrolujte výpisy a zamerajte sa na:

i. Čo a prečo to vidíme v smerovacej tabuľke? `(sh ip route)`
- Pribudli cesty do vzdialených sietí, keď sme spustili RIPv1?
  - Mali by.
- Dôkladne preskúmajte smerovaciu tabuľku, a uvedomte si, prečo smerovač vaše siete (LAN a Lo) sumarizoval:
  - Hint: viď prednáška – keď smerovač posiela update o sieti X rozhraním, ktoré patrí do inej major network, ako je tá do ktorej spadá sieť X, tak danú sieť sumarizuje classfull spôsobom, u nás na 192.168. #.0/24 (pri automatickej sumarizácii, ktorá sa pri RIPv1 nedá vypnúť)
  - Spravte ping medzi počítačmi, mal by prejsť.
    - V smerovacích tabuľkách je záznam o remote sieťach za susedným smerovačom, takže je všetko v poriadku.
    - Na zamyslenie: V poriadku by nebola konektivita v takej topológií, keby za smerovačom R2 bol ešte jeden smerovač R3, takisto s RIPv1 a automatickou sumarizáciou, ktorá sa nedá vypnúť.
      - V smerovacej tabuľke R2 by sa v tejto situácií objavil záznam o vzdialenej sieti 192.168. #.0/24 (sumarizovaný záznam, major network, class C), pričom v časti cez koho je možné sa dostať do týchto sietí (tzv. „via") by boli uvedený obaja susedia s metrikou 1, čiže aj R1 aj R3.
      - Dôsledkom by bolo, že pakety smerované do subsietí spadajúcich do major netwotk 192.168. #.0/24 by smerovač R2 potom v rámci load balancing rozhadzoval medzi svojich dvoch susedov R1 a R3, čo by malo za následkoch výpadky konektivity, pretože za R1 sú iba niektoré subsiete, a za R3 by boli zase nejaké iné.
      - Čiže v tomto prípade by nastal problém nazývaný ako „network discontinuity".

ii. Pozrite nastavenia RIP a posielanie RIPv1 updates `(sh ip protocols)`

iii. Pozrite výpis debugu, čo sa posiela a kam, čo prijíma (`debug ip rip`), pričom:
- Pred debugovaním je vhodné mať funkčné vzdialené prihlásenie na dané zariadenie (telnet alebo SSH, pre istotu, keby konzola prestala reagovať)

- debug zrušíte `undebug all`, alebo `no debug ip rip`

c. Spravte Wireshark capture RIPv1 správy – preskúmajte hlavičky IP, UDP, RIPv1 update:
   i. Na počítači si spustite Wireshark, dajte filter na rip, a preskúmajte hlavičky – spravte aj screen shot, ale takto:
      - rozbaľ si vo WS Ethernet hlavičku (pozri cieľovú MAC), L3 (IP) a L3 (UDP) netreba rozbaľovať, ale všimni si cieľovú IPv4 adresu a cieľový port, a rozbaľ si obsah RIP správy
      - Pozn.: Zatiaľ rozhranie vedúce k počítaču nie je nastavené ako pasívne, takže sa ním posielajú RIPv1 updates, a vieme ich čítať vo Wiresharku

5. Spustite RIPv2 a odsleduj výsledok

a. Nastavte version 2
b. Nechajte automatickú sumarizáciu (by default)
c. Skontrolujte výpisy `show ip route`, `sh ip protocols`, `debug ip rip`, zamerajte sa na:
   i. Dôkladne preskúmajte smerovaciu tabuľku, a uvedomte si, prečo smerovač vaše siete (LAN a Lo) sumarizoval:
      - Hint: viď prednáška – keď smerovač posiela update o sieti X rozhraním, ktoré patrí do inej major network, ako je tá do ktorej spadá sieť X, tak danú sieť sumarizuje classfull spôsobom, u nás na 192.168. #.0/24 (pri zapnutej automatickej sumarizácii – defaultne je zapnutá, vypínať ju budeme neskôr)
   ii. debug zrušíš `undebug all`, alebo `no debug ip rip`
d. Otestuj ping zo svojho PC na kolegove PC v dvojici, malo by prejsť.
e. Preskúmajte nekonečnú slučku pri smerovaní:
   i. Z PC1 pošli paket, do neexistujúcej subsiete z vašej major network, napr. 192.168.#.32/29, napríklad ping 192.168.#.33. Samozrejme bude neúspešný, ale:
      - Použi tracert do daného cieľa 192.168.#.33.
        - Sleduj ako si to dané dva smerovače prehadzujú medzi sebou (až kým nevyprší TTL).
f. Wireshark capture RIPv2 správy – preskúmaj hlavičky v tomto poradí: RIPv2 update - response, UDP, IP, Ethernet
   i. Pozn.: Ak beží Wireshark v promiskuitnom móde, vie zobrať aj to, čo nie je určené pre dané PC a jeho sieťovú kartu (napr. RIPv2 odoslaný multicastom pre susedné smerovače)

6. Vypnite automatickú sumarizáciu a odsleduj efekt

a. Vyriešte nekonečnú slučku vypnutím automatickej sumarizácie na oboch smerovačoch
   i. `no auto-summary` na oboch svojich smerovačoch
   ii. `sh ip route`, `sh ip protocols`
      - skontroluj ako v smerovacej tabuľke teraz vidíš siete LAN a Lo svojho kolegu v dvojici
      - Niekedy môžeš proces urýchliť zmazaním všetkých ciest v smerovacej tabuľke, a počkáš kým sa naplní znova: R# clear ip route *
   iii. Odsleduj znovu tracert do daného (neexistujúceho) cieľa 192.168.#.33 z vášho PC. Už váš smerovač by mal takýto ICMP paket zahodiť, nevznikne smerovacia slučka.
   iv. Skontroluj stále funkčnú konektivitu medzi PC1 a PC2 (ping..).

7. Nakonfigurujte manuálnu sumarizáciu

a. Skontrolujte najprv obsah smerovacej tabuľky
b. Sumarizujte svoju LAN a sieť Lo0 a prinúťte smerovač posielať update o tejto sumarizovanej sieti a nie jednotlivých sieťach cez obe sériové linky
    i. `ip summary-address` ...
        - pozor píše sa na výstupnom rozhraní, ktorým má odísť informácia o sumarizovanej sieti (čiže obe vaše linky ku kolegovi v dvojici)
c. `sh ip route` (ako sa mi zmenšila RT? Koľko vzdialených sietí ste videli pred sumarizáciou, a koľko vidíte teraz?), `sh ip protocols` (ako to tam vidím)

8. Preskúmajte využiteľnosť dvoch redudantných liniek medzi R1-R2

a. Pomocou `ping` s prepínačom –t otestujte dostupnosť z PC1 k PC2 a k Lo2 svojho kolegu
    i. Zistite či sa používa per-packet load ballancing, alebo per-destination load ballancing
        - Pozn.: Tu bude asistovať učiteľ, pretože použije sa debug ip packet na smerovači, ale v kombinácií s rozšíreným ACL na icmp request (toto bude v predmete až neskôr, tu len využijeme jeden ACL, ktorý máte nižšie, učiteľ vysvetlí)
            - `Router(config)# access-list 100 permit icmp any any echo`
            - `Router# debug ip packet 100`
        - Pozn.: Pokiaľ na konzole nevidíte výstup debugovania, spravte ping priamo zo smerovača:
            - `Router# ping IP_PC1 source vlan1`
                - a odsledujte výstup z debug-u (za IP dosaď čo treba...)
            - `Router# ping IP_Loop source vlan1`
                - a odsledujte výstup z debug-u (za IP dosaď čo treba...)
b. Na záver zrušte debugovanie: undebug all (alebo: no debug ip packet **100**)

9. Nastavte pasívne rozhrania

a. R#1: nastavte všetky rozhrania ako pasívne (`passive-interface default`) a zrušte passive na tých rozhraniach, kde to nie je vhodné
b. R#2: nastavte ako pasívne iba tie rozhrania, kde je to vhodné (špecificky vymenuj)
c. `sh ip protocols` – je tam vidieť aktuálne pasívne rozhrania?
d. Overte že konektivita vo vašej skupine sa neporušila

10. Redistribúcia default route

a. Na R#1:
    i. Pripojte tento smerovač do internetu cez hlavný prepínač, a nakonfiguruj si IP adresu pre toto rozhranie 10.100.0.#/16
        - `sh ip int br` (musí byť up/up)
    ii. Nakonfigurujte static default route smerom do internetu cez 10.100.0.254 (ISP smerovač, ktorý predkonfiguroval učiteľ, robí NAT preklad privátnych adries na verejnú IP, a má pripojenie do internetu)
        - `sh ip route` – musí tam byť viditeľná vytvorená defaultná statická cesta
        - `sh ip protocols` – pozrite čo pribudlo
    iii. Ohláste default route v RIPku (default information-originate)
b. Na R#2:
    i. `sh ip route` – vidí smerovač preposlanú default route?

c. Na počítačoch:
   i. Nastav DNS na 8.8.8.8
   ii. Otestuj konektivitu do Internetu
d. Presvedčte sa, že keď váš počítač pošle nejaký paket do nejakej neexistujúcej podsiete, ktorá spadá do sumarizovaného rozsahu vášho kolegu, tak opäť aj tu vznikne smerovacia slučka (spôsobí ju defult route, ktorú má smerovač R2, tú samozrejme potrebujeme, len si ukážeme aký problém môže vzniknúť v tejto situácií)
   i. Spravte shutdown svojho Lo0 (obaja)
      - Pozn.: keďže naša sumarizácia je tak tesná, že do nej spadajú iba dané dve siete (LAN a Lo), tak si nasimulujeme, že jedna je nedostupná.
   ii. Zo svojho PC spravte `tracert` na IP adresu kolegovho Lo (ktoré je teraz vypnuté)
      - Sledujte vzniknutú smerovaciu slučku
e. Vyriešte danú smerovaciu slučku pridaním discard route na vašom smerovači
   i. ip route ... *vaša sumarizovaná sieť s maskou*... null0
      - Upozornenie: Pozor pri tomto prípade, nedávate za ip route vzdialenú sieť, ale vašu lokálnu, sumárnu, ktoré zahŕňa obe vaše siete s PC aj s Lo.
   ii. overte, že už nevznikne smerovacia slučka:
      - zo svojho PC spravte tracert na IP adresu kolegovho Lo (ktoré je teraz vypnuté). Príde to až po kolegov smerovač, a ten by mal takýto ICMP paket zahodiť (vďaka discard route), nevznikne smerovacia slučka.
f. Na koniec pokusov v tomto bode znova zapnite Lo (t.j. no shut).

11. Redistribúcia statických ciest a priamo pripojených sietí (ktoré nie sú zahrnuté v RIP smerovaní)

a. Na R#2:
   i. Prepojte sa s jednou vybranou skupinou cez smerovače R#2
      - Prepojte sa vhodným ethernetovým káblom (podľa best)
      - Nakonfiguruj si IP adresu pre rozhranie (10.200.0.#/16), over že je v stave up/up, otetuj konektivitu k susednému smerovaču
   ii. Nakonfiguruj statickú cestu k vybranej skupine cez dané ethernetové rozhranie, snaž sa vytvoriť sumárny statický záznam (stačí /24)
      - over viditeľnosť - `sh ip route`
   iii. Redistribuj statické cesty v RIP (redistribute static)
      - Pozri zmenu v `sh ip protocols`
b. Na R#1:
   i. Over, že ti pribudol záznam o ceste k sieti susednej skupiny
c. Over, že susedná skupina tiež zrealizovala kroky 9a, 9b
d. Over konektivitu z PC1, PC2 k počítačom zo susednej topológie
e. Over konektivitu z PC1, a/alebo R1, do siete 10.200.0.0 (ktorákoľvek IP)
   i. Vyrieš tento problém redistribúciou priamo pripojenej siete na R1 v RIP doméne:
      - R2: `router rip, redistribute connected`
         - V IPv6 je to: `ipv6 router rip NAZOV_DOMENY, redistribute static`
            - Názov domény musia mať oba smerovače rovnaké
      - R1: over že vidíš sieť 10.200.0.0/16 v RT
   ii. Znova otestuj konektivitu, už by to malo byť bez problému

12. Autentifikácia v RIPv2 pre linky medzi smerovačmi

a. Pre sériovú linku použite plain text
b. Pre ethernetovú linku použite MD5
c. Skontroluj, či ste nestratili konektivitu k susedovi, ani medzi počítačmi
d. Pozrite zmienku o použitej autentifikácií v `sh ip protocols`

RIPng

Zopakuj celý proces pre RIPng pre IPv6, po každom kroku testuj čo treba (`sh ipv6 route, sh ipv6 protocols, debug ipv6 rip, ping, tracert`), stručne:

1. **Nakonfiguruj IPv6 adresy smerovačom aj počítačom**
   - Použi 2001:470:22B3:0#_ _::/64
     i. _ _ bude: 1A, AB za R1, 2A, 2B za R2, a 12, 21 medzi R1-R2
   - Otestuj konektivitu priamo pripojených *dvojíc*

2. **Zapni RIPng na rozhraniach**
   - Pozn.: IPv6 nemá žiadne triedy adries, takže RIPng nerieši automatickú sumarizáciu
   - Skontroluj obsah smerovacích tabuliek a `sh ipv6 protocols`

3. **Nakonfiguruj manuálnu sumarizáciu**
   - Robí sa na rozhraní: `ipv6 rip NAZOV_DOMENY summary-address ADRESA`
   - Skontroluj obsah smerovacích tabuliek a `sh ipv6 protocols`, odsleduj zmenu

4. **Na R1 nastav default route do internetu cez 2001:470:22B3:A::254 a redistribuuj v RIPng**
   - Pozn. 1: Redistribúcia v RIPng sa robí na rozhraní ! – tom ktoré má oznamovať susedom v RIPng doméne default route, ktorú on má v smerovacej tabuľke vytvorenú statickým záznamom
   - Pozn. 2: Daj pozor aby si default route redistribuoval iba jedným rozhraním (sériovým, alebo ethernetovým, nie obe)
   - Pozn. 3: Čo robí príkaz: `int s0/0, ipv6 rip NAZOV_DOMENY default-information originates`:
     i. *Originates the IPv6 default route (::/0) into the specified RIP routing process updates sent out of the specified interface.*
     ii. *Note: To avoid routing loops after the IPv6 default route (::/0) is originated out of any interface, the routing process ignores all default routes received on any interface.*
   - Zisti či danú IPv6 default route vidí aj R2
   - Otestuj dostupnosť do Internetu cez IPv6, napríklad 2001:4860:4860::8888 (google IPv6 DNS), z PC1 aj PC2

5. **Na R2 nastav IPv6 static route k vybranej inej skupine cez R2 v susednej skupine v sieti 2001:470:22B3:B::/64 a redistribuuj statickú cestu v RIPng. Redistribuuj na R2 aj priamo pripojené siete.**
   - `ipv6 router rip NAZOV_DOMENY, redistribute static, redistribute connected`
   - Skontroluj obsah smerovacích tabuliek a `sh ipv6 protocols`, odsleduj zmenu

6. **Autentifikáciu pre RIPng neriešime**

- *Since RIPng runs over IPv6, RIPng relies on the IP Authentication Header (see [11]) and the IP Encapsulating Security Payload (see [12]) to ensure integrity and authentication/confidentiality of routing exchanges. (RFC http://www.faqs.org/rfcs/rfc2080.html)*

7. Over konektivitu do vybranej susednej skupiny a do Internetu cez IPv6, napr. ping 2001:4860:4860::8888 (google IPv6 DNS).

- Over aj cez aké smerovače sa ide do daných cieľov cez tracert.

Záverečné upratovanie

1. Po skončení cvičenia nezabudnite po sebe upratať:
   a. `erase startup` (ak ste ukladali konfiguráciu do NVRAM)
   b. Odkáblujte si svoju časť topológie a vypnite smerovače aj počítače

Konfigurácia ISP smerovača (pre učiteľa, alebo šikovného študenta):

Ak neostala na smerovači pôvodná/základná konfigurácia (IPv6 tunel a pod.), treba ju nakopírovať z flash: config-2801.txt príkazom v privilegovanom móde (väčšinou ale je tam, takže netreba riešiť):

```
config replace flash:config-2801.txt
```

A k tejto základnej konfigurácii pridať toto (ctrl+c, ctrl+v v globálnom config móde na smerovači):

```
!
hostname ISP
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0/0
 no shut
 ip address 10.100.0.254 255.255.0.0
 ip nat inside
 no ipv6 address 2001:470:22B3::1/64
 ipv6 address 2001:470:22B3:A::254/64
!
interface GigabitEthernet0/0/1
 no shut
 ip nat outside
 ip add dhcp
!
ip nat inside source list 1 interface GigabitEthernet0/0/1 overload
!
access-list 1 permit 192.0.0.0 0.255.255.255
access-list 1 permit 10.100.0.0 0.0.255.255
access-list 1 permit 10.200.0.0 0.0.255.255
!
ip route 192.168.1.0 255.255.255.0 10.100.0.1
ip route 192.168.2.0 255.255.255.0 10.100.0.2
ip route 192.168.3.0 255.255.255.0 10.100.0.3
ip route 192.168.4.0 255.255.255.0 10.100.0.4
ip route 192.168.5.0 255.255.255.0 10.100.0.5
ip route 192.168.6.0 255.255.255.0 10.100.0.6
ip route 192.168.7.0 255.255.255.0 10.100.0.7
ip route 192.168.8.0 255.255.255.0 10.100.0.8
ip route 192.168.9.0 255.255.255.0 10.100.0.9
ip route 192.168.10.0 255.255.255.0 10.100.0.10
!
ipv6 route 2001:470:22B3:100::/56 2001:470:22B3:A::1
ipv6 route 2001:470:22B3:200::/56 2001:470:22B3:A::2
ipv6 route 2001:470:22B3:300::/56 2001:470:22B3:A::3
ipv6 route 2001:470:22B3:400::/56 2001:470:22B3:A::4
ipv6 route 2001:470:22B3:500::/56 2001:470:22B3:A::5
ipv6 route 2001:470:22B3:600::/56 2001:470:22B3:A::6
ipv6 route 2001:470:22B3:700::/56 2001:470:22B3:A::7
ipv6 route 2001:470:22B3:800::/56 2001:470:22B3:A::8
ipv6 route 2001:470:22B3:900::/56 2001:470:22B3:A::9
ipv6 route 2001:470:22B3:1000::/56 2001:470:22B3:A::10
```