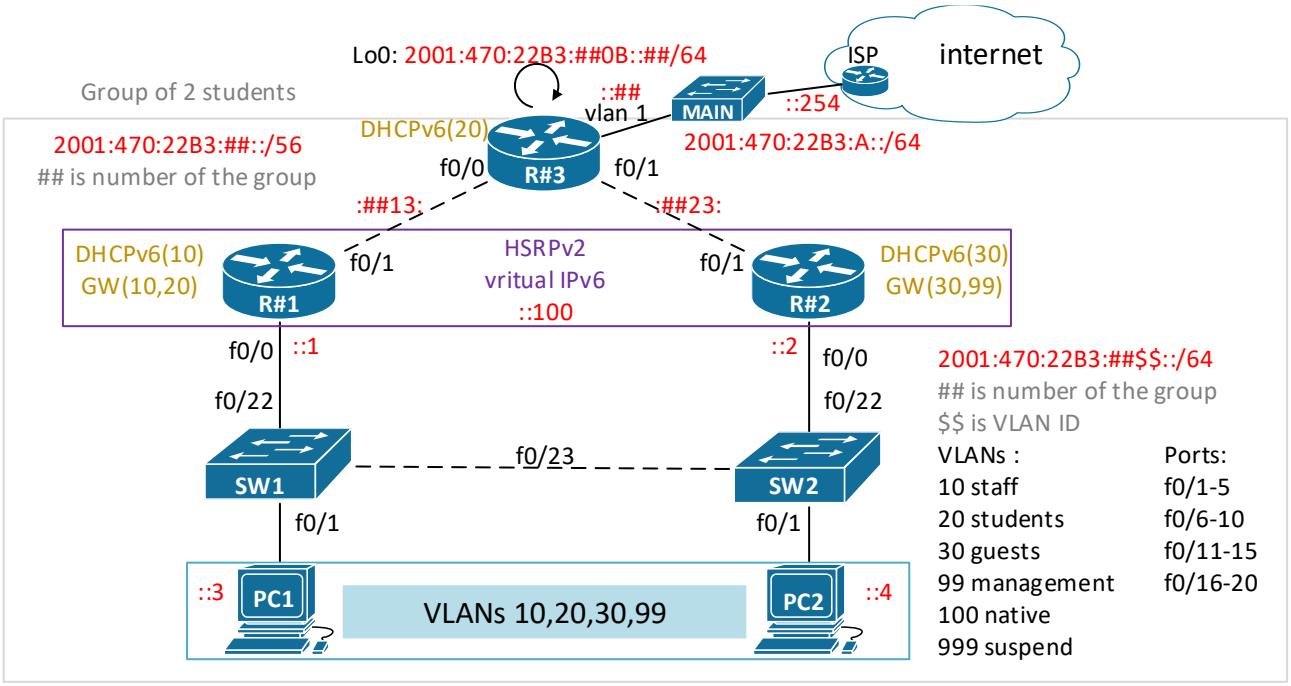
PS1 / Cvičenie 09 / **DHCPv6, HSRPv2, IPv6 ACLs, RIPng**

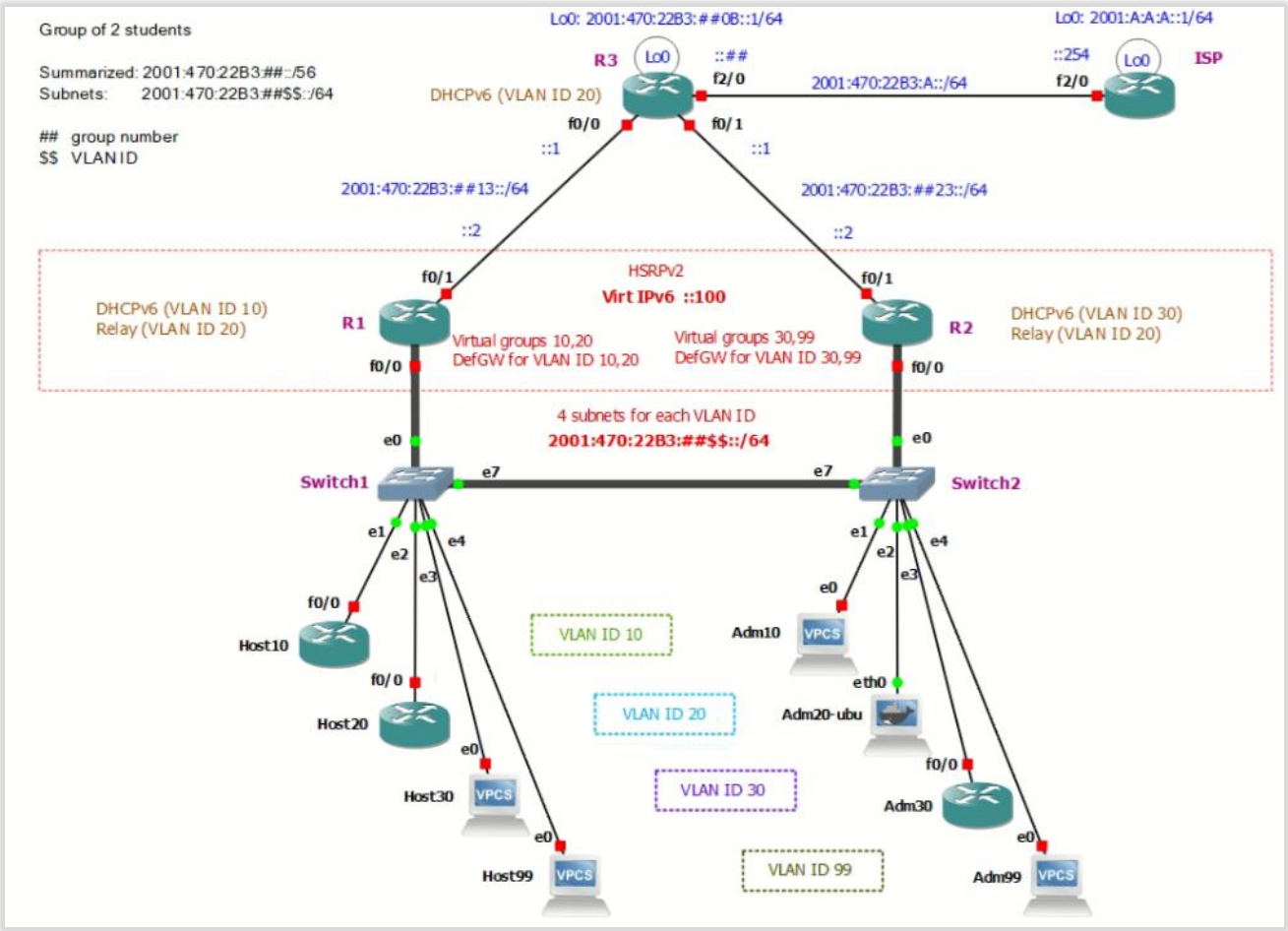
Topológia

Ver. A – pre prácu na reálnych zariadeniach v laboratóriu (Ver. B – pre prácu v GNS3 nájdete na 2. strane)
(nekáblujte skôr, ako spravíte kroky z: Inštrukcie a scenár)



Topológia

Ver. B – pre prácu na emulovaných zariadeniach vo virtuálnom prostredí GNS3
(topológia je pripravená pod názvom: **PS1-cv09-DHCPv6-HSRPv2--TEMPLATE**, ktorú vyučujúci nakopíruje pre všetky skupiny, pričom dohoda je dodržiavať názvoslovie: PS1-cv09-DHCPv6-HSRPv2-str15-JU-skupina01, kde str15 je deň a čas, a JU iniciály vášho cvičiaceho a 01 je číslo vašej skupiny):



Scenár a príprava:

Pracuje sa v dvojici, každá dvojica má dva smerovače R1,R2, dva prepínače, a smerovač R3, ktorý nakonfigurujú spoločne:

A. Voľba zariadení v reálnom labe:
   a. Smerovač **R3** zvoľte taký, ktorý má kartu **WIC-4ESW** (z nej sa pripojíte na MAIN prepínač cez int vlan 1), R1 a R2 môžu byť ľubovoľné.
   b. Prepínače **SW1** a **SW2** si vyberte **2960**, dôvod je nižšie ako Upozornenie A.

B. Pre prácu v **GNS3** (topológia je nižšie):
   a. potrebná je VPN, a prístup buď cez prehliadač: 158.193.152.63, alebo cez nainštalovaného GNS3 klienta ver. 2.2.25 (nie žiadna iná) – info máme v Moodle
   b. v zozname projektov hľadajte tento názov:
   PS1-cv09-DHCPv6-HSRPv2--TEMPLATE

i. Upozorňujeme, že nesmiete vstupovať a otvárať tento projekt, pretože po otvorení, nie je možné ho už duplikovať, musíte ho najprv zavrieť (ak máte projekt otvorená v niektorom okne v prehliadači, môže sa stať, že práve vy budete blokovať zatvorenie daného projektu)

ii. Podľa dohody študentské klony projektov budú mať názov: PS1-cv09-DHCPv6-HSRPv2-**str15-JU-skupina01**

- str15 –deň a čas vášho cvičenia, JU –iniciály vášho cvičiaceho, skupinaX – skupinu vám pridelí vyučujúci, pracuje sa v dvojiciach

c. Po otvorení Vášho projektu (s označením vašej skupiny), si naštartujete všetky zariadenia stlačením tlačidla Start/Play – hore v menu zelený trojuholník v obdĺžniku

d. Na CLI daných zariadení vojdete takto – pravým tlačidlom na zariadenie a:

i. V GNS3 klientovi: Console

ii. V prehliadači vo web GUI: Web console in new tab

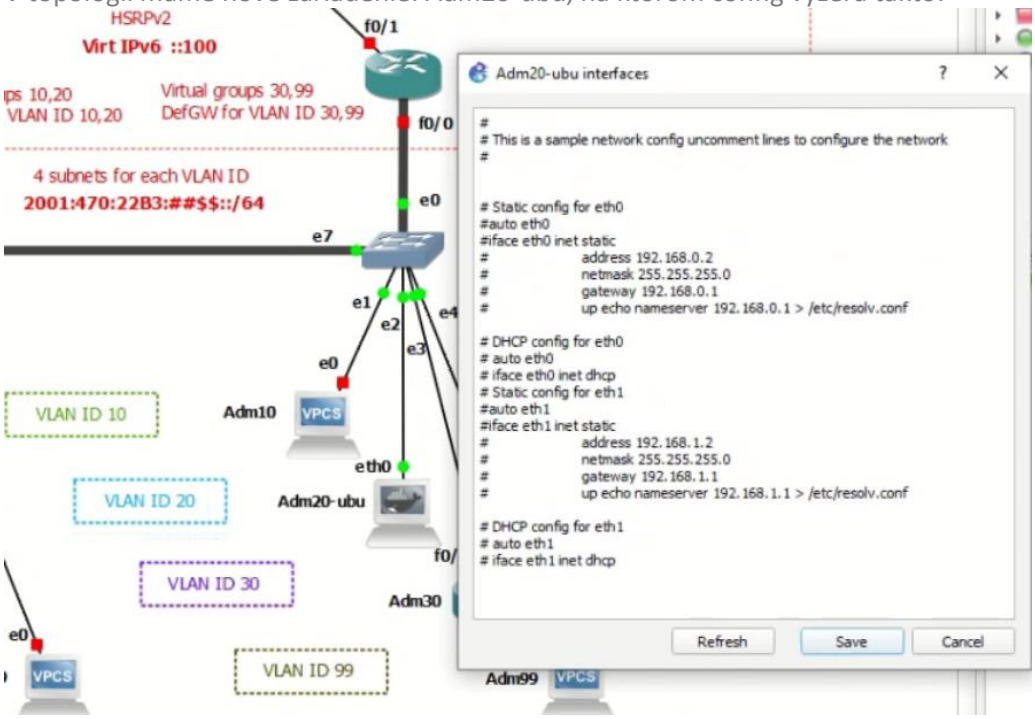
e. IP adresy na počítačoch nastavte takto:

i. Pravým tlačidlom na PC a Edit config a odkomentovať riadok:

- ip TUdajADRESU/TUdajMASKU TUdajIPdefaultGATEWAY, napr: `ip 192.1.10.3/24 192.1.10.1`, a pod to neskôr pripíšeš napr.: `ip 2001:470:22B3:10::3/64 auto` (auto - automaticky nastaví bránu, viď SLAAC proces, a vidieť ju budete vo výpise: show ipv6)
- Potvrdíte: Apply
- A ešte je potrebné config načítať/použiť: vojdite do CLI daného zariadenia (Console, alebo Web console in new tab) a zadajte príkaz: `load startup.vpc`

ii. Overenie nastavení zistíte príkazmi: `show ip, show ipv6` na VPCS klientoch a `ifconfig na` UbuntuDocker klientoch – napr. Adm20-ubu

iii. V topológii máme nové zariadenie: Adm20-ubu, na ktorom config vyzerá takto:



iv. Niektoré koncové stanice (klienti) máte v topológii ako VPCS, niektoré ako Ubuntu docker (ikona veľryby :-), a niektoré ako smerovače. Smerovače sme do topológie pridali preto, že VPSC koncoví klienti sú natoľko jednoduchí, že vedia IPv6 adresy dynamickým spôsobom získať iba cez SLAAC, ale nevedeli by sme

otetovať funkčnosť DHCPv6 statefull a stateless, preto sme ich nahradili na niektorých miestach smerovačmi
- Na smerovačoch IPv6 adresu staticky viete nastaviť, na porte ktorý vidíte v topológii.

f. keďže v GNS3 používame iný typ prepínača ako máme v reálnom laboratóriu, prosím berte do úvahy tieto zmeny, a podľa nich konfigurujte kroky v postupe – prepínač budeme konfigurovať cez Configure, zadaním parametrov do formuláru

g. **Ukladajte si priebežne konfiguráciu, lebo ak vy alebo váš kolega okno GNS3 klienta alebo okno prehliadača zavrie, tak prídete o všetko neuložené.**

h. Pokiaľ chcete po zavretí okna GNS3 aby vám ostal projekt bežať na pozadí, a neskôr sa k nemu vrátiť, tak v menu vyberte File – Edit Project (alebo cez web GUI: Projects settings – Edit project) – a tam zaškrtnite možnosť: Leave this project running in the background when closing GNS3.

i. Upozorňujeme, aby ste toto nerobili vždy a paušálne, ale len vtedy, keď naozaj chcete na tom robiť po krátkej prestávke, pretože zahlcujete zdroje servera, na ktorom pracujú mnohé iné skupiny študentov.

Dôležité upozornenia:

A. Prepínače voľte **2960**, podporujú IPv6 a budete si môcť spraviť aj vzdialené prihlasovanie cez telnet. Ak máte prepínač 2960 **a nebude mať podporu** pre **IPv6** (nepôjde príkaz `ipv6 add` na `int vlan 99`), doplniť to možno takto: `SW(config)#sdm prefer dual-ipv4-and-ipv6 default.` Na prepínačoch 2950 a 3550 so staršími IOSmi (12.x) sa podpora pre IPv6 nedá doplniť.

B. Vždy keď dávate PC do iného portu, pre príslušnosť do inej VLANy, **vypnite** a následne **zapnite** Cisco sieťovku, aby ste prinútili počítač zabudnúť tie IPv6 adresy, ktoré sa PC naučil zo správ Router Advertisement pre inú VLAN. Dodržte to počas riešenia všetkých úloh v tomto zadaní. Over si počet IPv6 adries na rozhraní: ipconfig /all

C. Pri všetkých IPv6 **ACLs** použite ako **názov** U a za ním číslo úlohy, ktorý dané ACL rieši – **U5, U6, ..** a použite na začiatku aspoň jednu poznámku/**remark**, ktorou stručne popíšete dané ACL, v jednej krátkej vete.

D. Vždy je dôležité rozhodnúť **kde** je najvhodnejšie daný ACL **aplikovať** !

E. **Pred** aplikovaním ACL je treba otestovať či máte požadovanú **konektivitu**! Pri testoch si budete meniť IP adresu na PC, podľa toho, akú prevádzku budete chcieť otestovať.

F. Všetky ACL bude vytvárať **každý** študent a aplikovať ich budú v dvojici vždy **po jednom**, vždy nový ACL nasadíte až potom, ako predošlý odstránite (nie z konfigurácie, len z daného rozhrania).

G. Tiež sa vždy **dohodnite s kolegom** vo dvojici (trojici), kto bude v ktorom čase testovať svoje ACLs, aby ste sa navzájom **nerušili**, nekazili si testy.

H. Využite možnosť logovania správ zachytených na danom ACL tak, aby sa vám zobrazovali na **console**. (pridaj „**log**“ na konci pravidla).

I. Na koniec ACL tam kde sa hodí (kde potrebujete zakázať všetku ostatnú prevádzku), vždy explicitne napíšte **`deny any`**, aby ste videli počet využití daného pravidla (matches v `show ip access`...)

J. Do svojho reportu z cvičenia si ukladajte:
- **runnin-config** - tú časť kde sa "hovorí o ACL" (stačí na záver cvičenia)
- výsledky **testovania** daného ACL (ping, ...), že zakázal/povolil čo mal
- na záver posledného ACL výpis: **show ip access list**

Adresovanie

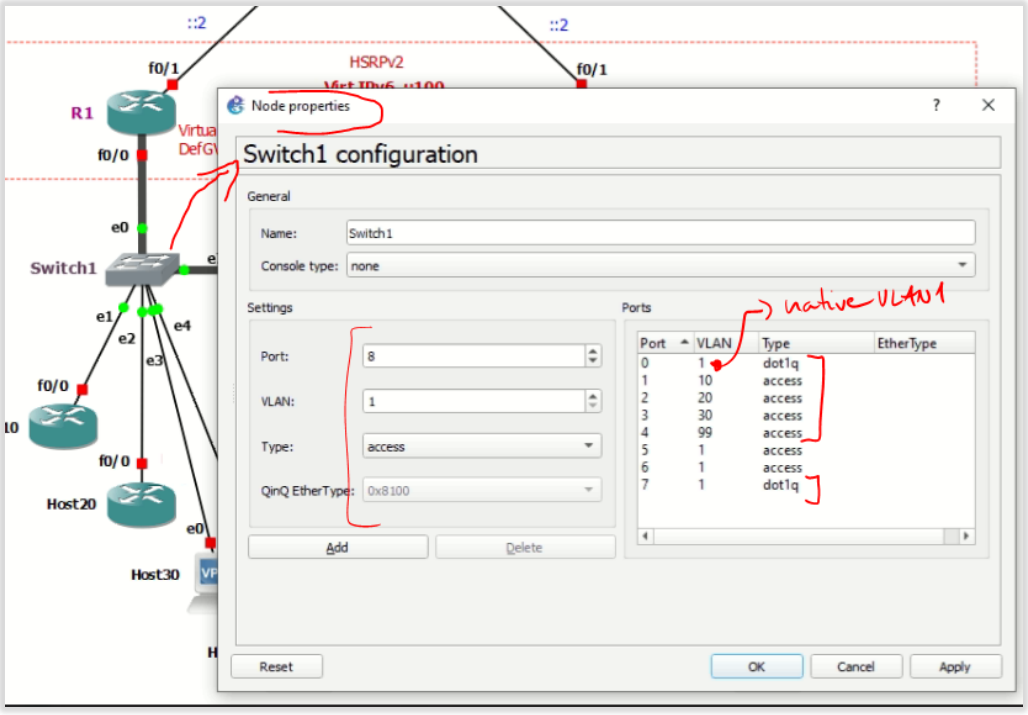
Pre pochopenie IPv6 adresovania (zatiaľ nič nekonfigurujete, konfigurovať budeme podľa postupu nižšie) - IPv6 rozsah 2001:470:22B3::/48 si rozdelíte pre VLANs a WANs nasledovne:

1. Použijete SubnetID (štvrtý hextet) tak, ako vidíte v obrázku s topológiou:
   a. 2001:470:22B3:##$$::/64
      i. kde ## je číslo vašej skupiny, t.j. 01, alebo 02, ... 10
      ii. a $$ je číslo VLANy, čiže 10, 20, 30, 99

   b. pre linky medzi smerovačmi R1-R3 a R2-R3 použijete siete ako vidíte v topológii:
      i. 2001:470:22B3:##13::/64
      ii. 2001:470:22B3:##23::/64
2. Smerovačom prideľujte IPv6 adresu od najnižšej
   a. Napr. pre skupinu 1, smerovač R1 pre subinterface f0/0.10 z VLAN 10: 2001:470:22B3:110::1/64, R2 bude mať 2001:470:22B3:110::2/64
3. Počítačom prideľujte IPv6 ľubovoľne
   a. napr. pre VLAN10 posledný hextet: 101, 102, pre VLAN20: 201,202, pre VLAN99: 991, 992
   b. alebo ako máte v topológii, ľavý počítač vždy ::3 a pravý ::4 v každej VLAN
   c. neskôr budú klienti získavať IPv6 adresné nastavenia cez DHCPv6, v bode 4 zadania, dovtedy budeme IPv6 adresy nastavovať manuálne

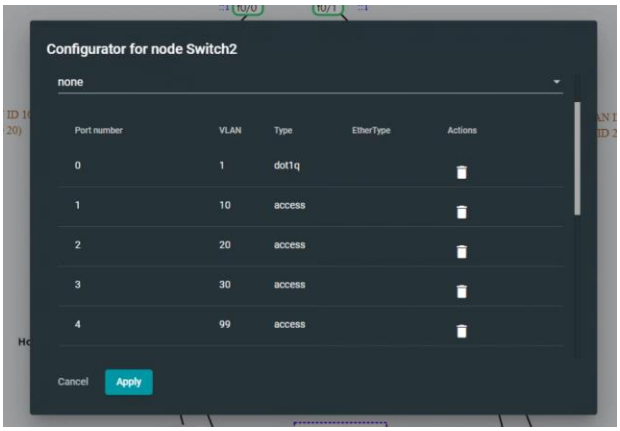
Postup

1. **Základná konfigurácia**
   a. Nastavte hostname R##1_Name, R##2_Name, R##3_Name (## je číslo vašej skupiny, Name je prvé meno študenta, ktorý bude zodpovedný za konfiguráciu daného zariadenia, nie priezvisko)
   b. Pre efektívnosť práce nastavte na smerovačoch:
      i. Zabráňte výpisu hlášok do písaného textu na konzole (zmiešavanie vstupu a výstupu CMD) `(line console 0, logging synchronous)`
      ii. Vypnite prekladanie doménových mien na IP adresy `(no ip domain-lookup)`
   c. Nastavte vhodne trunk porty a access porty na prepínači
      Pozn. pre GNS3 topológiu: Pre urýchlenie konfigurácie v GNS3, sme namiesto cisco switcha použili jednoduchý prepínač, ktorý sa konfiguruje cez *Configure* po kliknutí pravým tlačidlom myši na daný SW nasledovne (prosím berte do úvahy pri bodoch **i.** a **ii.** nižšie):



Pozn. pre GNS3 topológiu: ak pristupujete cez web GUI ku GNS3 serveru na KIS, tak toto

nastavenie budete mať vizuálne inak, ale obsah ten istý:



i. **Trunk** 2x
   - V reálnom labe: porty fa0/22, fa0/23, over: `sh int trunk`
   - V GNS3: porty e0 a e7, overenie v Configure /*Node properties*
ii. **Access** porty - do každej VLAN (10,20,30,99) priraď:
   - V reálnom labe: po 5 portov na každom prepínači, a over cez `sh vlan`
   - V GNS3: po jednom porte na každom prepínači, over v Configure /*Node properties*
iii. **Počítače** dajte do portov **v rovnakej VLAN** (v GNS3 už máte pripojené), IPv6 adresu z rovnakej VLAN (v GNS3 použite počítače na portoch v rovnakej VLAN) a **otestujte konektivitu** medzi nimi
   - Aplikujte upozornenie B!!
   - Nastavte počítačom aj IPv6 DNS server (v GNS3 nerobíme)
     - Napr. IPv6 google DNS: 2001:4860:4860::8888 (alebo 2001:4860:4860::8844)
     - Pozn. pre GNS3 topológiu: nenastavujte DNS server pre počítače, nebudeme využívať DNS, keďže nám v GNS3 topológii žiadny DNS server nebeží, ani nemáme z našej topológie pripojenie do internetu, len ho simulujeme Lo0 na ISP
iv. Zatiaľ si nerobte SSH na prepínač, budete tam cez konzolu, a neskôr si spravíte SSH prístup na smerovač (v jednom putty okne budete mať prepínač, v druhom smerovač). Ak ale silou mocou chcete teraz SSH prístup na prepínač, ok, ale ber do úvahy upozornenie A!
   - Pozn. pre GNS3 topológiu: v GNS3 nepotrebujete riešiť SSH, na každé zariadenie pristupujete cez telnet – emuluje pripojenie na konzolu zariadenia)

d. Vyriešte **interVLAN routing** na smerovačoch
   i. Každý smerovač bude mať **4 subrozhrania**
      - nezabudnite okrem IPv6 adresy nastaviť aj značkovanie dot1q a príslušnú VLAN !!!
      - zmeňte aj link-local adresu pre všetky 4 subrozhrania na: FE80::1 pre R1 a FE80::2 pre R2
      - nezabudnite povoliť IPv6 smerovanie (`ipv6 unicast-routing`)
   ii. **Počítačom** dajte **IPv6 adresy** z rôznych VLAN (v GNS3 si vyberte koncových klientov v rôznych VLAN) a otestujte konektivitu medzi nimi (pri práci v reálnom labe:

nezabudnite ich preradiť na iný port), ako bránu zatiaľ použite IPv6 adresy fyzických rozhraní, alebo ich link-local adresy

- Aplikujte upozornenie B!!
- Pozn. pre GNS3: počítače nepotrebujete nikam prepájať, vy už máte po 2 počítače v každej VLAN, takže len spravte test konektivity medzi PCs v rôznych VLAN.

e. Dokonfigurujte aj tretí smerovač **R3**, a rozhrania na R1 a R2 k nemu vedúce
   i. Nakonfigurujte aj rozhranie na R3 smerom k ISP (cez MAIN prepínač)
      - ISP IPv6 adresa: 2001:470:22B3:A::254
      - Vaša IPv6 adresa na R3: 2001:470:22B3:A::## (## je číslo vašej skupiny)
   ii. Zmeňte aj **link-local** adresy na rozhraní R1 smerom k R3 na FE80::1, podobne pre R2 na FE80::2 a pre R3 na všetkých rozhraniach na FE80::##03 (kde ## je číslo skupiny)
      - Pozn.: Ak by sa niekto chcel čudovať, prečo FE80::##03, tak si uvedomte, že na spoločnom segmente na MAIN prepínači tam bude veľa smerovačov R3 (a link-local adresa musí byť jedinečná/unique na danej linke/segmente)
      - Pozn. pre GNS3 topológiu: Pre vás predošlá poznámka nie je aktuálna, keďže každá dvojica pracuje vo svojej topológii, ktoré nie sú vzájomne prepojené. Čiže môžete mať link-local adresu aj FE80::3.
   iii. Overte konektivitu medzi každými dvomi priamymi susedmi R1<->R3, R3<->R2 a R3<->ISP

f. Nastavte **RIPng** na všetkých 3 smerovačoch, aby ste mali konektivitu v celej svojej topológii
   i. Uvedomte si, že smerovače R1, R2 používajú subrozhrania (kvôli tomu, že používame VLANy), preto nedávajte príkazy pre spustene RIPng na fyzické rozhranie, ale na subrozhranie!
   ii. Neaktivujte RIPng na R3 na rozhraní smerom k ISP !, tam budete neskôr riešiť statické smerovanie.

g. Na vrchnom smerovači R3 nastavte **statickú IPv6 default-route** k ISP, IPv6 adresu ISP smerovača máte uvedenú v obrázku, pričom:
   i. Nezabudnite ju na R3 aj oznamovať ostatným smerovačom
      - Najprv ju oznamujte na R3 na rozhraní vedúcom k R1, a overte v smerovacích tabuľkách R1 aj R2, či vidia default-route, a hlavne kto je tam uvedený ako next-hop!
      - Následne oznamujte default-route na R3 aj na rozhraní vedúcom k R2, a overte v smerovacích tabuľkách R1 aj R2, či vidia default-route, a hlavne kto je tam teraz uvedený ako next-hop! V tomto stave to nechajte.

h. **Overte IPv6 konektivitu** z R3 do Internetu (napr. IPv6 google DNS) a potom z počítačov do Internetu
   i. Napr. Google služby bežia aj nad IPv6
      - Pozn. pre GNS3: pre vás internet simulujeme Lo0 rozhraním na ISP, 2001:A:A:A::1/64. Nakonfigurujte si toto rozhranie, ak ešte nemáte. A aj ďalej v zadaní, ak sa píše o testoch smerom do internetu, pre vás to znamená test k IPv6 adrese Lo0 na ISP.
   ii. Na počítačoch si nastavte aj DNS server, ak ešte nemáte.
      - Pozn. pre GNS3: nie je potrebné.

i. Zvážte, ale zrejme by sa vám zišiel vzdialený prístup na R3, aby ste nemuseli chodiť prehadzovať konzolu. (v GNS3 nie je potrebné)

i. Ak máte prepínač 2960 a nebude mať podporu pre IPv6 (nepôjde príkaz `ipv6 add` na `int vlan 99`), doplniť to možno takto:
   - `SW(config)#sdm prefer dual-ipv4-and-ipv6 default`

ii. Na prepínačoch 2950 a 3550 so staršími IOSmi (12.x) sa podpora pre IPv6 nedá doplniť (my už také v labe RB303 nemáme).

2. HSRPv2 pre IPv6

a. Nastavte **R1** ako aktívnu bránu **pre VLAN 10, 20**, R2 bude záloha brány:

i. Ako číslo virtuálnej grupy použite číslo VLAN (aby to bolo prehľadnejšie)

ii.
```
interface f0/0.10
      ipv6 address 2001:470......../64
      standby version 2
      standby 10 ipv6 virtualnaIPv6adresa_zVLAN10
```
// pre VLAN99 použite: `standby 99 ipv6` **`autoconfig`** (počítače z VLAN99 by potom mali dostať od smerovača v správe Router Advertisements vrámci SLAAC virtuálnu IPv6 adresu brány - overte)

`standby 10 preempt` (staň sa aktívnym, ak ostatní majú menšiu prioritu)

`standby 10 priority XYZ` (zvýšiť na aktívnej bráne, default je 100)

("track" nie je potrebné zadávať)

b. HSRP skupina smerovačov R1 a R2 bude komunikovať cez multicast adresu **FF02::66**. Overte, že váš smerovač (aj R1, aj R2) bude spracovávať pakety určené na túto adresu:

i.
```
R1#sh ipv6 int f0/0.10
   Joined group address(es):
      FF02::1
      FF02::2
      FF02::66
      FF02::1:FF00:1
      FF02::1:FF11:1111
```

c. Nastav **R2** ako aktívnu bránu **pre VLAN 30, 99**, R1 bude záloha brány

i. Over konfiguráciu a aktuálny stav: `show standby`
   - Upozornenie: Ak oba smerovače (pre tú istú VLAN) sú active, to je signál, že to nefunguje dobre, zrejme sa „nevidia“, nemajú medzi sebou IPv6 konektivitu, alebo je HSRP nakonfigurované zle. Jeden musí byť active, druhý standby.

d. Zisti kadiaľ ide komunikácia medzi PCs (počítače musia mať nastavenú v konfigurácií svojej NIC **virtuálnu** IPv6 brány ! Nezabudni na upozornenie B):

i. PC1 (vo VLAN 10): cmd> tracert PC2

ii. PC2 (vo VLAN 30): cmd> tracert PC1

iii. PC1 (vo VLAN 99): nastav na tomto PC automaticky nastavenú IPv6 adresu, odsleduj akú dostal, a aký default gateway, ping a tracert na ISP, alebo k PC2

3. Kontrola vyučujúcim:

a. **Experiment 1**: shutdown rozhrania f0/0 na R1, odsleduj cez tracert kadiaľ ide prevádzka z PC1 do PC2 a opačne, daj si skontrolovať výsledok vyučujúcim. Následne daj rozhranie do pôvodného stavu.

b. **Experiment 2**: shutdown rozhrania f0/0 na R2, odsleduj cez tracert kadiaľ ide prevádzka z PC2 do PC1 a opačne, daj si skontrolovať výsledok vyučujúcim. Následne daj rozhranie do pôvodného stavu.

4. Nastavte DHCPv6 pre všetky počítače vo VLAN 10, 20 a 30

a. Pre VLAN 10 bude DHCPv6 server R1, rieš **statefull** DHCPv6

i. Na R1:
```
ipv6 dhcp pool STATEFULL_POOL_10
      address prefix [PREFIX_PRE_VLAN10::]/64 lifetime ? ?
```
(vhodne zvol časy, alebo zadaj infinite, pozri si **dodatok I.** na konci tohto zadania)

```
        dns-server 2001:4860:4860::8888 (IPv6 google DNS, alebo KIS IPv6 DNS: 2001:4118:300:120::2, alebo 2001:4118:300:120::4)
        domain-name DOMENA
int f0/0.10
        ipv6 dhcp server STATEFULL_POOL_10
        ipv6 nd managed-config-flag
sh ipv6 int
debug ipv6 dhcp detail
```

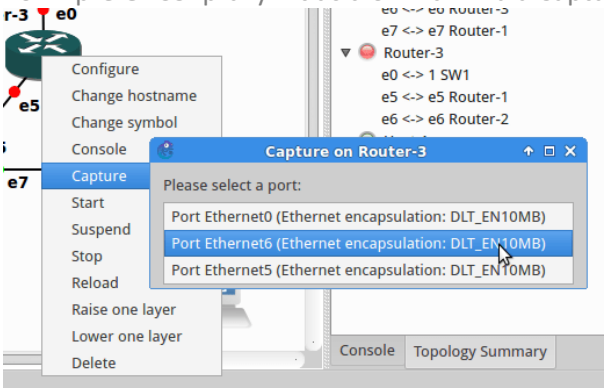
ii. Na klientoch/PCs vo VLAN10 nastav nech získajú IPv6 adresu dynamicky, ale pred tým si priprav odchytávanie komunikácie medzi klientom a serverom (bod iii.)

- **Pozn. pre GNS3**: Host10 (device: router) – pre ziskanie IPv6 adresy z DHCP:

```
interface FastEthernet0/0
ipv6 address dhcp rapid-commit (rapid-commit zabezpečí zrýchlenie procesu)
ipv6 enable
ipv6 nd ra suppress all (aby smerovač neposielal správy typu RA Router Advetisement, keďže z neho chceme mať len klienta)
```

iii. Odchyť si wiresharkom správu ICMPv6 a nájdi typ správy Router Advertisement a nájdi hodnoty flagov M a O (10)

- Pozn. pre GNS3: pravým tlačidlom na linku a Capture



b. Pre VLAN 30 bude DHCPv6 server R2, rieš **statefull** DHCPv6

c. Pre VLAN 20 bude DHCPv6 server R3, rieš **stateless** DHCPv6

i. Na R3:

```
ipv6 dhcp pool STATELESS_POOL_20
        dns-server 2001:4860:4860::8888 (IPv6 google DNS, alebo KIS IPv6 DNS: 2001:4118:300:120::2, alebo 2001:4118:300:120::4)
        domain-name [DOMENA]
int f0/0 (to isté aj na f0/1)
        ipv6 dhcp server STATELESS_POOL_20
sh ipv6 int
debug ipv6 dhcp detail
```

ii. Na R1 aj R2:

```
int f0/0.20
    ipv6 dhcp relay destination IPv6_ADRESA_R3
    ipv6 nd other-config-flag (tento príkaz musí byť tu, pretože prvý smerovač na ceste k DHCPv6 serveru oznamuje koncovému PC voľbu (SLAAC/ statefullDHCPv6/ statelessDHCPv6), a keby sme ho tam nezadali, smerovač sa rozhodne pre SLAAC)
```

iii. Odchyť si wiresharkom správu ICMPv6 a nájdi typ správy Router Advertisement a nájdi hodnoty flagov M a O (01)

- Pozn. pre GNS3: pravým tlačidlom na linku a Capture

d. Pre VLAN 99 nech sa IPv6 adresy prideľujú cez **SLAAC**

i. Na smerovači netreba dokonfigurovať nič – keď nemeníme hodnoty flagov M a O v ICMPv6 RA správe, tak sú defaultné 00, čo znamená použi SLAAC

ii. Na koncovom PC vo VLAN99 treba nastaviť, nech IPv6 adresu získa automaticky

iii. Odchyť si wiresharkom správu ICMPv6 a nájdi typ správy Router Advertisement a nájdi hodnoty flagov M a O (00)

e. Over pridelenie IPv6 adries, overte akú IPv6 dostali ako default GW (global unicast?/ link-local?/ adresu rozhrania, alebo vituálnu IPv6?) a overte konektivitu v rámci svojej topológie a k ISP z každej VLAN

i. Nezabudnite na upozornenie B!!

5. IPv6 ACL pre filtrovanie paketov v príkaze debug

a. Chcete si nechať zobrazovať správy o všetkých paketoch, ktoré si vymieňajú DHCP server s ľubovoľným klientom (hostom). Vytvorte preto ACL pre filtrovanie IPv6 paketov pre príkaz: **debug ipv6 packet <cislo_alebo_nazov_vaseho_ACL>**

Príkaz **debug ipv6 packet** vám zobrazí všetky pakety prichádzajúce alebo odchádzajúce z vašeho smerovača. Vašou úlohou je ale nechať si vypisovať informácie iba o IP paketoch, ktoré sa prenášajú medzi DHCPv6 serverom a ľubovoľným DHCPv6 klientom. Správy DHCP Discovery, Offer, Request, Acknowledgment sú platné pri DHCPv4 procese, pri DHCPv6 vieme o nadväznosti procesu ICMPv6 RA/RS, a následného DHCPv6 procesy pomocou správ SAIR - **S**OLICIT, **A**DVERTISE, **I**NFORMATION REQUEST/REQUEST, **R**EPLY. DHCPv6 komunikácia medzi serverom a klientom je nespojovo orientovaná, t.j. používa sa UDP ako transportný protokol, pričom pre posielanie dát od klienta na server sa používa **UDP port 546**, a pre posielanie dát zo servera ku klientovi sa používa **UDP port 547**.

i. Pozn.: DHCPv6 používa iné čísla portov ako DHCPv4, ktoré používa UDP porty 67 a 68.

b. Pozn.: Pri testovaní funkčnosti daného ACL v príkaze debug si dajte pozor, aby ste neboli na daný smerovač telnetnutý, pretože vtedy výsledky debug nevidieť, musíte tam byť cez konzolu, alebo po telnete na zariadenie použiť príkaz v privilegovanom móde: `terminal monitor`

6. IPv6 ACL – zákaz vstupu celej VLAN30, okrem admina, do VLAN10

a. Zakážte celej VLAN30 prístup do VLAN10, iba adminovi z VLAN30 prístup povoľ. Všetko ostatné nech je povolené.

b. Nasaďte a otestuj vytvorený ACL, že funguje:

i. Admin sa vie pingnúť do danej VLAN

ii. Host sa nevie pingnúť do danej VLAN (využi Wireshark a pozri sa čo príde ako odpoveď cez ICMP - hľadaj... Communication Administratively Filtered...) , ale ide mu konektivita do Internetu

c. Uprav daný ACL tak, aby povolenie platilo aj pre druhého admina (o 1 vyššia IP adresa). Nemaž celý ACL, iba doplň pravidlo na správne miesto do súčasného ACL.

d. Otestuj vytvorený ACL, že funguje

i. Obaja adminovia sa vedia pingnúť do vašej VLAN, aj do Inetu

ii. Host sa nevie pingnúť do vašej VLAN, ale ide mu konektivita do Inetu

7. Riešte nasledovný firewall pomocou IPv6 ACLs pre VLAN 20

Pozn. pre GNS3 topológiu: Admin20-ubu je Ubuntu host, v ktorom je možné cez curl robiť http requesty – na nejakú cieľovú IP (doménové mená v GNS3 nebudeme využívať), aby ste mohli robiť testy aj pre http služby. Keďže nám v GNS3 topológii nebežia žiadne reálne webové služby, využijeme to, že http služba beží na smerovači Host20 (okrem iného aj na Host10, aj Admin30). V realite by sme v prehliadači dali IPv6 adresu daného smerovača, a zobrazila by sa nám možnosť konfigurovať daný box cez web GUI. V GNS3 na Admin20-ubu využite daný príkaz curl (enterom si zistite možné prepínače).

a. Smer VON z VLAN20:

i. Povoľte iba http, HTTPS, DNS a DHCP a prístup na službu Remote Desktop Protocol (TCP/3389) v rámci celej topológie
ii. Povoľte odpovede na službu Remote Desktop Protocol odchádzajúce z VLAN siete
iii. Službu PING (ICMP echo) do celej topológie povoľte len jednej vybranej stanici
iv. Voľte politiku – čo nie je povolené, je zakázané

b. Smer DO VLAN30:
i. Povoľte vstup odpovedí na TCP spojenia vychádzajúce zvnútra LAN siete (nápoveda: ... established)
ii. Povoľte prístup na službu Remote Desktop Protocol na počítače vo VLAN30
iii. Povoľte zodpovedajúce prichádzajúce ICMP odpovede
iv. Povoľte DNS a DHCPv6 odpovede
v. Voľte politiku – čo nie je povolené, je zakázané

c. Keďže máte IPv6 konektivitu do Internetu, otestujte toto ACL na reálnej prevádzke smerom do a z Internetu.

8. **Kontrola vyučujúcim:**
a. Prezentuj funkčnosť predošlých 3 vytvorených IPv6 ACLs (že sa blokuje to čo má, a že je povolené to čo má byť povolené).

Ostatné ACL podľa času, ktorý vám ostane na cvičení:

9. **IPv6 ACL – zakáž telnet aj SSH na svoj smerovač pre všetky VLANy okrem VLAN99**
a. Vytvorte ACL, ktorý povolí iba staniciam vo VLAN 99 prístup na router, ktorý je ich bránou do internetu. Použite IPv6 ACL aplikovaný na rozhranie vty
b. Otestujte funkčnosť ACL
i. Žiadne PC z VLAN 10, 20 ani 30 sa nevie pripojiť na svoj smerovač cez telnet ani ssh.
ii. Ktorékoľvek PC z VLAN99 sa pripojí cez telnet aj ssh.

10. **IPv6 ACL – zakáž prístup na WWW a TFTP servery do VLAN30**
a. Zistili ste, že niektorí klienti vo VLAN30 si nainštalovali WWW a TFTP server. Z hľadiska bezpečnosti vašej siete je to neprípustné. Aby ste predišli riziku, zakážete prístup **zvonku** do VLAN30 na tieto služby.
b. Otestujte funkčnosť ACL:
i. ping z PC v inej VLAN na PC vo VLAN30 – prejde OK
ii. PC v inej VLAN sa nevie pripojiť na TFTP server na počítači vo vašej VLAN (použite TFTPd utilitu na ploche vášho PC, upravte adresár pre ukladanie súborov prenášaných cez TFTP na taký, do ktorého máte právo zápisu)
c. Uprav daný ACL tak, že prístup na WWW a TFTP bude povolený iba na jednu vyhradenú IPv6 adresu vo VLAN30. Následne otestuj funkčnosť.

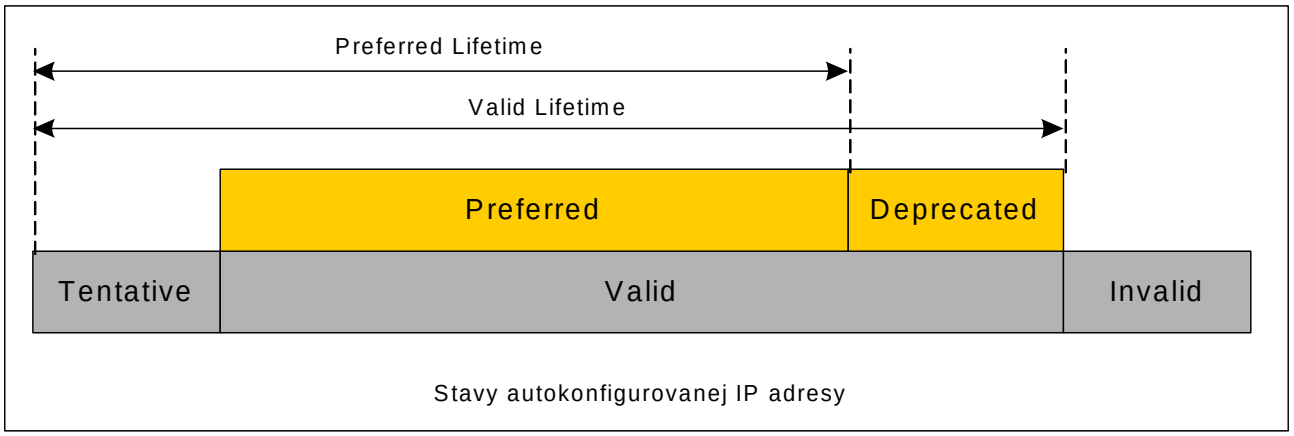
11. **IPv6 ACL – zakáž 1 hostovi z VLAN10 prístup kamkoľvek, povoľ mu len http**
a. Nové použitie jednej zo staníc (**Host**) vo vašej sieti, vás prinútilo nastaviť prísnejšie obmedzenia. Vytvorte také pravidlo, ktoré bude povoľovať danej stanici prístup na Internet (rozumej kdekoľvek vo vašej topológii) len cez HTTP a HTTPs a všetky ostatné porty zakáže.
b. Otestujte funkčnosť ACL:
i. Admin z VLAN10 vie preniesť súbor cez TFTP na PC do inej VLAN, host nie
ii. Host z VLAN10 vie pristúpiť na svoju bránu cez http – do prehliadača zadajte IPv6 adresu svojej brány (na smerovači treba ale povoliť prístup cez http: `ipv6 http server`)

Dodatok I.: Platnosť autokonfigurovanej adresy

- Stavy automaticky nastavenej adresy:
  - Tentative (neoverená, pokusná)
    - V procese preverovania unikátnosti (Duplicate Address Detection)
    - Unicast komunikácia je zakázaná
    - Multicast komunikácia – len správy Neighbor Advertisement
  - Valid (platná)
    - Unikátnosť adresy bola potrvrdená
    - Adresu je možné používať
    - Stav Valid obsahuje v sebe ďalšie 2 stavy: Preferred a Deprecated

      Preferred (normálny stav) – adresa je platná

      Deprecated (neschválená) – adresa je platná, ale je zbavená schopnosti nadväzovať nové spojenia, existujúca komunikácia môže prebiehať ďalej
  - Invalid (neplatná)
    - Do tohto stavu sa adresa dostane po uplynutí časovača Valid Lifetime
    - Adresa v tomto stave nie je použiteľná
- Autokonfigurovaná adresa prechádza týmito stavmi cyklicky, trvanie stavov získa zo správy **Router Advertisement**
- Autokonfigurované adresy obvykle patria na koncové stanice, smerovače ich spravidla nevyužívajú



Stavy autokonfigurovanej IP adresy

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 (v opačnom prípade tento krok preskočiť):

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

A k tejto základnej konfigurácii pridať toto (ctrl+c, ctrl+v najrpv do notepadu, aby sa vymazalo formátovanie a následne odtiaľ ctrl+c, ctrl+v v globálnom config móde na smerovači):

```
!
hostname ISP
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0/0
 no shut
 no ipv6 address 2001:470:22B3::1/64
 ipv6 address 2001:470:22B3:A::254/64
!
interface GigabitEthernet0/0/1
 no shut
!
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
```