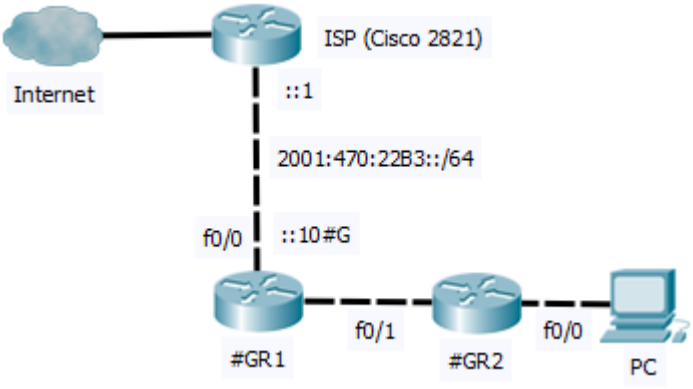
PS2 / Cvičenie 03 / **Opakovanie - DHCPv6, IPv6 ACLs, RIPng**

Fyzická topológia



Dôležité upozornenia:

A. 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.
B. Vždy je dôležité rozhodnúť **kde** je najvhodnejšie daný ACL **aplikovať** !
C. **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.
D. 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).
E. Využite možnosť logovania správ zachytených na danom ACL tak, aby sa vám zobrazovali na **console**. (pridaj „**log**“ na konci pravidla).
F. 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`...)
G. Pokiaľ tieto príklady robíte ako prípravu na skúšku, alebo máte už za sebou cvičenie o DHCP a NAT, zapojte si jeden zo smerovačov do internetu, s použitím NAT (prípadne aj DHCP) aby ste si mohli reálnejšie otestovať funkčnosť vytváraných ACLs. Na tomto cvičení to za vás spraví učiteľ (nakonfiguruje ISP).

Postup:

1. **Pridelený IPv6 rozsah 2001:470:22B3:#G00::/56 si rozdeľte pre VLANs a WANs:**
   a. Okrem fyzických prepojov vytvorte na smerovačoch aspoň 3 Loopback rozhrania.
   b. Pre SubnetID použite štvrtý hextet.
   c. Smerovačom prideľujte najnižšiu IPv6 adresu, počítačom ľubovoľne.
2. **Základná konfigurácia**
   a. Nastavte hostname #GR#R
   b. Nastavte korektne IPv6 adresy, zmeňte link-local adresy do prijateľnejšieho tvaru.
   c. Pre efektívnosť práce nastavte:
      i. Zabráňte na prepínačoch výpis 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)`
   d. Nastavte smerovačom telnet aj SSH prístup.
   e. Nastavte netradičný banner MOTD.
   f. Overte konektivitu.
3. **RIPng**

a. Nastavte RIPng na smerovačoch, aby ste mali konektivitu v celej svojej topológii.
b. Na vrchnom smerovači R1 nastavte statickú IPv6 default-route k ISP, pričom:
    i. Nezabudnite ju na R1 oznamovať smerovaču R2
        - Overte v smerovacích tabuľkách, či smerovače vidia default-route, a hlavne kto je tam uvedený ako next-hop.
c. Overte IPv6 konektivitu z R1 do Internetu (napr. IPv6 google DNS) a potom z počítačov do Internetu
    i. Napr. Google služby bežia aj nad IPv6
    ii. Na počítačoch si nastavte aj DNS server, ak ešte nemáte.
d. Sumarizujte prefixy.

4. Nastavte DHCPv6 pre počítač

a. DHCPv6 server R2, rieš statefull DHCPv6
    i.
```
ipv6 dhcp pool STATEFULL_POOL
      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::8.8.8.8
```
(IPv6 Google DNS, alebo KIS DNS: 2001:4118:300:120::2, alebo 2001:4118:300:120::4)
```
      domain-name DOMENA
int f0/0
      ipv6 dhcp server STATEFULL_POOL_10
      ipv6 nd managed-config-flag
sh ipv6 int
debug ipv6 dhcp detail
```
    ii. Odchyť si wiresharkom správu ICMPv6 a nájdi typ správy Router Advertisement a nájdi hodnoty flagov M a O (10)
b. DHCPv6 server R1, rieš stateless DHCPv6
    i. Na R1:
```
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 f0/1
      ipv6 dhcp server STATELESS_POOL
sh ipv6 int
debug ipv6 dhcp detail
```
    ii. NaR2:
```
int f0/0
    ipv6 dhcp relay destination IPv6_ADRESA_R1
    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)
c. 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

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). DHCP komunikácia medzi serverom a klientmi sú nespojovo orientované, t.j. používajú UDP ako transportný protokol, pričom pre posielanie dát od klienta na server sa používa **UDP port 67**, a pre posielanie dát zo servera ku klientovi sa používa **UDP port 68**. (pozn.: DHCP používa rovnaké dve čísla portov, ktoré sú pridelené organizáciou IANA pre protokol bootp)

6. **IPv6 ACL – zákaz vstupu do vašej siete z inej siete, okrem smerovača**
   a. **Vysvetlenie:** Zakážte vstup do vašej siete zo siete kolegu zo skupiny (#G+3 modulo počet skupín), okrem adresy jeho smerovača z danej siete. Všetko ostatné nech je povolené.
   b. Nasaďte a otestuj vytvorený ACL, že funguje:
      i. Smerovač sa vie pingnúť do vašej siete.
      ii. Host sa nevie pingnúť do vašej siete (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 inú IP smerovača (o 1 vyššia IP adresa). Nemaž celý ACL, iba doplň pravidlo na správne miesto do súčasného ACL.
   d. Otestuj vytvorený ACL, že funguje
      i. Smerovač sa vie pingnúť do vašej siete z obidvoch adries, aj do Inetu
      ii. Host sa nevie pingnúť do vašej VLAN, ale ide mu konektivita do Inetu
7. **Riešte nasledovný firewall pomocou IPv6 ACLs:**
   a. Smer VON zo siete:
      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 zo siete
      iii. Službu PING (ICMPv6 echo) do celej topológie povoľte len jednej vybranej stanici
      iv. Voľte politiku – čo nie je povolené, je zakázané
   b. Smer DO siete:
      i. Povoľte vstup odpovedí na TCP spojenia vychádzajúce zvnútra LAN siete (nápoveda: ... established)
      ii. Povoľte prístup na službu Remote Desktop Protocol na počítače v sieti
      iii. Povoľte zodpovedajúce prichádzajúce ICMPv6 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 siete, okrem vybraných**
   a. Vytvorte ACL, ktorý povolí iba staniciam zo sietí skupiny (#G+3 modulo počet skupín) prístup na váš router. Použite IPv6 ACL aplikovaný na rozhranie vty
   b. Otestujte funkčnosť ACL
10. **IPv6 ACL – zakáž prístup na WWW a TFTP**

a. Zistili ste, že niektorí klienti v sieti si nainštalovali WWW a TFTP server. Z hľadiska bezpečnosti vašej siete je to neprípustné. Aby ste predišli riziku, zakážete prístup **zvonku** do siete na tieto služby.
b. Otestujte funkčnosť ACL:
    i. ping z PC v inej sieti na PC – prejde OK
    ii. PC v inej sieti sa nevie pripojiť na TFTP server na počítači vo vašej sieti (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 v sieti skupiny (#G+3 modulo počet skupín). Následne otestuj funkčnosť.

11. IPv6 ACL – zakáž 1 hostovi zo siete prístup kamkoľvek, povoľ mu len http

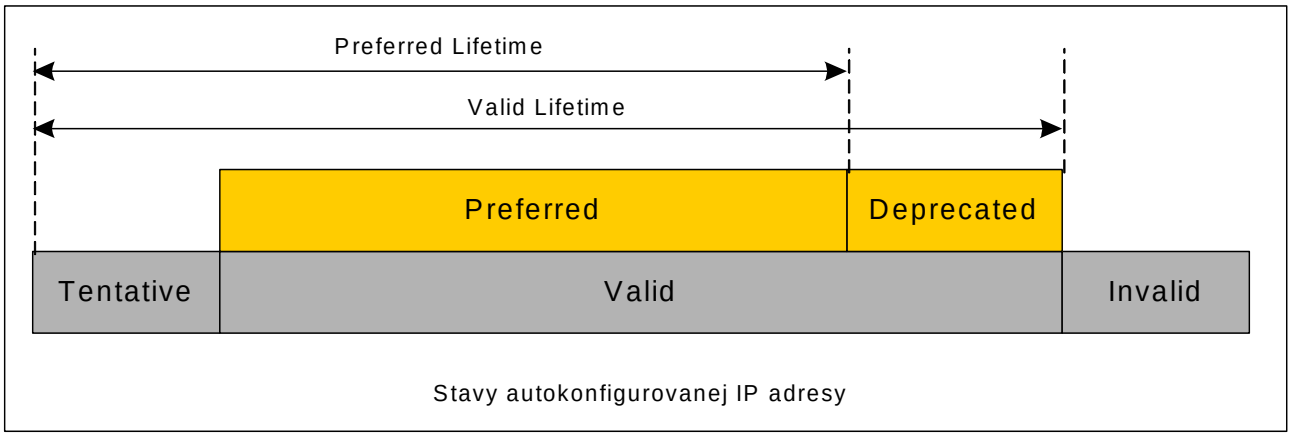
a. Nové použitie jednej zo staníc (**Host**) vo vašej sieti, vás prinútilo nastaviť prísnejšie obmedzenia. Vytvorte také pravidlo, ktoré bude povoľovať danej stanici prístup na Internet (rozumej kdekoľvek vo vašej topológii) len cez HTTP a HTTPs a všetky ostatné porty zakáže.
b. Otestujte funkčnosť ACL:
    i. PC vie pristúpiť na svoju bránu cez HTTP – do prehliadača zadajte IPv6 adresu svojej brány (na smerovači treba ale povoliť prístup cez http: `ip 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