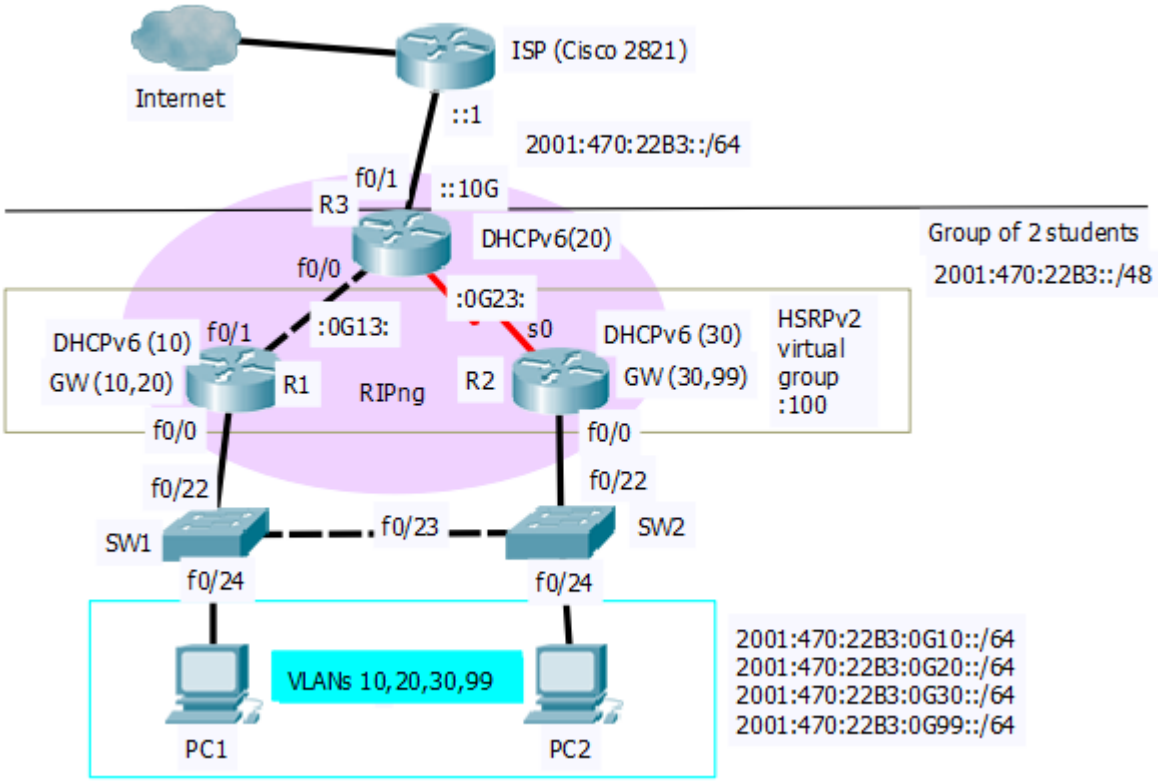
PS2 / Cvičenie 03 / **Opakovanie - DHCPv6, HSRPv2, IPv6 ACLs, RIPng**

Topológia



Dôležité upozornenia:

A. Prepínače voľte **2960**, podporujú IPv6 a budete si môcť spraviť aj vzdialené prihlasovanie cez telnet.
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**

K. 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::/48 si rozdeľte pre VLANs a WANs:**
   a. Použite SubnetID (štvrtý hextet), jeden možný návrh máte v obrázku s topológiou.
   b. Smerovačom prideľujte IPv6 adresu od najnižšej, počítačom ľubovoľne – napr. pre VLAN10 posledný hextet: 101, 102, pre VLAN20: 201,202, pre VLAN99: 991, 992.
2. **Základná konfigurácia**
   a. Nastavte hostname R#G1, R#G2, R#G3
   b. 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)`
   c. Nastavte vhodne trunk porty a access porty na prepínači
      i. Trunk 2x (fa0/22, fa0/23), over: sh int trunk
      ii. Access porty – po 5 portov do každej VLAN (10,20,30,99), over: sh vlan
      iii. Počítače dajte do portov v rovnakej VLAN, IPv6 adresu z rovnakej VLAN a otestujte konektivitu medzi nimi
         - Aplikuj upozornenie B!!
         - Nastavte počítačom aj IPv6 DNS server
            - Napr. IPv6 google DNS: 2001:4860:4860::8888 (alebo 2001:4860:4860::8844)
   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)
      ii. Počítačom dajte IPv6 adresy z rôznych VLAN a otestujte konektivitu medzi nimi (nezabudnite ich preradiť na iný port, ako bránu zatiaľ použite IPv6 adresy fyzických rozhraní, alebo ich link-local adresy)
         - Aplikujte upozornenie B!!
   e. Dokonfigurujte aj tretí smerovač, a rozhrania na R1 a R2 k nemu vedúce
      i. Nakonfigurujte aj rozhranie na R3 smerom k ISP
         - *Upozornenie 1*: k ISP idete priamym UTP káblom, pripájate sa na jeden zo 16 L2 ethernetových portov na smerovači, ktoré sú v jednej VLAN 1. ISP má svoju IPv6 adresu nakonfigurovanú práve pre toto int vlan1, smerom k vám.
         - *Upozornenie 2*: spravte test konektivity k ISP z R3. Pri fantómových problémoch skúste `shutdown` a `no shutdown` rozhrania vedúceho z R3 k ISP.
      ii. Zmeňte aj link-local adresy na všetkých rozhraniach R1 na FE80::1, podobne pre R2 na FE80::2 a pre R3 na FE80::G03 (kde G je číslo skupiny)
      iii. Overte konektivitu medzi každými dvomi priamymi susedmi R1<->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. Vhodné by ale bolo redistribuovať na R3 priamo pripojené siete (`redistribute connected`) v RIPng, čím zabezpečíte, aby sa R1 a R2 dozvedeli aj o sieti medzi R3 a ISP, inak by nebola pre nich dostupná (pre celkovú konektivitu to nie je potrebné, ale pre testy – keď chcete pingať ISP, alebo vonkajšiu IPv6 adresu R3, tak je to celkom vhodné)

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
ii. Na počítačoch si nastavte aj DNS server, ak ešte nemáte.

i. Zvážte, ale zrejme by sa vám zišiel vzdialený prístup na R3, aby ste nemuseli chodiť prehadzovať konzolu.
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

3. 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:DB8......../64
      standby 10 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
d. Zisti kadiaľ ide komunikácia medzi PCs (počítače musia mať nastavenú v konfigurácií svojej NIC **virtuálnu** IPv6 brány !):
   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 Lo0 na R3, alebo k PC2

4. 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.
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.

5. 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 ? ?
      dns-server 2001:4860:4860::8888
      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
```

   (vhodne zvol časy, alebo zadaj infinite, pozri si dodatok I. na konci tohto zadania)
   (IPv6 google DNS, alebo KIS IPv6 DNS: 2001:4118:300:120::2, alebo 2001:4118:300:120::4)

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

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
      domain-name DOMENA
int f0/0
      ipv6 dhcp server STATELESS_POOL_20
sh ipv6 int
debug ipv6 dhcp detail
```

   (to isté aj na f0/1)
   (IPv6 google DNS, alebo KIS IPv6 DNS: 2001:4118:300:120::2, alebo 2001:4118:300:120::4)

   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)

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

6. 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)

7. 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

8. Riešte nasledovný firewall pomocou IPv6 ACLs pre VLAN 20:

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 (ICMPv6 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 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.

9. **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:

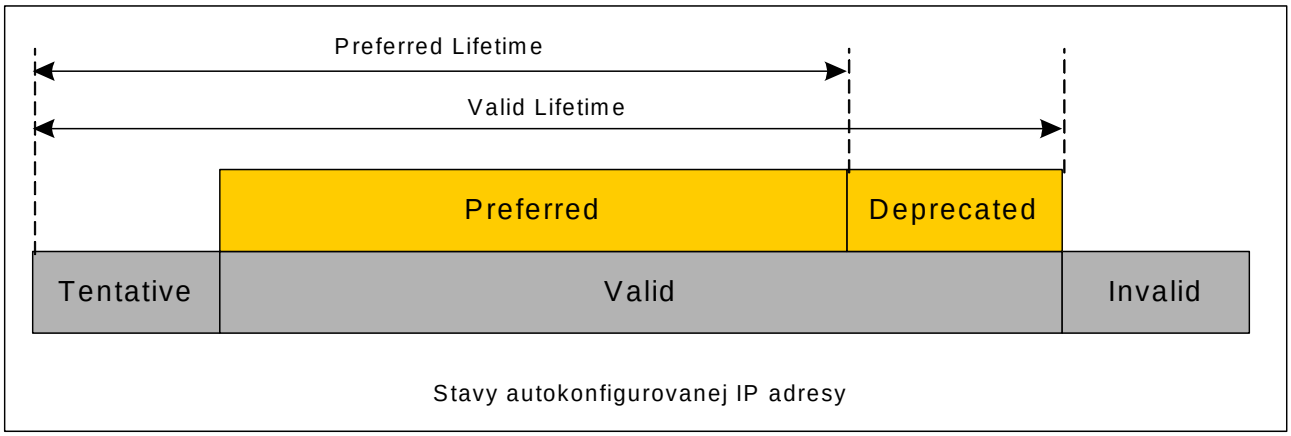
10. **IPv6 ACL – zakáž telnet aj SSH na svoj smerovač pre všetky VLANy okrem VLAN99**
    a. Vytvorte ACL, ktorý povolí iba staniciam vo VLAN 99 prístup na router, ktorý je ich bránou do internetu. Použite IPv6 ACL aplikovaný na rozhranie vty
    b. Otestujte funkčnosť ACL
        i. Žiadne PC z VLAN 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.
11. **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.
12. **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: `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