

IPV6 NDP, SPRÁVA ADRIES, DHCPV4 A BEZ/STAVOVÝ DHCPV6, IPV4/IPV6 STATICKÉ SMEROVANIE

Bc. Lukáš Urbančok



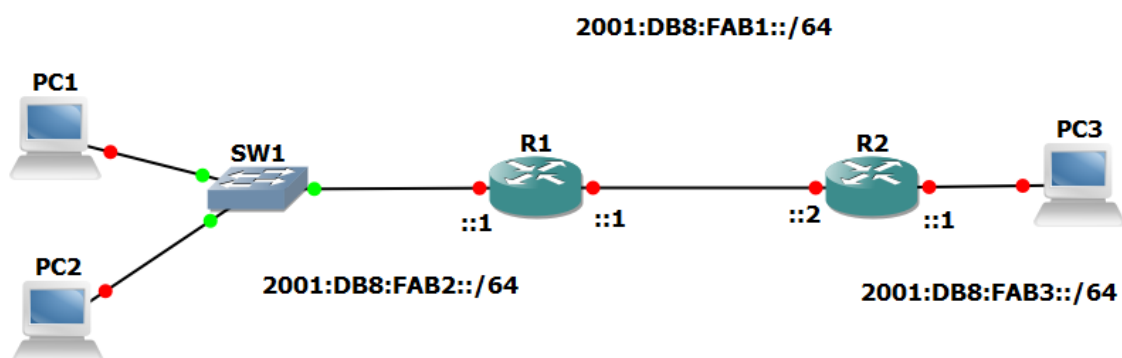
1 IPV6 NDP (NEIGHBOR DISCOVERY PROTOCOL)

V tejto úlohe sa preskúmajú základné typy IPv6 adresy vo **Wireshark**. Pridelovanie rôznych typov adresy **pre smerovače** a host'ov. Následne sa preskúma rozdiel adresy s IPv4 a *mapovanie L3 na L2* adresu pomocou **protokolu NDP**. Poslednou časťou NDP bude **odhaľovanie** smerovačov *RS* a *RA*. Používajú sa jednoduché **topológie** v *GNS3* z laboratórnej úlohy o vzdialenej správe IPv4 a IPv6 siete, ktoré sú upravené pre potreby danej úlohy. IPv6 používa úplne odlišný spôsob **získovania L2** adresy a cieľom tejto úlohy sa s ním zoznámiť. [1]

1.1 Zadanie:

Pomocou úlohy over funkčnosť IPv6 adresy a preskúmaj **komunikáciu** medzi uzlami IPv6.

1.2 Topológia:



Obr. 1: Ukážka jednoduchšej a zložitejšej topológie a príklad IPv6 adresácie [autor]

1.3 Teória:

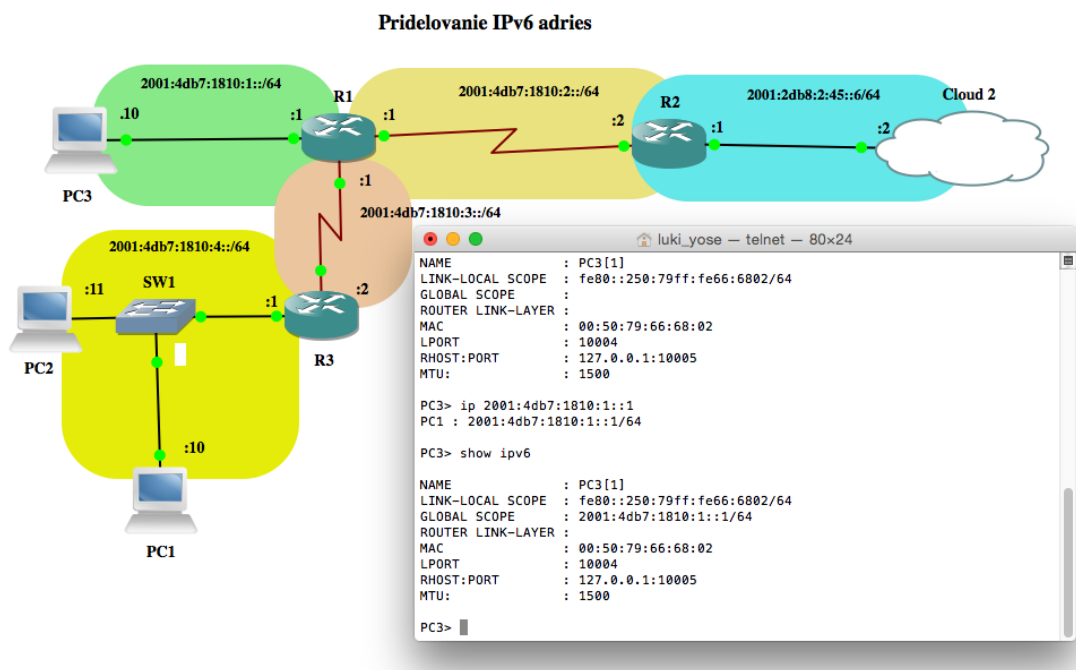
Rozlišujú sa 3 **typy prenosov** unicast, multicast a anycast. Na základe nich musí značka toku **reflektovať** všetky možnosti pri týchto prenosoch. Na rozdiel od klasickej **klasifikácie**, kde rozlišujeme zdroj, cieľ, port, transportný protokol, IPv6 stačí táto trojica.

- **Unicast** (individuálne) – dáta sú posielané host'ovi a rozlišujú jedného príjemcu/sieťové rozhranie;
- **Multicast** (skupinové) – identifikácia skupiny príjemcov, smerovače musia posielat' dáta pre všetky sieťové zariadenia, ktoré sú členmi danej skupiny FF::/8;
- **Anycast** (výberové) – nové v IPv6, rozlišuje sa skupina príjemcov, ale pakety doručené jednému (najbližšiemu). Týmto sa dosiahne rozkladanie záťaže (load

balancing) medzi viacerými uzlami v skupine a optimalizuje sieťovú prevádzku a v neposlednom rade sa šetrí šírka prenosového pásma chrbticovej siete;

- v IPv6 neexistuje **broadcast** adresy, nahradzuje sa pomocou adresy lokálnej linky. Správa a pridelovanie adres; [2][4]

Sieťový inžinier má tri možnosti nastavenie adres pomocou **statického pridelenia**, pomocou *DHCPv6* a *NDP* (objavovanie susedov) alebo bezstavovou autokonfiguráciou, ktorá využíva *EUI-64*. Nasledujúci *Obr. 2* sa venuje **pridelovaniu IPv6**:



Obr. 2: Príklad pridelovania IPv6 adres a ukážka statickej alokácie v software GNS3 [7]

Statické pridelenie IPv6 adres

Manuálne nastavenie celej *128 bitovej unicast* adresy – či už globálnej alebo lokálnej. Na *Obr. 2* sú **staticky nastavené** adresy pre lokálne rozhrania smerovačov a koncových uzlov. *PC3* má **automaticky** pridelenú linkovú-lokálnu adresu *FE00::250:79FF:FE66:6802* podľa svojej fyzickej *MAC* adresy a staticky nastavenú *IPv6* *2001:4db7:1810:1::1*. [5]

1.4 Požadované zdroje:

GNS3 a Wireshark



IOS smerovače – šablóna smerovača s **Ethernet** rozhraním [3]

1.5 Postup:

Topológia obsahuje 2 smerovače *c7200*, ktoré sú navzájom prepojené pomocou rozhrania *Ethernet 1/0* rozhrania. Je **implementované** IPv6 smerovanie k zabezpečeniu plnej dostupnosti z *PC1* do *PC2*. Následne by sa mali objaviť i **linkovo-lokálne adresy**, ktoré začínajú *FE80* a globálne adresy začínajúce 2 alebo 3 nasledované tromi ďalšími znakmi. *GNS3* má k dispozícii **Virtual PC simulátor**, voľne dostupný navrhnutý Paulom Mengom, ktorý je veľmi jednoduché pre ovládanie. Je niekoľko predvolených vyhradených adries pre nešpecifikovaný **::**, **spätnoväzbová slučka** (Loopback) *IPv6 ::1*, multicast *FFxx::* a mnohé ďalšie, čo bolo rozobraté v 1. Kapitole DP. V nasledujúcej úlohe **je použitá sieť** *2001:DB8:FABC:1111::/64*. Pred samotným **zapnutím** zariadení je spustené nahrávanie medzi *rozbočovačom a R1, R1 a R2* a spustenie host'ov. Pre skúmanie autokonfigurácie **povoľuje** zasielanie IPv6 prenos k ostatným zariadeniam z *CEF* na smerovači *ipv6 unicast-routing* a priradujú sa MAC adresy. Zámerne boli znova vybrané MAC adresy **príznačné** pre rozhranie smerovača v podsieti. [5]

Rozhranie má minimálne 2 IPv6 adresy a to globálnu a linkovo-lokálnu. Pri linkovej-lokálnej adrese môžu **Cisco smerovače** použiť *EUI-64* štandard a na základe MAC adresy vygenerovať ID host'a (druhú časť 64bitov IPv6 adresy). V našom prípade je na strane *R1* do **vnútornej siete** k rozbočovaču nastavená napevno *FE80::1* nasledujúca *link-local* . Následne sú priradené **podobné adresy** pre ostatné smerovače a sú aktivované porty. V neposlednom rade sa nastaví **predvolená cesta** pre smerovač *R1*, že IPv6 pakety, ktoré nebudú mať možnosť zistiť cieľ podľa smerovej tabuľky, budú posielané na adresu *R2 2001:DB8:FAB2::2*. Základný **syntax** statickej cesty je sieť kam sa chce dostať a nasledujúca IP adresa suseda/odchádzajúce rozhranie/prípadne linkovo-lokálna adresa. Podľa prvého príkladu sa nastaví **ostávajúce rozhrania**, v nižšie uvedenej tabuľke sú pripravené implementačné príkazy (cmd): [5]

Tab. 1: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

R1	R2
 R1 implementacia NDP .txt	 R2 implementacia NDP .txt

Po nastavení by mali byť schopné **otestovať** základnú komunikáciu pomocou *pingu* medzi smerovačmi. Prvá **strata paketu** je spôsobená v dôsledku *NDP protokolu* a výučby okolo

IPv6 operácií. PC sa **automaticky** naučia vlastnú IPv6 adresu po zadaní: *ip auto* sa vygeneruje 64 bitov host ID podľa MAC adresy. Po **overení** *ipconfig (show ip)* by si mali počítače navzájom dosiahnuť IPv6 adresu. [6]

Ďalej sú zobrazené **nastavenia** jednotlivých PC a rozhraní smerovačov s filtrom:

```
PC1> ip auto
GLOBAL SCOPE      : 2001:db8:fab2:0:2050:79ff:fe66:6800/64
ROUTER LINK-LAYER : 00:01:63:22:11:11
```

Obr. 3: Generovanie IPv6 adresy pre virtuálne PC1 [autor]

Dané virtuálne stanice môžu byť **nahradené smerovačmi**, ale otestujú GNS3 možnosti. Nasledujúce stanice *PC2 a PC3* sú **automaticky** nastavené ako *PC1*, takže sa použil príkaz *show ipv6* pre kompletné overenie IPv6 autokonfigurácie adres na *PC2 a PC3*:

<pre>PC2> show ipv6 NAME : PC2[1] LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6801/64 GLOBAL SCOPE : 2001:db8:fab2:0:2050:79ff:fe66:6801/64 ROUTER LINK-LAYER : 00:01:63:22:11:11 MAC : 00:50:79:66:68:01 LPORT : 10003 RHOST:PORT : 127.0.0.1:10002 MTU : 1500</pre>	<pre>PC3> show ipv6 NAME : PC3[1] LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6802/64 GLOBAL SCOPE : 2001:db8:fab3:0:2050:79ff:fe66:6802/64 ROUTER LINK-LAYER : 00:01:63:33:22:22 MAC : 00:50:79:66:68:02 LPORT : 10009 RHOST:PORT : 127.0.0.1:10008 MTU : 1500</pre>
---	---

Obr. 4: Zobrazenie IPv6 adresy pre virtuálne PC2 a PC3 (vpcs dynamips) [autor]

Použitím príkazu *show ipv6 interface brief* a filtrovaním *Ethernet rozhrania* sa overí **nastavenie a stav ipv6 unicast adres** a linkových lokálnych adres:

<pre>R1#show ipv6 inter brief section Ethernet1 Ethernet1/0 [up/up] FE80::1 2001:DB8:FAB2::1 Ethernet1/1 [up/up] FE80::201:63FF:FE11:1111 2001:DB8:FAB1::1 Ethernet1/2 [administratively down/down] unassigned Ethernet1/3 [administratively down/down] unassigned</pre>	<pre>R2(config)#do show ipv6 inter brief section Ethernet1 Ethernet1/0 [up/up] FE80::1 2001:DB8:FAB3::1 Ethernet1/1 [up/up] FE80::201:63FF:FE11:2222 2001:DB8:FAB1::2 Ethernet1/2 [administratively down/down] unassigned Ethernet1/3 [administratively down/down] unassigned</pre>
--	---

Obr. 5: Potvrdenie natvrdo priradenej IPv6 adresy pre rozhrania smerovačov R1a R2 [autor]

Testovanie pingom susednej IPv6 **natvrdo priradenej** pre smerovač *R2* a následne *PC*:

```
R1(config)#do ping 2001:DB8:FAB1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:FAB1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/32/84 ms
```

Obr. 6: Testovanie dostupnosti susedného rozhrania smerovača R2 [autor]

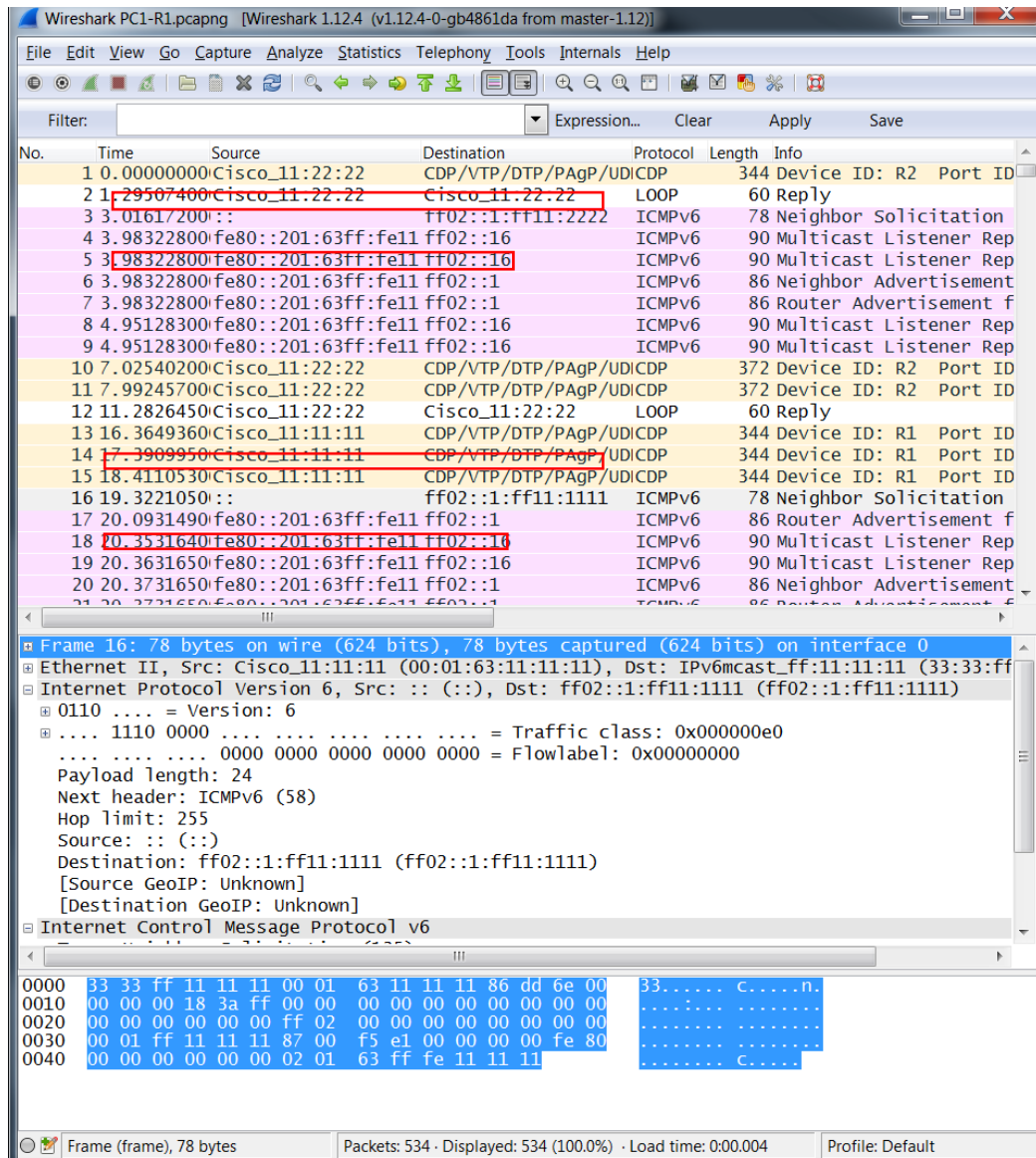
```
R1#ping 2001:db8:fab2:0:2050:79ff:fe66:6801
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:FAB2:0:2050:79FF:FE66:6801, timeout is 2 s
econds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/28/68 ms
```

Obr. 7: Testovanie dostupnosti virtuálnej stanice PC2 zo smerovača R1 [autor]

Po vykonaní týchto testov je možné **analyzovať** komunikáciu medzi *PC1* a *R1*, prípadne medzi smerovačmi *R1* a *R2* vo Wiresharku. Napríklad paket číslo 16 medzi *smerovačom* a *PC1* má za účel **detekcie duplicity** adries (*DAD - Duplicate Address Detection*). Keď si **rozrolujú** hlavičku tretej vrstvy, vidia nešpecifikovanú zdrojovú adresu ::. To preto, že *R1* pred začatím **vyšielania** používa *linkovo-lokálnu adresu FE80::/1*. Pokiaľ sa chce overiť, či už niekto používa danú *IPv6 adresu*, vždy **zdrojová adresa** je nešpecifická a cieľová adresa bude začínať s *FF*, čo je multicast adresa spojená s linkovo-lokálnou *FE80::/1*. Detailný rozbor o technológií nie je **cieľom** tejto laboratórnej úlohy. **Zat'aženie** (payload) je v tomto prípade *ICMPv6*, ktorý sa používa pri viacerých funkciách *NDP*, čo zahrnuje i odhalenie *L2 adresy suseda*. [5]

Nevýhodou *SLAAC* konfigurácie je, že nezaist'uje **nastavenie DNS** servera, doménových názvov či *SIP* servery a nezaist'uje žiadnu správu adries vo fonde.

U *IPv4* sa používal **známy ARP**, ktorý zahrňoval *L3 na L2 mapovania*, avšak v *IPv6* neexistuje *broadcast*. Pokiaľ sa pozrie na nasledujúci **paket 18**, zdrojová adresa je *FE80::/1a*, cieľová *L3 adresa* je multicast. Po vykonaní **pingu** príkazu sa nám narolujú pakety 380-394, ktoré zahrňujú celý proces echo žiadosti a odpovede. Táto **komunikácia** naučí rozpoznávať linkovo-lokálnu, globálnu adresu, tok multicasu a nešpecifické adresy. Ideálny prípad je **porovnať** teoretické znalosti so správami *RS/RA* a *NS/NA*. [5]

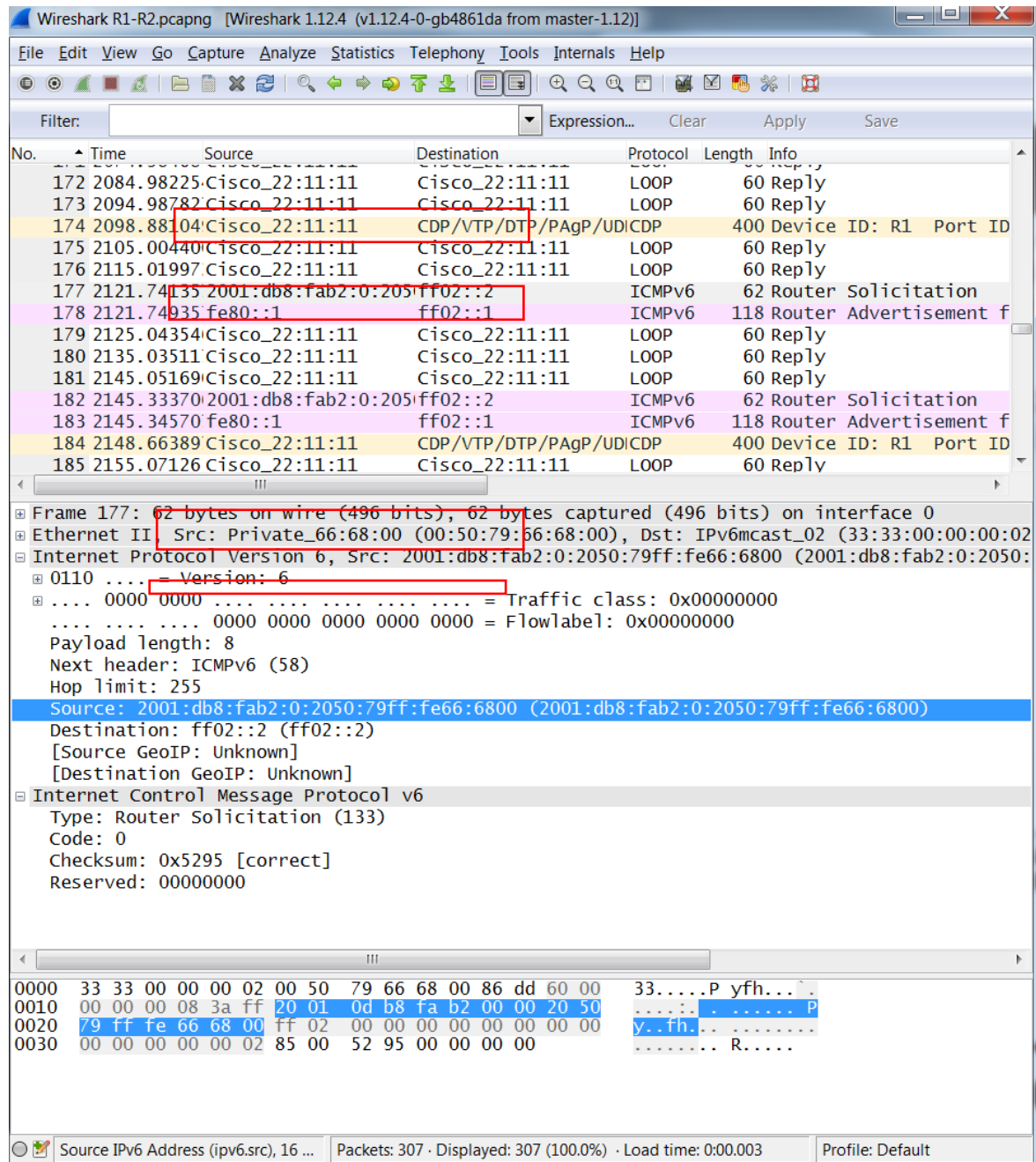


Obr. 8: Ukážka NDP protokolu z odchytných paketov medzi PC1 a R1 [autor]

Pri detailnom skúmaní paketov sa zistí, že pomocou NS je možné si mapovať L2 adresu, ktorá je uložená v Ethernet II, na základe ktorej sa preloží adresa na multicast skupiny, na ktorej bude načúvať dané zariadenie. Pozorné oko si všimne rozdiel i v type: IPv6 (0x86dd) a IPv4 (0x800). Pri odpovedi PC v NA je vidieť ICMP zaťaženie, L2 MAC adresu, ktorú posielala ako odpoveď v jednej multicast skupine. Pre zjednodušenie adresácie je možné použiť i EUI-64 pre generovanie IPv6 do prefixu podľa L2 adresy. [6]

Pri skúmaní premávky medzi smerovačmi paket číslo 11 v ICMPv6 je vidieť zdrojovú L2 adresu. L3 adresy IPv6 sú použité FE80::/1 ako zdrojová a známa multicast adresa uzlov FE02::1 a indikácia ďalšej hlavičky je nastavená na ICMPv6. Ďalším príkladným paketom je 177 RS, ktorý slúži pri hľadaní smerovačov. Paket je generovaný R1. Pri skúmaní IPv6

je zdrojová adresa `2001:db8:fab2:0:2050:79ff:fe66:6800`, z *PCI* cieľová adresa je multicast skupina pre smerovače. *L2* vrstva MAC adresy **známej** multicast adresy skupiny. [5]



Obr. 9: Ukážka paketu RS a RA pri hľadani smerovača z *PCI* [autor]






Známa **multicast** adresa skupiny je `33:33:00:00:00:01`. V detaile *ICMPv6* RA odpovede zo smerovača je **zaujímavo** uložená odpoveď z *L2* adresy smerovača `0000.63222.1111` pre prefix `2001:db8:fab2` vo forme RA. Pri rozrolovaní sa zistí, že smerovač posielal host'ovi *PCI* detailné informácie o smerovači a lokalizácii. RS **posiela** host'a na nájdenie smerovača. [6]

- ▣ Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x8103 [correct]
 - Cur hop limit: 64
 - ▣ Flags: 0x00
 - Router lifetime (s): 1800
 - Reachable time (ms): 0
 - Retrans timer (ms): 0
 - ▣ ICMPv6 Option (Source link-layer address : 00:01:63:22:11:11)
 - ▣ ICMPv6 Option (MTU : 1500)
 - ▣ ICMPv6 Option (Prefix information : 2001:db8:fab2::/64)
 - Type: Prefix information (3)
 - Length: 4 (32 bytes)
 - Prefix Length: 64
 - ▣ Flag: 0xc0
 - Valid Lifetime: 2592000
 - Preferred Lifetime: 604800
 - Reserved
 - Prefix: 2001:db8:fab2:: (2001:db8:fab2::)

Obr. 10: ICMPv6 informácie v správe RA od smerovača R1 [autor]

Výsledné nastavenie smerovačov pre overenie funkčnosti *IPv4* a *IPv6 adresácie* a zisťovanie *MAC adries* pomocou *NDP* protokolu. [5]

Tab. 2: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

R1	R2	vPCs1-3	Wireshark PC1-R1	Wireshark R1-R2
 R1.txt	 R2.txt	 vPC .txt	 Wireshark PC1-R1.pcapng	 Wireshark R1-R2.pcapng

1.6 Otázky na zamyslenie o IPv4 a IPv6 adresácii a protokolu NDP:

1. Aké typy IPv4 a IPv6 adresies poznáte ? Popíšte: [1]

SPOLOČNÉ

Unicast (individuálne)

- dáta sú posielané host'ovi a rozlišujeme jedného príjemcu/ sieťové rozhranie;

Multicast (skupinové)

- identifikácia skupiny príjemcov, smerovače musia posielat' dáta pre všetky sieťové zariadenia, ktoré sú členmi danej skupiny FF::/8;

ROZDIELY:

Anycast (všesmerové) IPv4

- dáta sú posielané všetkým uzlom v danej podsieti môžu byť adresované naraz; čo je bezpečnostná hrozba a na hraniciach siete je väčšinou táto možnosť zakázaná;

Anycast (výberové) IPv6

- nové v IPv6, sa rozlišuje skupina príjemcov, ale pakety doručené jednému (najbližšiemu). Týmto sa dosiahne rozkladanie zát'aže (load balancing) medzi viacerými uzlami v skupine a optimalizuje sieťovú prevádzku a v neposlednej rade sa šetrí šírka prenosového pásma chrbticovej siete; u IPv6 neexistuje broadcast adresy, nahradzuje sa pomocou adresy lokálnej linky;

2. Aké tri možnosti pridelovania IPv6 adresies môžu správcovia použiť ? [5]

Statického pridelenie (manuálne), pomocou DHCPv6 a NDP (objavovanie susedov) alebo bezstavovou autokonfiguráciou SLAAC, ktorá využíva EUI-64.

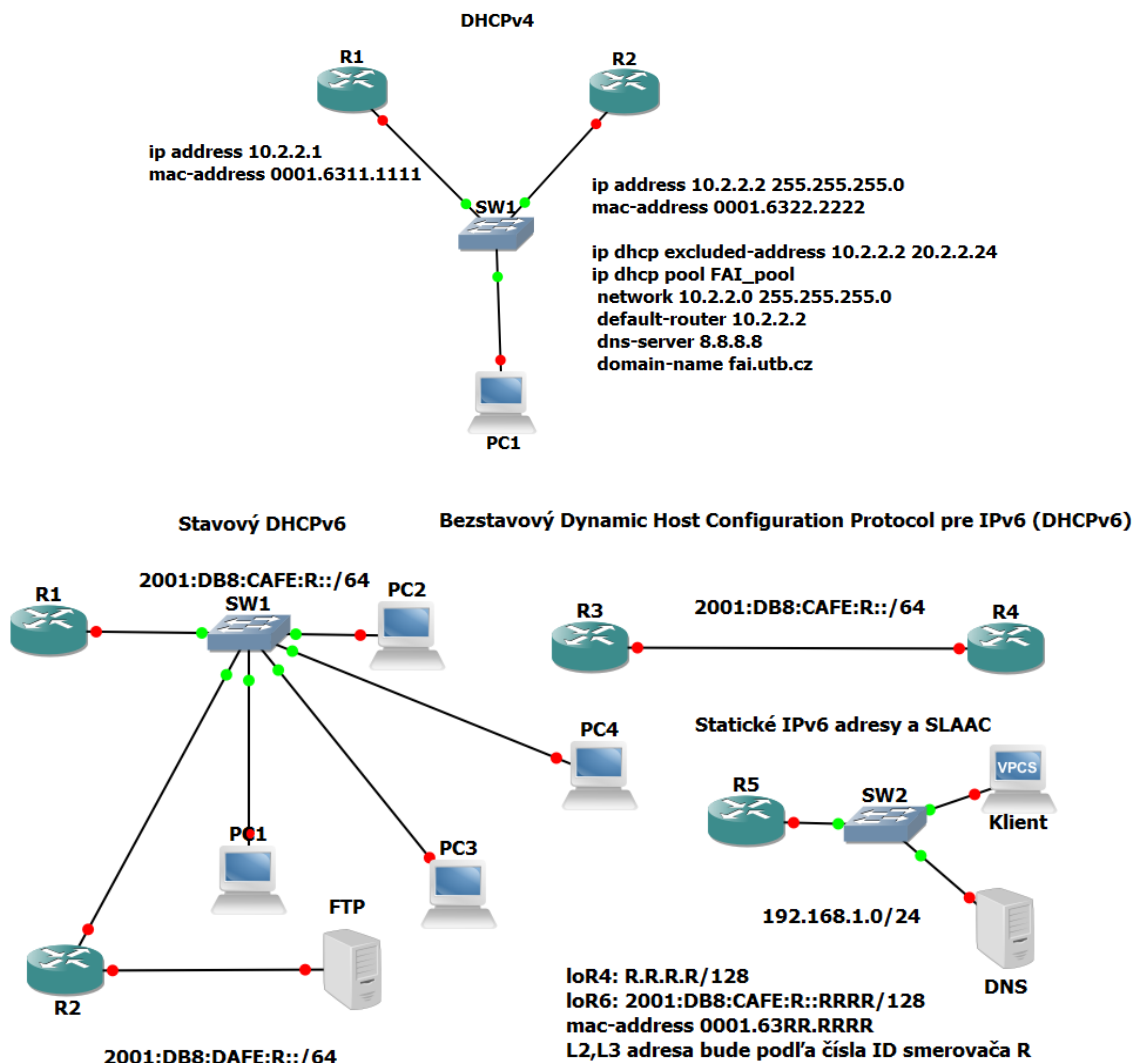
2 SPRÁVA IPV4 A IPV6 ADRES – DHCPV4 A DHCPV6

V tejto laboratórnej úlohe sa **preskúma** správa *IPv4* a *IPv6* adres sietí. Pomocou Wiresharku sú procesy pri **pridelovaní** statických a dynamických adres pomocou *DHCP*. Používa sa topológia v **GNS3**, kde sú zohľadnené tri možnosti pridelovania *IPv6* adres.

2.1 Zadanie:

V nasledujúcej laboratórnej úlohe sa **konfigurujú** *IPv6* adresy (staticky, SLAAC a *DHCPv6*) a analyzujú sa spôsoby overenia pridelených adres s využitím všetkých možností. [5]

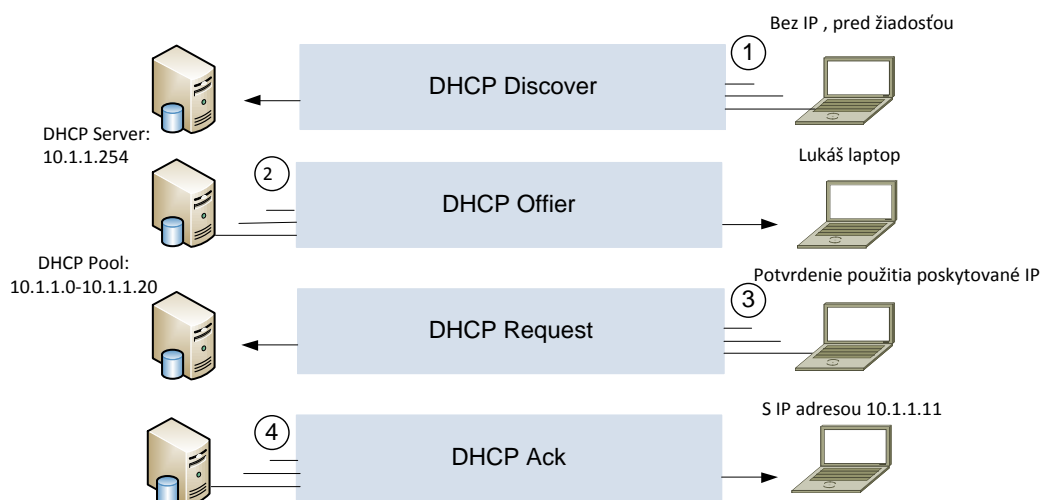
2.2 Topológia:



Obr. 11: Topológia pre test DHCPv4, IPv6 stavový a bezstavový DHCPv6 [autor]

2.3 Teória:

Predpokladá sa, že je známe, čo je **IP adresa** a ako vypadá, či už v *DEC* alebo *BIN* podobe. **Rozdelenie** adries do *tried A, B, C*, výpočet sieťovej alebo broadcastovej adresy nie je náplňou tejto úlohy. V prípade potreby zopakovať si **IP protokol**, verí sa, že odkazy na literatúru v diplomovej práci budú dostatočným zdrojom. Adresy môžu byť **pridelované** staticky alebo dynamicky. **DHCP** (Dynamic Host Configuration Protocol) je dynamické pridelovanie bloku adries servera pre sieťové zariadenia. Ako je na nasledujúcom *Obr. 12* PC pri štarte žiada o IP adresu od DHCP servera pomocou **DISCOVER** broadcastu (v danej VLAN), aby mohol pracovať v sieti. Tento **paket** je poslaný každému v danej podsieti, prípadne ak je smerovač nastavený ako *relay agent* (definuje spôsob ako sa dostať k DHCP serveru – odkaz pomocou *ip helper address*). V prípade lokálneho **DHCP servera**, nasleduje proces *OFFER*, čím sa ponúkne IP adresa pre host'a, jej platnosť a prípadne ďalšie detaily. Na prenos týchto vyjednávacích paketov sa používa 4. vrstva **UDP protokolu 67** pre *DHCP* server a 68 pre DHCP klienta. Následne sa **klient** pomocou žiadosti *REQUEST* dotazuje na konkrétnu adresu a server prideluje host'ovi danú *IP masku, DNS server* a predvolenú bránu. DHCP pre *IPv4* a celý proces je preskúmaný pomocou **Wiresharku**. Kde pri detailnom rozbere sa zistí, že 2-4 správa môže byť broadcast prípadne unicast, čo záleží na flagu, aký nesie paket. [2]

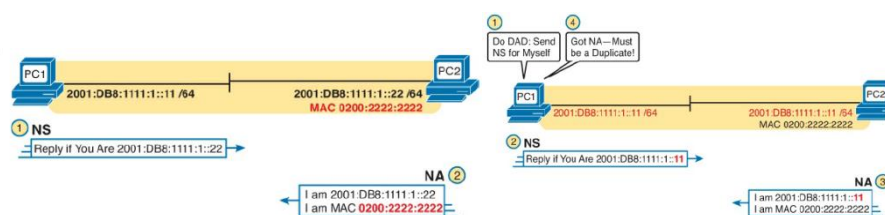


Obr. 12: Proces pridelovania IP adries pomocou DHCP serveru [5][6]

Hlavným rozdielom pri **dynamickom pridelovaní IPv4 a IPv6** je *mapovanie L3 na L2* adresy. IPv4 k tomu používa **ARP protokol**, naopak IPv6 k tomu používa **NDP** (čo je detailnejšie popísané v samotnej diplomovej práci), takže sa bude odkazovať na ňu. Spomenú sa len **funkcie**, ktoré zabezpečuje: [1]

- Objavovanie smerovačov
- Objavovanie MAC adries
- Detekcia duplicity adries
- Bezstavová autokonfigurácia SLAAC

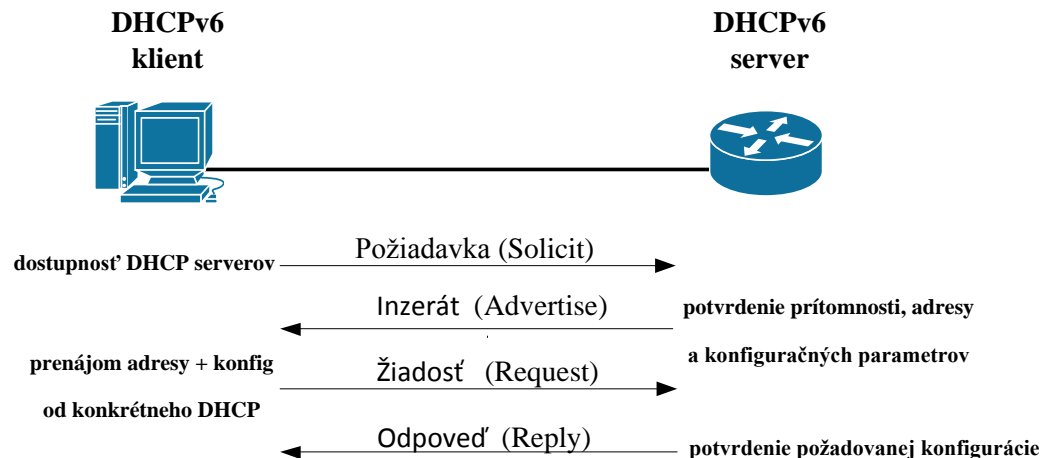
Bezstavová autokonfigurácia je akýsi mini *DHCP* server, ktorý beží na stanicach často bez ich vedomia. Používajú sa **linkové adresy**, jedinou vec, čo sa používa z centrálného servera je prefix, ktorý je použitý pre sieť a podľa *MAC adresy* si doplní identifikátor rozhrania.



Obr. 13: Objavovanie linkových adries susedov a duplicity [2][5]

Hostia používajú Dynamic Host Configuration Protocol (**DHCP**), aby dostali IPv6 adresy. Tento **adresný manažment** je podobný chovaniu IPv4 (*RFC 3315*), kde boli adresy priradované centrálnou autoritou DHCP serverom. *DHCPv6* sa skladá (Obr. 14): [4]

1. Požiadavka (**Solicit**) – DHCPv6 klient hľadá server, posiela žiadosť na multicast adresu (všetci DHCPv6 relay agenti a servery) na konfiguráciu IP adresy;
2. Inzerát (**Advertise**) – správa s obsahujúcou konkrétnou možnosťou konfigurácie od DHCPv6 servera, ktorý prijal žiadosť a má platnú konfiguráciu IPv6 pre klienta;
3. Žiadosť (**Request**) – klient vyberie zo všetkých možností jednu konfiguráciu a odošle vybranému serveru požiadavku o pridelenie konkrétnej adresy;
4. Odpoveď (**Reply**) - server odošle požadovanú konfiguráciu pomocou tejto správy;



Obr. 14: Štyri správy stavovej DHCPv6 medzi klientom a serverom [1][6]

DHCPv6 zavádza **DUID** (DHCP Unique Identifier), je daný výrobcom, ktorý náhodne vygeneruje zvolené hexadecimálne znaky so špecifickou dĺžkou reťazca. *DUID* je viazané na **operačný systém**, je trvalý v čase a nemal by závisieť na technickom vybavení klienta. Spätne priradenie IPv6 adresy k danému klientovi cez *DHCPv6* je prakticky nemožné. Klient používa identifikátor (zhluk **konfiguračných informácií**), vďaka ktorému sa rozlišujú rozhrania, ktoré klient zahŕňa. Vďaka objavovaniu susedov a všetkých smerovačov, služba **DHCPv6** nemusí mať predvolený smerovač, a preto nie je poslaná ani klientovi. Klient sa ju vďaka **NDP protokolu** z lokálneho smerovača naučí. [6]

DHCP (bezstavový spojený s autokonfiguráciou SLAAC, RFC 2462)

Host' autonómne **konfiguruje** jeho vlastnú lokálnu linkovú adresu (pripojí identifikátor rozhrania). **Router Solicitation (RS)** sú posielané počas bootovania zariadenia, čím host' žiada o konfiguráciu, čím urýchli komunikáciu. Alebo **smerovač** sám v pravidelných intervaloch inzeruje všetky pripojené uzly v sieťovom segmente pomocou **Router Advertisement (RA)** - oznamovacie správy s informáciami o sieti a predvolenom smerovači pre pakety smerované mimo siete. Pomocou **objavovania susedov** sa overí, či používa iný host' v sieti rovnakú linkovú adresu. Pokiaľ detekcia **duplicitných adries (DAD)** prebehne v poriadku a sú obdržané všetky parametre zo smerovača, uzol si adresu pridelí (*RFC 3315*). **Lokálna linková adresa** je povinná pre komunikáciu dvoch susedných zariadení, navyše sa používa i v smerovacích protokoloch ako next-hop adresy,

avšak nie sú smerovateľné. Ich **platnosť** je len v rámci sieťovej domény, preto pri ich použití je potreba špecifikovať rozhranie (*ping* na susedovu lokálno-linkovú adresu). [4]

DHCPv6 (stavový)

Hostia používajú *Dynamic Host Configuration Protocol (DHCP)*, aby dostali IPv6 adresy. Možnosti stavovej *DHCPv6* konfigurácie je venovaná nasledujúca laboratórna úloha 2.

2.4 Požadované zdroje:

GNS3 a Wireshark

IOS smerovače – **šablóna smerovača** s Ethernet rozhraním [3]

2.5 Postup:

Prvá jednoduchšia **topológia** obsahuje 2 smerovače *c7200*, ktoré sú navzájom prepojené pomocou rozhrania Ethernet 1/0. **Smerovač R2** bude náš *DHCP server* a *R1* sa bude správať ako klient použitím *ip address dhcp* pod špecifickým rozhraním. Následne vo **Wiresharku** sa môžu pozrieť na celú komunikáciu medzi *R1*(klientom) a *R2*(serverom). **DHCP server** sa nastavuje priamo v konfiguračnom rozhraní, definovaním poolu s menom *FAI_pool*. Následne je špecifikovaný **adresný rozsah** pomocou adresy a masky. Ďalej je dobrým zvykom nastaviť **predvolenú bránu**, *DNS server* (Google 8.8.8.8) v neposlednej rade sa doba pôžičky adresy a vyhradený rozsah. **Vyhradený rozsah** (excluded addresses) sa používa pre servery, smerovače a statické adresy, na ktoré sú odkazované ostatné služby, ktorých zmenou by sa mohla ovplyvniť stabilita a funkcia aplikácií. V laboratórnej úlohe bolo vyčlenených prvých 10 adries z podsieťového rozsahu. Je dôležité si krokovať **konfiguráciu**, preto sú ukázané i príkazy na overenie nastavenia DHCP servera a pridelených adries klientom s možnosťou párovať MAC adresu s IP adresou. [4]

Čo sa týka *IPv6*, otestujú si **bezstavovú autokonfiguráciu (SLAAC)**, pri ktorej sa host naučí prefix použitím *NDP*, vezme prefix a vytvorí si vlastnú *IP adresu* a identifikátor rozhrania. Identifikátor **rozhrania** je špecifický pre *MAC adresu* (*Cisco* používa *EUI-64*, ostatné systémy si môžu použiť náhodné hodnoty), na záver sa ešte otestuje duplicita adries, že v sieti nie je použitá inou stanicou. Vďaka **SLAAC** sa klient naučí IP a prefix, ale nie *DNS server*. Toto je slabinou, ktorou sa líši **stavový DNS server**. Stavom sa myslia IP adresy, ktorých doba prenájmu vypršala. *SLAAC* si neudržiava záznam o ničom o klientoch. Stavový **DHCPv6** pracuje podobne ako *v4* len používa odlišné vyjednávacie

správy, čo je popísané v 1.2.5 diplomovej práci. *DHCP* poskytuje nám IP adresu, **prefix**, DNS server a NDP zabezpečí predvolenú bránu prípadne ďalšie voľby pre klienta. V prípade, že **DHCP** server nie je na rovnakej podsieti je vyžadovaný *DHCP relay* pre posunutie správy na centrálny DHCP server, k čomu využíva *IPv6* špeciálne multicast adresy (*FF02::1:2*). [5]

Pre **konfiguráciu** rozhraní virtuálnych liniek a nastavenie databázy užívateľov sa používajú nasledujúce príkazy:

Tab. 3: Syntax aplikovaných príkazov a vysvetlenie významu pri konfigurácii DHCPv4 [autor]

	Syntax + Príkaz	Význam/Účel
Syntax príkazu: Krok 1:	ip dhcp pool name R2(config)# ip dhcp pool FAI_pool	Vytvorenie mena DHCP a vstup do konfig. režimu.
Syntax príkazu: Krok 2:	network network-number [{mask /prefix-length}] R2(dhcp-config)# network 10.1.1.0 255.255.255.0	Špecifikácia siete a masky prípadne prefixu
Syntax príkazu: Krok 3:	default-router address [address2 ... address8] R2(dhcp-config)# default-router 10.0.0.2	Špecifikácia predvoleného smerovača pre klienta
Syntax príkazu: Krok 4:	dns-server address [address2 ... address8] R2(dhcp-config)# dns-server 8.8.8.8	Špecifikácia DNS servera pre klienta
Syntax príkazu: Krok 5:	domain-name domain R2(dhcp-config)# domain-name fai.utb.cz	Špecifikácia domény pre klienta
Syntax príkazu: Krok 6:	lease {days [hours [minutes]] infinite} R2(dhcp-config)# lease 2	Špecifikácia doby prenajatia adresy pre
Syntax príkazu: Krok 7:	ip dhcp excluded-address low-address [high-address] R2(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.24	Špecifikácia adresy, kt. DHCP server nesmie dať
Syntax príkazu: Krok 8:	ip helper-address R2(config)# ip helper-address 10.1.1.9	Povoľuje posúvať UDP broadcast z rozhrania
Syntax príkazu: Krok 9:	show ip dhcp pool R2# show ip dhcp pool	Zobrazenie nastavenia DHCP poolu IPv4 adresy
Syntax príkazu: Krok 10:	ip address dhcp R1(config-if)# ip address dhcp	Nastavenie klienta pre použitie DHCP
Syntax príkazu: Krok 11:	show dhcp server R1#show dhcp server	Zobrazenie nastavenia DHCP servera zo strany
Syntax príkazu: Krok 12:	show ip route begin Gateway R1#show ip route begin gateway	Zobrazenie smerovej tabuľky a bránu
Syntax príkazu: Krok 13:	copy running-config startup-config /write memory R2 (config-if)# # copy running-config startup-config	Uloženie aktuálneho nastavenia do NVRAM.

Nakoľko v pôvodnej konfigurácii je nastavený rozsah pre 2 aktívne adresy, je potrebné zmeniť obe nastavenia sieťových kariet. Na strane servera je potreba postupovať príkazmi podľa Tab. 26 a zmeniť maska rozhrania *Ethernet1/0* na 255.255.255.0. Na strane klienta zrušiť statické nastavenie, ideálne rozhranie dať do predvoleného stavu pomocou *default*

interface Ethernet1/0 a následne použitím príkazu *ip address dhcp* pre DHCP pod špecifickým rozhraním sa nám automaticky prideli IP adresa pre port. Pred samotným aktivovaním portu bolo zapnutie zachytávanie paketov. [1]

```
R2#show ip dhcp pool
```

```
Pool FAI_pool :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 1
Excluded addresses               : 20
Pending event                     : none
1 subnet is currently in the pool :
Current index      IP address range      Leased/Excluded/Total
10.2.2.72         10.2.2.1          - 10.2.2.254        1 / 20 / 254
```

Obr. 15: Zobrazenie nastavenia DHCP poolu IPv4 adres na smerovači R2 [autor]

Príkazy v kroku 12-14 sa **používajú** u hostí s Windows OS pre zobrazenie informácií o sieťovej karte. V konečnom dôsledku pri správe veľkého množstva klientov je dobrým zvykom si vytvoriť zoznam host'ov s odpovedajúcimi L2 a L3 adresami pre autentifikáciu chýb ako je to v ďalšej tabuľke Tab. 4.

Tab. 4: Laboratórna úloha DHCP súkromná kancelária- Posledná zmena:2/18/2016 [autor]

Sieť L3	Maska	MAC L2	Popis
10.2.2.1-254	255.255.255.0	*	Rozsah adres pre kanceláriu
10.2.2.1-20	255.255.255.0	cc01.2938.0010	IP pre server
10.2.2.1	255.255.255.0	0063.6973.636f.2d63.	DHCP SERVER
10.2.2.71	255.255.255.0	0001.6322.2222	Sekretariát/Účtovníčka
10.2.2.72	255.255.255.0	0001.6322.1111	Marketing

Keď sa aktivuje ladenie *debug ip dhcp server events*, tak je vidieť ako **DHCP server** kontroluje prenájaté adresy, prípadne sa prideli nová adresa. Pokiaľ chcú skontrolovať počet **žiadosti** slúži k tomu príkaz *show ip dhcp server statistics*, tým si môžu overiť či niekto negeneruje podvrhované žiadosti a nevznikajú konflikty v tabuľke. [4]

Pomocou príkazov vyššie v Tab. 3 sa **nakonfiguruje** R2 DHCP server a pred samotným spustením DHCP **offer** na R1 klient pomocou *ip dhcp auto* spustí sa Wireshark. Po aktivácii **autokonfigurácie** sa na strane klienta objaví systémový log o pridelení adresy:

```
*Mar 1 00:21:36.611: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 10.2.2.1, mask 255.255.255.0, hostname R1
```

```
R1#show dhcp server
DHCP server: ANY (255.255.255.255)
Leases: 1
Offers: 1      Requests: 1      Acks : 1      Naks: 0
Declines: 0    Releases: 0      Query: 0      Bad: 0
DNS0: 8.8.8.8, DNS1: 0.0.0.0
Subnet: 255.255.255.0  DNS Domain: fai.utb.cz
```

Obr. 16: Zobrazenie štatistik DHCP poolu IPv4 adres [autor]

Obr. 16 zobrazuje i priradený **DNS server** a predvolenú bránu, ktorú si môžu overiť pomocou smerovacej tabuľky. Pri tejto príležitosti je možné si vyskúšať filtrovanie pomocou **PIPE**, kde sa hľadá začínajúce slovo *Gateway* (predvolená brána):

```
R1#show ip route | begin Gateway
Gateway of last resort is 10.2.2.2 to network 0.0.0.0

    10.0.0.0/24 is subnetted, 1 subnets
C       10.2.2.0 is directly connected, Ethernet1/0
S*     0.0.0.0/0 [254/0] via 10.2.2.2
```

Obr. 17: Zobrazenie predvolenej brány (gateway) v smerovacej tabuľke [autor]

Následne je celá **premávka** a proces priradenia IPv4 je možné zobrazit' vo Wiresharku. Pomocou filtru *bootp*, čo je predchodca DHCP. [4]

Obr. 18 zobrazuje paket78, ktorý po **rozrolovaní** nám prezradí detailné informácie o *L2* a *L3* vrstve. **L2 zdrojové rozhranie** je spojené s *Eth1/0 (0001.6311.1111)* a cieľovou broadcast adresou (*FFFF.FFFF.FFFF*) s nádejou, že je v sieti zariadenie, ktoré odpovie na discovery paket. Pokiaľ sa rozrolujú **L3 informácie**, zjavia sa *0.0.0.0* ako zdrojová *L3* adresa a broadcast *255.255.255.255* ako cieľová adresa, čo je logické, pretože host' ešte nevie adresu, aká mu bude pridelená a posieľa to na všetkých host'ov v broadcastovej doméne.[5]

The screenshot displays the Wireshark interface with a filter set to 'bootp'. The packet list pane shows several DHCP Discover packets followed by a DHCP Offer packet (No. 82) and a DHCP Request packet (No. 83). The Offer packet is highlighted with a red box. The packet details pane for the Offer packet shows the following structure:

- Ethernet II, Src: Cisco_11:11:11 (00:01:63:11:11:11), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: Cisco_11:11:11 (00:01:63:11:11:11)
- Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
 - Version: 4
 - Header Length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECT))
 - Total Length: 604
 - Identification: 0x0011 (17)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 255
 - Protocol: UDP (17)
 - Header checksum: 0xb980 [validation disabled]
 - Source: 0.0.0.0 (0.0.0.0)
 - Destination: 255.255.255.255 (255.255.255.255)
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]
- User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
- Bootstrap Protocol (Discover)

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII part shows the broadcast address 'C...D.C.H...E...'.

Obr. 18: Ukážka zachyteného DHCP offer paketu s L2 a L3 broadcastu [autor]

Wireshark tiež odкрýva IP hlavičku s protokolom *UDP (17)* a L4 informácia so zdrojovým portom *68* (*klient = R1*) a cieľový port *67* (*server = R2*). Jedná sa o známe **porty** pridelené pre DHCP proces. Ďalšie **správy** discover, offer, request a acknowledgment môžu byť preskúmané v uloženom wireshark súbore. Nižšie v **dátovej časti** je vidieť zaťaženie, čo predstavuje bootstrap protokol, kde je zaujímavý *bootp flag*, čo znamená, že každý klient si nastaví broadcast a všetky 4 správy bude klient posielat' na broadcastovú adresu. Nasledujúca správa offer posielala DHCP server **ARP žiadosť** so

správou: „ Používa niekto adresu *10.2.2.1* ak áno pošli mi *L2* adresu .“ Týmto sa **DHCP server** vyhne prenájmu adresy, ktorá je použitá inou stanicou. Pokiaľ **ARP** je úspešné, *DHCP server* bude pokračovať pingom danej adresy, čo potvrdí používanie danej adresy niekým iným. Nakoniec daná **adresa**, teda nemôže byť použitá, inak by došlo ku konfliktu. Nakoľko v našej jednoduchšej topológii nik danú adresu nepoužíval a neexistuje žiadna **ARP odpoveď**, server ponúkne danú adresu klientovi. Pri detailnom preskúmaní paketu 82 „*OFFER*“ **zdrojový port** je 67 a **cieľový** 68 a ponúka adresu *10.2.2.1*.

Pri **rolovaní** nižšie je zaujímavé, že sieťová maska, predvolená brána, *DNS server* je už v tejto správe. Následne v pakete 83 **REQUESTU** klient potvrdzuje, že je spokojný s pridelenou adresou a pokračuje vo vyjednávaní. **Výsledok** je paket 84 **ACKNOWLEDGEMENT** s kópiou ip adresy, sieťovej masky, predvolenej brány a *DNS servera*. [4][8]

78	152.790739	0.0.0.0	255.255.255.255	DHCP	618	DHCP Discover	-
82	154.856857	10.2.2.2	255.255.255.255	DHCP	342	DHCP Offer	-
83	154.876858	0.0.0.0	255.255.255.255	DHCP	618	DHCP Request	-
84	154.932861	10.2.2.2	255.255.255.255	DHCP	342	DHCP ACK	-


```

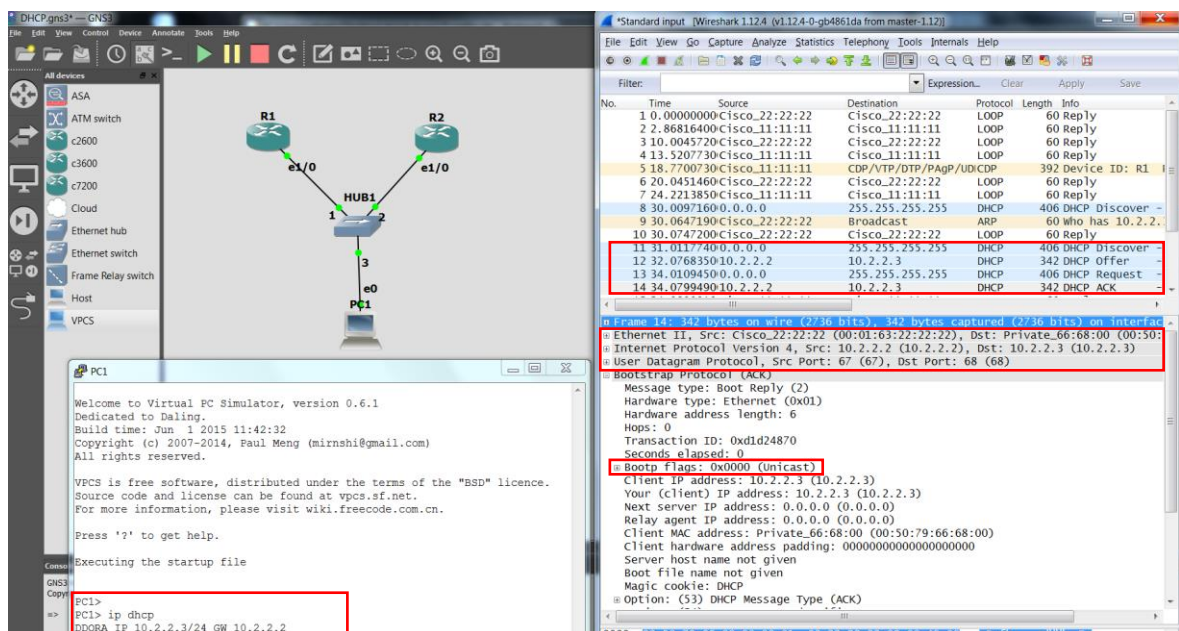
⊞ Bootp flags: 0x8000 (Broadcast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 10.2.2.1 (10.2.2.1)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: Cisco_11:11:11 (00:01:63:11:11:11)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
⊞ Option: (53) DHCP Message Type (ACK)
  Length: 1
  DHCP: ACK (5)
⊞ Option: (54) DHCP Server Identifier
  Length: 4
  DHCP Server Identifier: 10.2.2.2 (10.2.2.2)
⊞ Option: (51) IP Address Lease Time
  Length: 4
  IP Address Lease Time: (86400s) 1 day

```

Obr. 19: Zobrazenie bootp flagu a detail **ACKNOWLEDGEMENT** od servera [autor]

Druhou možnosťou je **priradenie** unicast možnosti pre *DHCP*. Overiť je to možné pomocou **virtuálneho PC** v GNS3, napríklad pripojením R1 do rozbočovača, R2 do rozbočovača pomocou rovnakých rozhraní a PC tiež pre žiadosť *DHCP*. GNS3 má k dispozícii *Virtual PC* simulátor, voľne dostupný navrhnutý Paulom Mengom, ktorý je veľmi jednoduché pre ovládanie. Pre nastavenie **automatickej konfigurácie** jednoducho sa použije *ip dhcp* príkaz, čo spôsobí, že PC prejde celým procesom. Skrátené pri trakovaní

rozdiel oproti predchádzajúcej verzii je *nenastavenie bootp flagu*, čo spôsobí posielanie Unicastu od DHCP servera na rozdiel od predchádzajúceho broadcastu. Na základe poslanej **MAC adresy** server odpovedá pomocou L2 adresy a správa sa dostane späť na PC. Takže ešte pred priradením **IP adresy** klientovi je použitá cieľová MAC adresa. Až po posledný paket, čo je **DHCP acknowledgment**, ktorý posiela späť na cieľovú MAC adresu klienta, ktorý požadoval IP adresu, je nahrávaná premávka dát vo Wiresharku. [8]



Obr. 20: Priradenie IPv4 adresy pre virtuál PC pomocou Unicast možnosti pre DHCP [autor]

Potvrdenie priradení IP adres z pohľadu DHCP servera:

```
R2#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/
                Hardware address/
                User name
10.2.2.1        0063.6973.636f.2d30.
                3030.312e.3633.3131.
                2e31.3131.312d.4574.
                312f.30
10.2.2.3        0100.5079.6668.00      Feb 23 2016 09:20 PM   Automatic   Active
```

Obr. 21: Kontrola priradených unicast IPv4 adres pomocou show ip dhcp binding [autor]

Tab. 5: Show příkazy overující DHCP nastavenie a DHCPv4 konfigurácie [autor]

R1	R2
<pre>R1#show run inter eth 1/0 R1(config)# ipv6 unicast-routing R1(config)#interface Ethernet1/0 R1(config-if)#mac-address 0001.6311.1111 R1(config-if)# ip address dhcp R1(config-if)# full-duplex R1(config-if)# ipv6 address 2001:DB8:FABC:111::5/64 R1(config-if)#ipv6 enable R1(config-if)#no shutdown R1(config-if)# interface Loopback1 R1(config-if)# ipv6 address 2001:DB8:FBBC:6666::6666/128 R1(config-if)#ipv6 enable R1(config-if)#no shutdown</pre>	<pre>R2# show ip route begin Gateway R2# ip dhcp pool R2# ip dhcp server R2(config)# ipv6 unicast-routing R2(config)#ip dhcp pool FAI_pool R2(dhcp-config)# network 10.2.2.0 255.255.255.0 R2(dhcp-config)# default-router 10.2.2.2 R2(dhcp-config)# dns-server 8.8.8.8 R2(dhcp-config)# domain-name fai.utb.cz R2# show ip dhcp binding R2# show ip dhcp server statistics R1(config)#interface Ethernet1/0 R1(config-if)#mac-address 0001.6311.1111 R1(config-if)# ip address dhcp R1(config-if)# full-duplex R1(config-if)# ipv6 address 2001:DB8:FABC:111::5/64 R1(config-if)#ipv6 enable</pre>






V prípade ďalšej **zákazníckej siete** za smerovačom R1 je možné použiť tzv. Relay agenta, ktorý bude predávať žiadosti na **DHCP server** a nebolo potrebné vytvárať ďalší server a zvýšili s tým integritu použitých adries. Z technologického hľadiska je z dôvodu obmedzenia broadcastovej domény, potrebné pridať **funkcionalitu** preposielania UDP broadcastov, ktoré sú prijaté na rozhranie. Nasledujúca Tab. 6 ukazuje ako to nastaviť:

Tab. 6: Vytvorenie sumarizácie ciest na sériovom rozhraní S0/0 na smerovači MARS [autor]

<pre>R1(config-if)# interface Eth1/1 R1(config-if)# ip helper-address 10.2.2.2 R2(config)# ip dhcp excluded-address 10.2.2.110.2.2.10</pre>

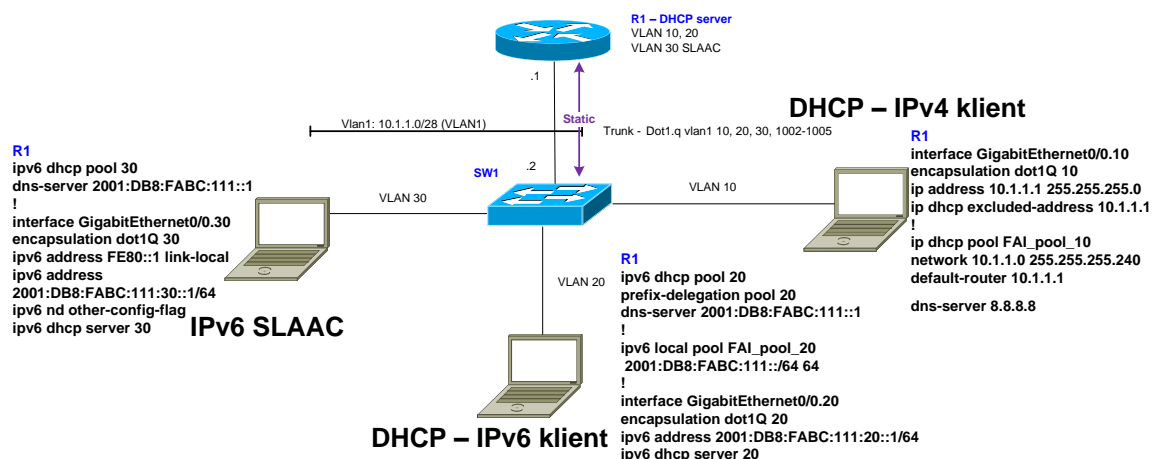
Posledným **příkazom** z Tab. 6 je možné vyčleniť adresy pre servery a statické pridelenia. Výsledné **nastavenie** smerovačov pre overenie funkčnosti IPv4 a IPv6 adresácie a zisťovania MAC adries.

Tab. 7: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

R1	R2	vPCs	Wireshark UNI	Wireshark BC
 R1.txt	 R2.txt	 vPC .txt	 dhcp_unicast.pcapng	 dhcpbc.pcapng

Na základe predchádzajúcej laboratórnej úlohy IPv6 a NDP je zrejmé, čo všetko je potrebné **konfigurovať** pre aktivovanie IPv6 adres, príp. predchádzajúca jednoduchšia topológia mala nastavené statické IPv6 adresy. Bolo zmienené, ako prebieha **zistovanie a asociácia** adres L3 vrstvy s adresami L2 vrstvy. Táto úloha používa i **simuláciu prepínača** pre rozdelenie podsietí pri virtuálnej lokálnej sieti VLAN. Nakoľko je možné sa stretnúť so správou **dynamických adres** pomocou externých DHCP serverov, spravovaných systémovými administrátormi – toto je dôležité si ujasniť pri navrhovaní dizajnu siete za okrúhlym stolom v prítomnosti všetkých strán, kto za čo zodpovedá. [5]

V nasledujúcej laboratórnej úlohe sa predpokladá, že je **potrebné** riešiť DHCP pre IPv4 a IPv6 smerovače, nakoľko sa chcú ušetriť náklady za ďalšiu externú službu. Ukážka možného návrhu **DHCPv6 servera** na smerovači pre rôzne VLANy je na nasledujúcom obrázku i s konfiguráciou:



Obr. 22: Príklad dizajnu všetkých možností IPv6 adresácie s konfiguráciou na smerovači [autor]

Predpokladá sa situácia, že **sieťový inžinier** má nastaviť **SLAAC** (bezstavový) a **stavový DHCPv6** pre zákazníka podľa topológie z bodu 2.2 a pre tretieho klienta s R5 má byť použitá **DHCPv4**, nakoľko sa rozhodol počkať s migráciou a použiť statické adresy IPv6, takže sa zopakuje nastavenie z predchádzajúcej časti, ktoré už nebude popisované.

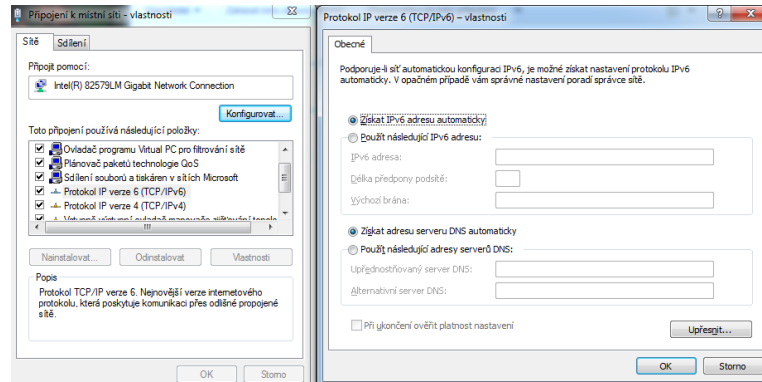
2.5.1 Prepoj sieť podľa druhej topológie z bodu 2.2 a nastav základné nastavenie.

Podľa obrázku je potreba prepojiť sieť v prípade použitia **emulovaného prepínača** a je potrebné aktivovať šablónu s podporou IPv6 (*sdm prefer dual-ipv4-and-ipv6 default*). **Základné nastavenie** sa rozumie vypnutie **DNS lookup**, premenovanie zariadenie, nastavenie banerov, šifrovanie hesiel v zdrojovom kóde, pridanie autentifikácie pre

privilegovaný režim, konzolu a virtuálne linky, prípadne nastavenie synchronizácia logovania a uloženie zmien do *NVRAM*. V prípade prepínača je dobrým zvykom zatvoriť nepoužívané porty, v prípade nepodpory *IOU* je možné preskočiť.[3]

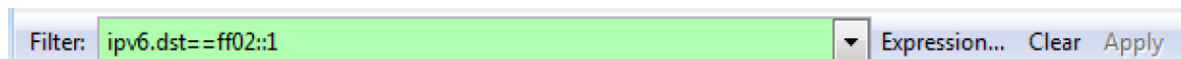
2.5.2 Nastavenie bezstavového DHCPv6 a aktivovanie IPv6.

Over **nastavenie** IPv6 sady v operačnom systéme v nastavení LAN.



Obr. 23: Nastavenie protokolu IPv6 (TCP/IPv6) v operačnom systéme Windows [autor]

V prípade **overenia** všetkých klientov. je možné zapnúť odchyťavanie paketov medzi *R1* a *SW1*. Vo Wiresharku je vhodné filtrovať **multicast** pre všetky uzly na linke *FF02::1*, z dôvodu kontroly len RA správ, ako je zobrazené nižšie:



Obr. 24: Filtrovanie multicast pre všetky uzly na linke FF02::1 [autor]

Na **smerovači** je potrebné povoliť zasielanie IPv6 prenosu k ostatným zariadeniam z *CEF* na smerovači *ipv6 unicast-routing*, nastaviť *FE80::1* the *IPv6 link-lokálnu adresu*, priradiť MAC adresy a aktivovať port *Eth1/0*. Samotné **nastavenie SLAAC**, overenie, že smerovač *R1* je súčasťou skupiny multicast je podobné predchádzajúcej laboratórnej úlohe.

Tab. 8: Nastavenie SLAAC na SW1 a zobrazenie nastavenia PC1 [autor]

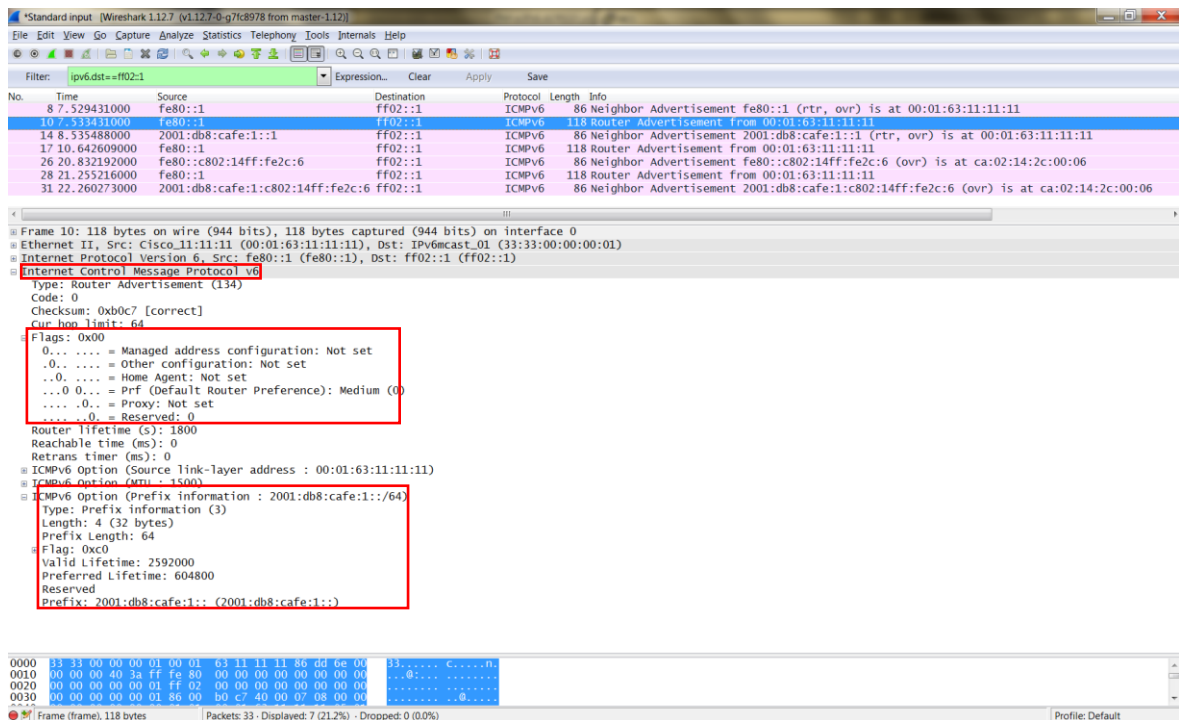
```
R1(config)# ipv6 unicast-routing
R1(config)# interface FastEthernet0/1
R1(config-if)#ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 address FE80::1 link-local
R1(config-if)# no shutdown
SW1(config-if)#interface vlan 1
SW1(config-if)#ipv6 address autoconfig
R1# show ipv6 interface g0/1
SW1# show ipv6 interface
PC1# ip auto
```

Pomocou jednoduchého `show ip (ipconfig /all)` príkazu je možné overiť nastavenie IPv6 pridelených adries a predvolený smerovač.

```
PC1> ip auto
GLOBAL SCOPE      : 2001:db8:cafe:1:2050:79ff:fe66:6800/64
ROUTER LINK-LAYER : 00:01:63:11:11:11
```

Obr. 25: Nastavená IPv6 adresa pomocou SLAAC pomocou VPC [autor]

V odchytených paketoch vo Wiresharku je vidieť **RA správy** alebo sa môže aktivovať filtrovanie pre multicast skupiny `FF02::1` pre host'ov vid' :[8]



Obr. 26: RA správa, ktorá bola zachytená; flag ICMPv6 rozlišuje typ DHCPv6 [autor]

Z predchádzajúceho Obr. 26 v **podložke flag** protokolu *ICMPv6* sa v prípade plnohodnotného *DHCPv6* nastavujú parametre Managed address configuration, Other configuration. Ďalšie overenie je na prepínači *SWI*, kde sa pomocou *SLAAC* získa IPv6 adresa pre rozhranie *VLANI*:

```

sw1#show ipv6 interface
FastEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::C802:14FF:FE2C:6
No Virtual link-local address(es):
Stateless address autoconfig enabled
Global unicast address(es):
  2001:DB8:CAFE:1:C802:14FF:FE2C:6, subnet is 2001:DB8:CAFE:1::/64 [EUI/CAL/PRE]
    valid lifetime 2591982 preferred lifetime 604782
Joined group address(es):
  FF02::1
  FF02::1:FF2C:6
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
Default router is FE80::1 on FastEthernet0/1

```

Obr. 27: Overenie poskytnutej IPv6 unicast adresy pomocou SLAAC [autor]

2.5.3 Nastav bezstavový DHCPv6 na smerovačoch R3 a R4 s podporou DNS

Nasledujúca časť sa **zameriava** na nastavenie bezstavového **DHCPv6** na smerovači. Po **priradení adresy** si nepamätá stavy daných adries, čo je overené v nasledujúcej časti.

Tab. 9: Nastavenie bezstavového DHCPv6 na R3 a R4 a zobrazenie nastavenia DHCPv6 [autor]

```

R3/R4 (config)# ipv6 unicast-routing
R3(config)# ipv6 dhcp pool cafe-test-luki
R3(config-dhcpv6)# domain-name fai.utb.cz
R3(config-dhcpv6)# dns-server 2001:DB8:CAFE:2::DB01
R3(config-dhcpv6)# exit
R3/R4 (config)# interface Ethernet1/0
R3(config-if)#ipv6 address FE80::1 link-local
R3(config-if)#ipv6 address 2001:DB8:CAFE:2::1/64
R3/R4(config-if)#ipv6 enable
R4(config-if)#ipv6 address autoconfig
R3(config-if)# ipv6 dhcp server cafe-test-luki
R3(config-if)# ipv6 dhcp server cafe-test-luki rapid-commit
R3(config-if)# ipv6 nd other-config-flag
R3(config-if)# end
R3# show ipv6 dhcp binding
R3/R4# show ipv6 dhcp interface Eth1/0
R3/R4# show ipv6 interface Eth1/0
R3# show ipv6 dhcp pool

```

Po **nastavení smerovačov** si opäť pre kontrolu nastaví odchyťovanie paketov vo Wiresharku a povolí ladenie na oboch smerovačoch: [8]

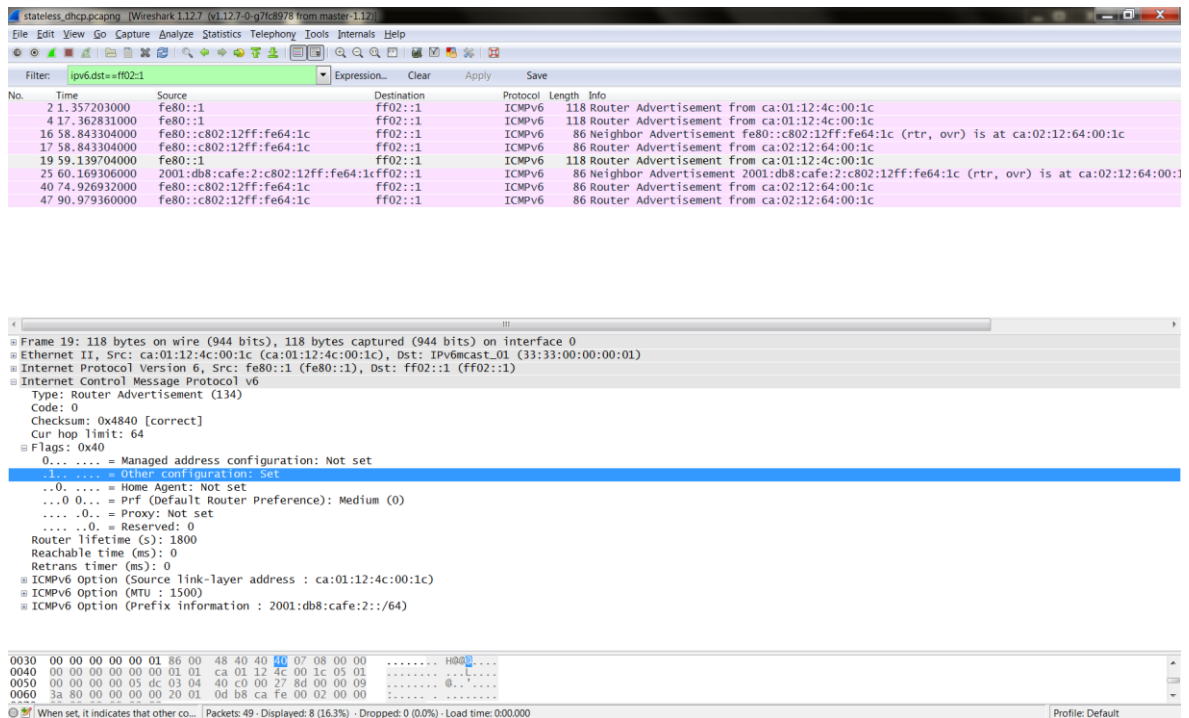
```
R4(config)#inter e1/0
R4(config-if)#shu
R4(config-if)#no shu
*Mar 28 07:30:41.823: IPv6 DHCP: Stopping client stateless autoconfig
*Mar 28 07:30:41.823: IPv6 DHCP: Unconfiguring DNS server 2001:DB8:CAFE:2::DB01
*Mar 28 07:30:41.827: IPv6 DHCP: Unconfiguring domain name fai.utb.cz
R4(config-if)#no shut
R4(config-if)#
*Mar 28 07:30:45.343: IPv6 DHCP: detailed packet contents
*Mar 28 07:30:45.343:   src FE80::C802:12FF:FE64:1C
*Mar 28 07:30:45.343:   dst FF02::1:2 (Ethernet1/0)
*Mar 28 07:30:45.343:   type INFORMATION-REQUEST(11), xid 2378002
*Mar 28 07:30:45.343:   option ELAPSED-TIME(8), len 2
*Mar 28 07:30:45.343:     elapsed-time 0
*Mar 28 07:30:45.343:   option CLIENTID(1), len 10
*Mar 28 07:30:45.343:     00030001CA0212640008
*Mar 28 07:30:45.343:   option ORO(6), len 4
*Mar 28 07:30:45.343:     DNS-SERVERS,DOMAIN-LIST
*Mar 28 07:30:45.343: IPv6 DHCP: Sending INFORMATION-REQUEST to FF02::1:2 on Ethernet1/0
*Mar 28 07:30:45.343: IPv6 DHCP: DHCPv6 changes state from IDLE to INFORMATION-REQUEST (STATELESS) on Ethernet1/0
*Mar 28 07:30:45.355: IPv6 DHCP: Received REPLY message
*Mar 28 07:30:45.355: IPv6 DHCP: Received REPLY from FE80::1 on Ethernet1/0
*Mar 28 07:30:45.359: IPv6 DHCP: detailed packet contents
*Mar 28 07:30:45.359:   src FE80::1 (Ethernet1/0)
*Mar 28 07:30:45.359:   dst FE80::C802:12FF:FE64:1C (Ethernet1/0)
*Mar 28 07:30:45.359:   type REPLY(7), xid 2378002
*Mar 28 07:30:45.359:   option SERVERID(2), len 10
*Mar 28 07:30:45.359:     00030001CA01124C0008
*Mar 28 07:30:45.359:   option CLIENTID(1), len 10
*Mar 28 07:30:45.359:     00030001CA0212640008
*Mar 28 07:30:45.359:   option DNS-SERVERS(23), len 16
*Mar 28 07:30:45.359:     2001:DB8:CAFE:2::DB01
*Mar 28 07:30:45.359:   option DOMAIN-LIST(24), len 12
*Mar 28 07:30:45.359:     fai.utb.cz
*Mar 28 07:30:45.359: IPv6 DHCP: Adding server FE80::1
*Mar 28 07:30:45.359: IPv6 DHCP: Processing options
*Mar 28 07:30:45.359: IPv6 DHCP: Configuring DNS server 2001:DB8:CAFE:2::DB01
*Mar 28 07:30:45.359: IPv6 DHCP: Configuring domain name fai.utb.cz
*Mar 28 07:30:45.359: IPv6 DHCP: DHCPv6 changes state from INFORMATION-REQUEST to IDLE (REPLY_RECEIVED) on Ethernet1/0
```

Obr. 28: Ladenie bezstavového DHCPv6 na R4 po zatvorení a otvorení rozhrania Eth1/0

[autor]

Tab. 10: Nastavenie ladenie bezstavového DHCPv6 na R3 a R4 [autor]

```
R3/R4#debug ipv6 dhcp
R3/R4#debug ipv6 dhcp detail
R3/R4#debug ipv6 dhcp database
R3#undebug all
```



Obr. 29: Zachytené RA správy vo FLAG nastavení je nastavený Other configuration [autor]

Overíme DHCP, že nie sú klienti - príkazy *show ipv6 dhcp binding, show ipv6 dhcp pool*:





Tab. 11: Overenie nastavenia bezstavového DHCPv6, kde sa neukladá stav IPv6 adries [autor]

R3	R4
<pre>R3#show ipv6 dhcp pool DHCPv6 pool: cafe-test-luki DNS server: 2001:DB8:CAFE:2::DB01 Domain name: fai.utb.cz Active clients: 0 R3#show ipv6 dhcp inter R3#show ipv6 dhcp interface Ethernet1/0 is in server mode Using pool: cafe-test-luki Preference value: 0 Hint from client: ignored</pre>	<pre>R4#show ipv6 dhcp interface Ethernet1/0 is in client mode State is IDLE List of known servers: Reachable via address: FE80::1 DUID: 00030001CA01124C0008 Preference: 0 Configuration parameters: DNS server: 2001:DB8:CAFE:2::DB01 Domain name: fai.utb.cz</pre>

Bezstavový DHCPv6 je praktický a menej náročný na konfiguráciu, vo väčších organizáciách môže byť spojený so stavovým DHCPv6, ktorý sa stará o DNS a NTP. Nakoľko sa tento typ nestará o **stav požičaných IPv6 adries** vo veľkých organizáciách práce toto zabezpečí obrovský pokles réžií. U *IPv6* neriešime množstvo **IPv6 adries**.

Výsledné **nastavenie** smerovačov pre overenie funkčnosti *bezstavového DHCPv6* na smerovačoch R3 a R4:[5]

Tab. 12: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

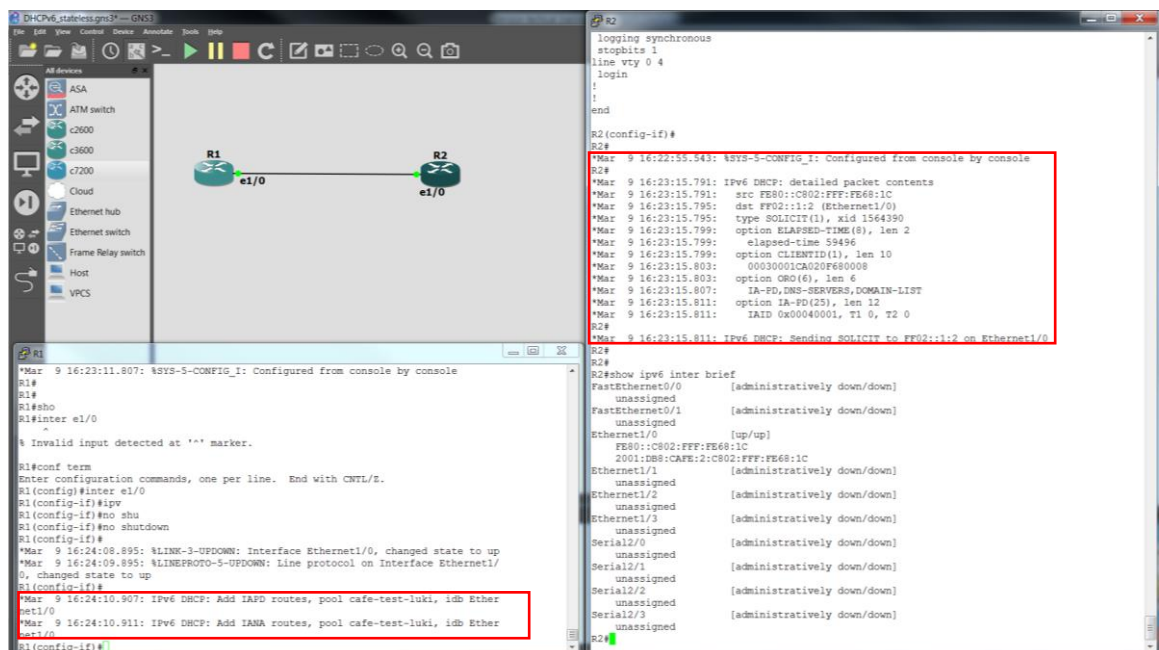
R3	R4	Wireshark	GNS3
 R3.txt	 R4.txt	 stateless.pcapng	 stateless_DHCPv6.gns3

2.5.4 Nastav stavový DHCPv6 na smerovačoch R3 a R4

Ako bolo napísané v teórii stavový **DHCPv6** je centrálné riadený a klienti získavajú IPv6 adresy prostredníctvom *DHCPv6 servera*, ktorý ich môže pridelovať pomocou módov:

- **Rapid-Commit** (zrýchlený) – výmena len dvoch správ (solicit and reply)
- **Normal Commit** (klasický) – klasická výmena správ podľa *Obr. 14*

V prípade **aktivovania** zrýchleného procesu je potrebné nastaviť klientovi i serveru. Obrovskou výhodou v prípade testovania v **GNS3**, že je možné si danú topológiu skladať ako lego, začne sa nastavovaním funkcionality medzi 2 smerovačmi, do ktorej následne sa pridávajú konfigurácie všetkých zariadení, ďalej je možný *ladenie DHCP* pri otvorení rozhrania:[5]



```

R1#
R1#
R1#show
R1#inter e1/0
% Invalid input detected at '' marker.
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#inter e1/0
R1(config-if)#ipv
R1(config-if)#no shu
R1(config-if)#no shutdown
R1(config-if)#
*Mar  9 16:24:08.895: %LINE-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Mar  9 16:24:09.895: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up
R1(config-if)#
*Mar  9 16:24:10.907: IPv6 DHCP: Add IAPD routes, pool cafe-test-luki, idb Ether
net1/0
*Mar  9 16:24:10.911: IPv6 DHCP: Add IANA routes, pool cafe-test-luki, idb Ether
net1/0
R1(config-if)#

R2#
logging synchronous
stopbits 1
line vty 0 4
login
!
!
end
R2(config-if)#
R2#
*Mar  9 16:22:55.543: %SYS-5-CONFIG_I: Configured from console by console
R2#
*Mar  9 16:23:15.791: IPv6 DHCP: detailed packet contents
*Mar  9 16:23:15.791: src FE80::C802:FFF:FE68:1C
*Mar  9 16:23:15.795: dst FF02::1:2 (Ethernet1/0)
*Mar  9 16:23:15.795: type SOLICIT(1), xid 1564390
*Mar  9 16:23:15.799: option ELAPSED-TIME(8), len 2
*Mar  9 16:23:15.799: elapsed-time 59496
*Mar  9 16:23:15.799: option CLIENTID(1), len 10
*Mar  9 16:23:15.803: 00030001CA020F680008
*Mar  9 16:23:15.803: option ORO(6), len 6
*Mar  9 16:23:15.807: IA-PD,DBS-SERVERS,DOMAIN-LIST
*Mar  9 16:23:15.811: option IA-PD(25), len 12
*Mar  9 16:23:15.811: IAID 0x00040001, T1 0, T2 0
R2#
*Mar  9 16:23:15.811: IPv6 DHCP: Sending SOLICIT to FF02::1:2 on Ethernet1/0
R2#
R2#show ipv6 inter brief
FastEthernet0/0      [administratively down/down]
                    unassigned
FastEthernet0/1     [administratively down/down]
                    unassigned
Ethernet1/0         [up/up]
                    FE80::C802:FFF:FE68:1C
                    2001:DB8:CAFE:2:C802:FFF:FE68:1C
Ethernet1/1         [administratively down/down]
                    unassigned
Ethernet1/2         [administratively down/down]
                    unassigned
Ethernet1/3         [administratively down/down]
                    unassigned
Serial2/0           [administratively down/down]
                    unassigned
Serial2/1           [administratively down/down]
                    unassigned
Serial2/2           [administratively down/down]
                    unassigned
Serial2/3           [administratively down/down]
                    unassigned
R2#

```

Obr. 30: Povolenie používania ladenia pri spustení DHCPv6 [autor]

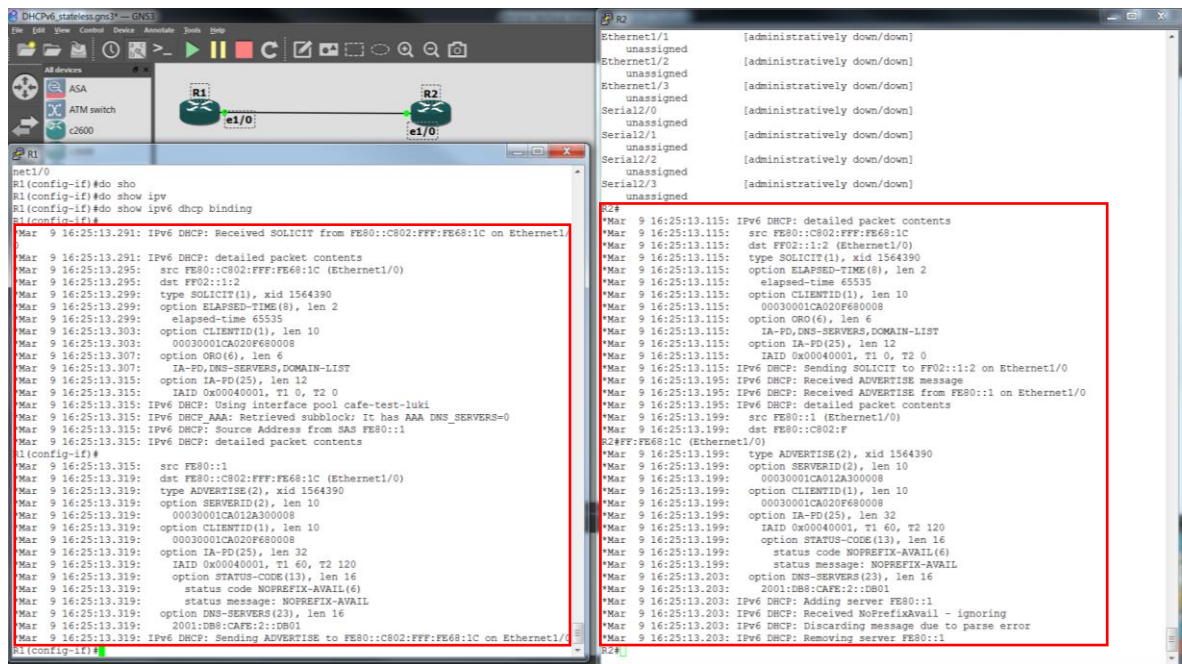
```

R1#show ipv6 inter e1/0
Ethernet1/0 is administratively down, line protocol is down
IPv6 is tentative, link-local address is FE80::201:63FF:FE11:1111 [TEN]
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:CAFE:2::1, subnet is 2001:DB8:CAFE:2::/64 [TEN]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
Hosts use DHCP to obtain other configuration.

```

Obr. 31: Povolenie používania DHCPv6 pre získanie smerovateľných adries [autor]

Podobne ako v predchádzajúcom pri **aktivácii posielania RA správ**, keď je rozhranie aktivované je potrebné u stavového servera aktivovať navyše *ipv6 nd managed-config-flag* pod rozhraním z dôvodu používania **DHCPv6** pre získanie smerovateľných adries. Posledné príkazy, ktoré musia byť aktivované sú *ipv6 nd route-owner*, *ipv6 nd autoconfig prefix*, *ipv6 nd autoconfig default-route*, ktoré **premostia** ND s RA prijímaných na rozhraniach a povolí ND zaviesť predvolenú cestu k smerovaču. Prípadne *ipv6 address dhcp rapid-commit* pre **povolenie módu rapid-commit**, čo musí byť nastavené i na strane servera vid' TAB nižšie. Následne začne prebiehať **celý proces** pridelovania adries spolu a preposielanie **DNS a NTP serverov** s uchovávaním záznamov o klientoch v databáze. [4]



Obr. 32: Ladenie správ pri stavovej DHCPv6 medzi klientom a serverom vid' Obr. 14

[autor]

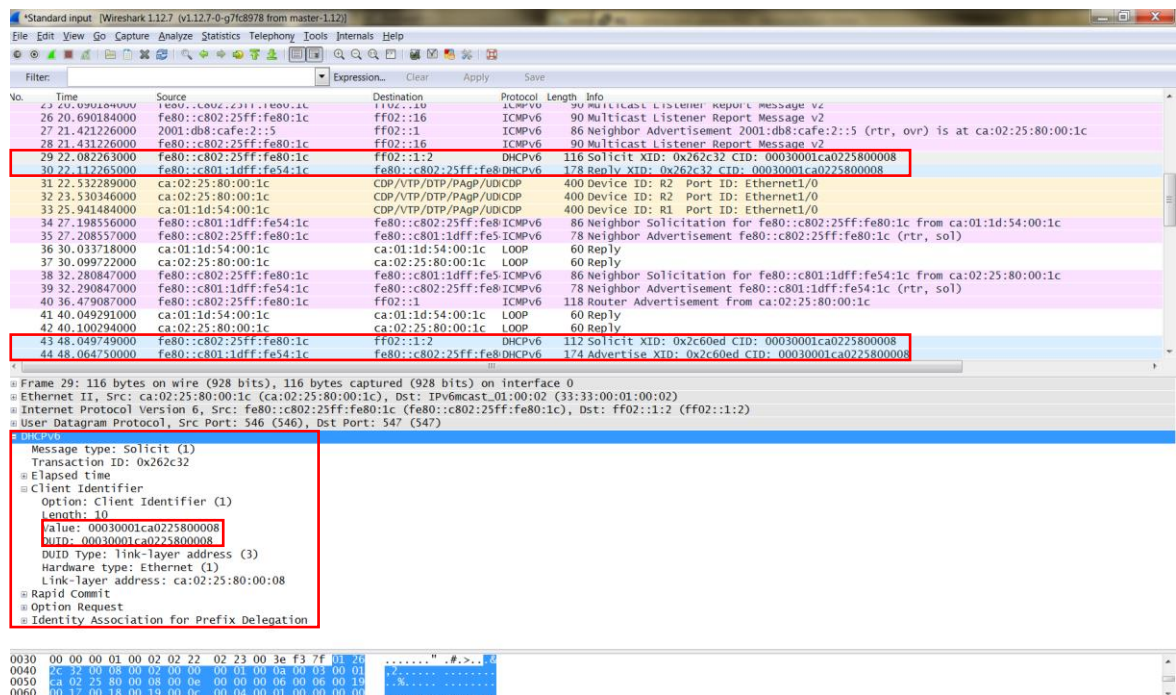
Následne už len sa pridá **prepínač**, kde sa otvoria potrebné porty a všetko je nastavené. S nastavením **DHCPv6** je možné obmedziť životnosť paketov pri špecifikácii prefixu pomocou voliteľného príkazu *lifetime*. Prípadne na smerovači R2, kto je **pozorný** si všimol, že je potrebné nastaviť i relay agenta z dôvodu odlišnej siete. Ide len o **príkaz** *ipv6 dhcp relay destination 2001:DB8:CAFE:1::1* FastEthernet1/0, čo je rozhranie do lokálnej siete FTP. Avšak pre **FTP** sa predpokladá nastavenie **statickej adresy** a dodatočné smerovanie, čo je náplňou ďalších laboratórnych úloh. [5]

Tab. 13: Nastavenie DHCPv6 na R1a R2 [autor]

```
R1/R2(config)# ipv6 unicast-routing
R1/R2(config)# ipv6 cef
!
R1(config)# ipv6 dhcp pool cafe-test-luki
R1(config-dhcpv6)# stavovy-fai.utb.cz
R1(config-dhcpv6)# 2001:DB8:CAFE:2::DB01
R1(config-dhcpv6)# exit
R1/R1 (config)# interface Ethernet1/0
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#ipv6 address 2001:DB8:CAFE:2::1/64
R1/R2(config-if)#ipv6 enable
R1(config-if)#ipv6 address autoconfig
R1(config-if)# ipv6 dhcp server cafe-test-luki
!R1(config-if)# ipv6 dhcp server cafe-test-luki rapid-commit !je možné použiť zrýchlený mód
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# end
R2(config)# interface Ethernet1/0
R2(config-if)# ipv6 address 2001:DB8:CAFE:2::5/64
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 dhcp client pd cafe-test-luki rapid-commit
R2(config-if)#ipv6 dhcp relay destination 2001:DB8:CAFE:2::1
R2(config-if)#ipv6 dhcp relay source-interface Ethernet1/0
R2(config-if)#ipv6 dhcp relay trust
!
R1# show ipv6 dhcp binding
R1/R2# show ipv6 dhcp interface Eth1/0
R1/R2# show ipv6 interface Eth1/0
R1# show ipv6 dhcp pool
```

```
R1(config-if)#
*Mar 28 12:21:24.583: IPv6 DHCP: Received SOLICIT from FE80::C802:25FF:FE80:1C on Ethernet1/0
*Mar 28 12:21:24.587: IPv6 DHCP: detailed packet contents
*Mar 28 12:21:24.587:   src FE80::C802:25FF:FE80:1C (Ethernet1/0)
*Mar 28 12:21:24.591:   dst FF02::1:2
*Mar 28 12:21:24.591:   type SOLICIT(1), xid 3252233
*Mar 28 12:21:24.591:   option ELAPSED-TIME(8), len 2
*Mar 28 12:21:24.595:     elapsed-time 0
*Mar 28 12:21:24.595:   option CLIENTID(1), len 10
*Mar 28 12:21:24.599:     00030001CA0225800008
*Mar 28 12:21:24.599:   option RAPID-COMMIT(14), len 0
*Mar 28 12:21:24.599:   option ORO(6), len 6
*Mar 28 12:21:24.599:     IA-PD,DNS-SERVERS,DOMAIN-LIST
*Mar 28 12:21:24.599:   option IA-PD(25), len 12
*Mar 28 12:21:24.599:     IAID 0x00040001, T1 0, T2 0
*Mar 28 12:21:24.599: IPv6 DHCP: Using interface pool cafe-test-luki
*Mar 28 12:21:24.603: IPv6 DHCP_AAA: Retrieved subblock; It has AAA DNS_SERVERS=0
*Mar 28 12:21:24.603: IPv6 DHCP: Source Address from SAS FE80::C801:1
R1(config-if)#DFF:FE54:1C
*Mar 28 12:21:24.603: IPv6 DHCP: detailed packet contents
*Mar 28 12:21:24.607:   src FE80::C801:1DFF:FE54:1C
*Mar 28 12:21:24.607:   dst FE80::C802:25FF:FE80:1C (Ethernet1/0)
*Mar 28 12:21:24.611:   type REPLY(7), xid 3252233
*Mar 28 12:21:24.611:   option SERVERID(2), len 10
*Mar 28 12:21:24.611:     00030001CA011D540008
*Mar 28 12:21:24.615:   option CLIENTID(1), len 10
*Mar 28 12:21:24.615:     00030001CA0225800008
*Mar 28 12:21:24.615:   option RAPID-COMMIT(14), len 0
*Mar 28 12:21:24.619:   option IA-PD(25), len 32
*Mar 28 12:21:24.619:     IAID 0x00040001, T1 60, T2 120
*Mar 28 12:21:24.619:   option STATUS-CODE(13), len 16
*Mar 28 12:21:24.623:     status code NOPREFIX-AVAIL(6)
*Mar 28 12:21:24.623:     status message: NOPREFIX-AVAIL
*Mar 28 12:21:24.631:   option DNS-SERVERS(23), len 16
*Mar 28 12:21:24.631:     2001:DB8:CAFE:2::DB01
*Mar 28 12:21:24.631:   option DOMAIN-LIST(24), len 20
*Mar 28 12:21:24.631:     stavovy-fai.utb.cz
*Mar 28
R1(config-if)# 12:21:24.631: IPv6 DHCP: Sending REPLY to FE80::C802:25FF:FE80:1C on Ethernet1/0
```

Obr. 33: Ladenie skráteneho DHCPv6 rapid-commit procesu [autor]



Obr. 34: Odchytené pakety s DUID (id klient a server DHCPv6) [autor]







DUID (DHCP Unique Identifier) jednoznačne **identifikuje** pár (klient, server), na základe linkovej lokálnej adresy a MAC adresy. **DUID** zostáva rovnaké i v prípade restartu. [5]

```
R2(config-if)#do sh ipv6 dhcp int
Ethernet1/0 is in client mode
State is SOLICIT
List of known servers:
  Reachable via address: FE80::C801:1DFF:FE54:1C
  DUID: 00030001CA011D540008
  Preference: 0
Configuration parameters:
  IA PD: IA ID 0x00040001, T1 60, T2 120
  DNS server: 2001:DB8:CAFE:2::DB01
  Domain name: stavovy-fai.utb.cz
Prefix name: cafe-test-luki
Rapid-Commit: enabled
```

Obr. 35: Kontrola DHCPv6 na strane klienta so špecifickým DUID [autor]

Nastavenie adres podľa *Obr. 11* písmeno *R* predstavuje odkaz na číslo smerovača, ktorý určuje **konvenciu** mien. V *R5* je pomocou *Eth1/1* je pripojený k prepínaču ako pobočka dcéry k topológii holdingu firmy. Výsledné **nastavenie smerovačov** pre overenie funkčnosti správy IPv4 a IPv6 adres pomocou *DHCPv4* a stavový a bezstavový *DHCPv6* + *SLAAC*:

Tab. 14: Konfigurácia smerovačov R1, R2 a R5 v Cisco IOS 15.2(4) S3 [autor]

R1	R2	R5	PCx	Wireshark UNI	GNS3
 R1.txt	 R2 DNS.txt	 R5.txt	 pc1_dhcp.txt	 dhcpv6statefull.zip	 DHCPv6_stavovys.gns3

2.6 Otázky na zamyslenie o DHCP IPv4 a IPv6:

1. Aké správy si vymieňa klient a DHCPv4/DHCPv6 server pri prenájme adresy.

DHCPv4 = Discover, Offer, Request, Acknowledgment

DHCPv6 = Solicit, Advertise, Request, Reply

2. Čo zabezpečuje protokol NDP ?

Objavovanie smerovačov

Objavovanie MAC adries

Detekcia duplicity adries

Bezstavová autokonfigurácia SLAAC

3. Aké spôsoby poznáte pre získanie IPv6 adresy ?

Statické pridelenie IPv6 adries

DHCP (bezstavový spojený s autokonfiguráciou SLAAC, RFC 2462)

DHCPv6 (stavový)

4. Pomocou akého príkazu je možné meniť šablónu pre koexistenciu IPv4 a IPv6 protokolov v prepínačoch? Aký príkaz povoľuje IPv6 adresy a smerovanie v sieti ?

Tab. 15: Nastavenie koexistencie IPv4 a IPv6 protokolu [autor]

```
SW1(config)# sdm prefer dual-ipv4-and-ipv6 default
R1(config)# ipv6 unicast-routing
```

5. Akým príkazom sa aktivuje SLAAC pre rozhranie ? Prečo potrebujeme stavový DHCPv6, keď pomocou SLAAC je možné získať IPv6?

Tab. 16: Nastavenie SLAAC IPv6 adresy pre rozhranie [autor]

```
R1(config-if)#ipv6 address autoconfig
```

SLAAC nám nezabezpečí výmenu DNS ani NTP serveru. Často je použité hybridné riešenie, kde sa využíva **minimálnych réžií** pri SLAAC a niekde je stavový DHCPv6.

6. Je možné urýchliť proces 4 správ pri získaní IPv6 adresy v stavovom DHCPv6 ?

Tab. 17: Nastavenie rapid-commit procesu v stavovom DHCPv6 [autor]

```
R3(config-if)# ipv6 dhcp server cafe-test-luki rapid-commit
```

3 STATICKÉ SMEROVANIE PRE IPV4 A IPV6

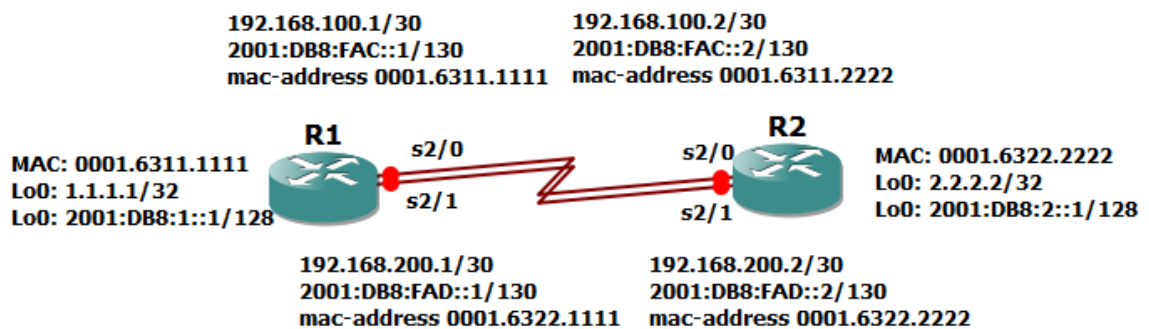
V tejto laboratórnej úlohe preskúmame možnosti **statického smerovania** pre *IPv4* a *IPv6*. Príkladom môže byť, že sieťový **špecialista**.

3.1 Zadanie:

Vytvor jednoduchú **topológiu** 2 smerovačov a over funkčnosť statického smerovania.

3.2 Topológia:

Konfigurácia IPv6 je rovnaká ako u protokola *IPv4* musíme mať heslo, doménu a kľúče.



Obr. 36: GNS3 topológia z laboratórnej úlohy Ethernet pre overenie funkčnosti statického smerovania [autor]

3.3 Teória:

Rozdiely medzi **smerovačmi** a **prepínačmi** je ľahké si predstaviť na základe **OSI modelu**, na ktorej vrstve dané sieťové zariadenie pracuje. Nakoľko **smerovač** pracuje na **3. sieťovej vrstve**, **prepínač** používa **2. datovú/linkovú vrstvu** OSI modelu. **Prepínač** sa rozhoduje na základe **MAC adresy**, ktorú má uloženú **MAC tabuľke**. Každý neznámy **rámec** na základe **zdrojovej adresy** si spojí port s **príchodzím rámcom**. Na základe tejto asociácie pri odbalení **paketu kontroluje MAC adresu cieľového uzla** a pošle na **odchádzajúce rozhranie**. Smerovač pracuje podobne, ale s **IP adresami** a na základe **smerovacej tabuľky** sa posielajú na odchádzajúce rozhranie. **Kolíznu/Broadcastovú doménu**, na ktorej sa šíri **rámec** /paket limituje **prepínač/smerovač**. V prípade priamo pripojených sietí k rozhraniu, sú cesty pridávané automaticky do smerovacej tabuľky

s označením **C (connected)**. Avšak, čo ak chcú dosiahnuť siete, ktoré sú za broadcastovou doménou (obmedzenou smerovačmi alebo **VLAN**)? [1][2] [6]

Všeobecne zoberaté je možnosť použiť **statické** alebo **dynamické** smerovanie. V laboratórnej úlohe je použité **statické smerovanie**, ktorého nevýhodou je, že každá cesta musí byť nastavená manuálne. V prípade veľkých **zákazníckych sietí** je nemožné. Statické cesty sa najčastejšie používajú ako záložné cesty, príp. **smerovanie na dvojbodový spoj** medzi poskytovateľom Internetu. Statické cesty je možné kontrolovať v smerovacích tabuľkách *show ip route* s označením **S (static)**. Pri rozsiahlych sieťach je **žiaduce** si pokladať **otázky** typu: Ako sa **šíry premávka** sieťou v **oboch smeroch** ? Je špecifikované na smerovačoch, **ako sa má paket šíriť** pri **odpovede ICMP** pri pingu ? Pri prechode paketu smerovačom, je vždy **kontrolovaná smerovacia tabuľka**, pre kontrolu **adresy cieľového uzlu**. Ak v smerovacej tabuľke nie je daná sieť a nie je definovaná **predvolená cesta**, paket je zahodený.

Predvolená cesta je **špecifickým typom statickej cesty**, kde sú definované všetky siete pomocou **0.0.0.0 0.0.0.0** pre **IPv4** a **:::0** pre **IPv6**. Všeobecný syntax pre statickú cestu je :

```
R1(config)#ip route prefix mask address interface dhcp distance name next-hop-name permanent track
```

Pre účely, tohto kurzu si vystačíme s **červenými parametrami**, ktoré sú povinné údaje. Písma **kurzívou** sa doplnia podľa siete, **kde sa chcú dostať** (prefix mask address) a zadajú **odchádzajúce rozhranie** ako sa tam dostať prípadne, IP adresu **nasledujúceho skoku**. Využívanie len výstupného rozhrania v **statických cestách** bez uvedenia IP adresy nasledujúceho skoku sa odporúča len pre **point-to-point** linky. Keď sa to zhrnie, výhody **statického smerovania** sú bezpečnosť (neposiela smerovacie aktualizácie), nie je možné odchytiť dáta a rekonštruovať **topológiu** siete, nie je možné podstrčiť **chybné smerovacie informácie**), **predpovedateľnosť** (správca kontroluje smerovanie smerovača), **žiadne vymieňanie sieťových dát** (šetrí sa prenosová kapacita siete) a v neposlednej rade **žiadne zaťaženie** smerovača pri budovaní smerovacích tabuliek. Naopak ako **nevýhody** je možné uviesť slabá adaptabilita na zmeny v sieti a **vysoká náročnosť** na údržbu (správca musí všetko ručne nastaviť). Pre **multi-access** siete sa odporúča použiť **kombináciu výstupné rozhranie** a IP adresa nasledujúceho skoku. [4]

3.4 Požadované zdroje:

GNS3 a Wireshark

IOS smerovače – šablóna smerovača s **Ethernet** rozhraním [3]

3.5 Postup:

Topológia obsahuje 2 **smerovače c7200**, ktoré sú navzájom prepojené pomocou sériových rozhraní *S2/0* a *S2/1*. Sú **priradené adresy** z C podsiete *192.168.100/200.x/30* a aktivované porty príkazom *no shutdown*. Pre **konfigurovanie** sa používa konzola putty, ktorú si môžu zmeniť na obľúbený terminál (RemoteNG, SecureCRT apod). Pri **vysielaní** si špecifikuje MAC adresu pre R1 a R2.

V tejto úlohe preskúma možnosti **statického smerovania** pre *IPv4* a *IPv6*. Príkladom môže byť, že **sieťový špecialista** v spoločnosti AB&B, dostal žiadosť od zákazníka, ktorý má 2 určené linky prepojiť sieť v Bratislave so Zlínom. Ide o linky, ktoré sú **účtované** za každý prenesený bit, takže smerovacie protokoly neprichádzajú v úvahu. Preto je potrebné nastaviť statické a **predvolené IPv6 cesty**, aby sa urobila spoľahlivá a bezpečná cesta k zákazníkovi.

3.6 Ciele práce

Nasledujúce **ciele** boli navrhnuté vedúcim projektu v spoločnosti AB&B, po detailnej kontrole siete. Pôvodné nastavenie smerovačov pred vašimi zmenami obsahuje **čistý IOS** s licenciou. Pre **konfiguráciu IPv6** je potrebný *C7200-ADVIPSERVICESK9-M, 15.2(4)S5*.

Nasledujúca laboratórna úloha ukazuje ako nastaviť statické smerovanie pre *IPv4* a *IPv6*, prípadne ladenie nastavenia na úrovni **CCNA certifikácie**. Boli použité **sériové rozhrania**. **Väčšina testov** je ukazovaná na *IPv6*. Rozdiel je v porovnaní s *IPv4*, že je **pridaná** linková lokálna adresa. [1]

3.6.1 Nastavte všetky IPv4 a IPv6 adresy podľa topológie

V prípade nastavenia **časovania** na sériovom spoji by mal byť *clock rate len* na *DCE*. Ale je pridaný pod každý **sériový spoj** pre istotu. Po **nastavení** je vhodné si overiť základnú komunikáciu pomocou *pingu* suseda. Prípadne **overiť** poslednými príkazmi nastavené adresy a status linky:

Tab. 18: Prvotná konfigurácia IPv4 a IPv6 adres a povolenie IPv6 smerovania [autor]

```
!Bratislava:
conf term
hostname Bratislava
!
ipv6 unicast-routing
!
inter s2/0
ip add 192.168.100.1 255.255.255.252
mac-address 0001.6311.1111
ipv6 enable
ipv6 address 2001:DB8:FAC::1/130
no shut
!
inter s2/1
ip add 192.168.200.1 255.255.255.252
mac-address 0001.6322.1111
ipv6 enable
ipv6 address 2001:DB8:FAD::1/130
no shut
!
show ip inter brief
show IPv6 route
show IPv6 route
show IPv6 inter brief
!
!
!Zlin:
conf term
hostname Zlin
!
ipv6 unicast-routing
!
inter s2/0
ip add 192.168.100.2 255.255.255.252
mac-address 0001.6311.2222
ipv6 enable
ipv6 address 2001:DB8:FAC::2/130
no shut
!
inter s2/1
ip add 192.168.200.2 255.255.255.252
mac-address 0001.6322.2222
ipv6 enable
ipv6 address 2001:DB8:FAD::2/130
no shut
!
show ip inter brief
show IPv6 route
show IPv6 route
show IPv6 inter brief
```

3.6.2 Nastavte spätnoväzbovú slučku 0 pre Bratislavu testovanie dostupnosti zákazníckej siete IPv4 a IPv6

Dobrý zvykom pri **testovaní zariadení** v laboratórnej úlohe je vytvoriť si spätnoväzbovú slučku, čím je možné v budúcnosti si testovať inzerovanie sietí, blokovanie premávky:

Tab. 19: Konfigurácia IPv4 a IPv6 spätnoväzbových slučiek pre všetky rozhrania [autor]

```
!Bratislava:
inter Lo0
ip address 1.1.1.1 255.255.255.255
mac-address 0001.6300.1111
ipv6 enable
ipv6 address 2001:DB8:1::1/132
no shut
```

3.6.3 Nastavte spätnoväzbovú slučku pre Zlin testovanie dostupnosti zákazníckej siete IPv4 a IPv6

Dobrý zvykom pri **testovaní** zariadení v laboratórnej úlohe je vytvoriť si spätnoväzbovú slučku, čím je možné v budúcnosti si testovať inzerovanie sietí, blokovanie premávky:

Tab. 20: Konfigurácia IPv4 a IPv6 spätnoväzbových slučiek pre všetky rozhrania [autor]

```
!Zlin:
inter Lo0
ip address 2.2.2.2 255.255.255.255
mac-address 0001.6300.2222
ipv6 enable
ipv6 address 2001:DB8:2::1/32
no shut
```

```
Bratislava#show ip inter brie | section up
Serial2/0          192.168.100.1   YES manual up          up
Serial2/1          192.168.200.1   YES manual up          up
Loopback0         1.1.1.1         YES manual up          up
Bratislava#show ipv6 inter brie | section up
Serial2/0          [up/up]
FE80::C801:26FF:FEE0:8
2001:DB8:F::1
2001:DB8:FAC::1
Serial2/1          [up/up]
FE80::C801:26FF:FEE0:8
2001:DB8:FAD::1
Loopback0         [up/up]
FE80::C801:26FF:FEE0:8
2001:DB8:1::1
Zlin#show ip inter brie | section up
Serial2/0          192.168.100.2   YES manual up          up
Serial2/1          192.168.200.2   YES manual up          up
Loopback0         2.2.2.2         YES manual up          up
Zlin#show ipv6 inter brie | section up
Serial2/0          [up/up]
FE80::C802:26FF:FEF8:8
2001:DB8:FAC::2
Serial2/1          [up/up]
FE80::C802:26FF:FEF8:8
2001:DB8:FAD::2
Loopback0         [up/up]
FE80::C802:26FF:FEF8:8
2001:DB8:2::1
```

Obr. 37: Testovanie priradených IPv4 a IPv6 pre rozhrania [autor]

3.6.4 Bratislava: vytvorte statickú cestu ukazujúcu na spätnoväzbovú slučku 0 na strane Zlína, tak aby tok dát prechádzal cez sieť 192.168.100.0/30 pre protokol IPv4 a 2001:DB8:FAC::2/130 pre protokol IPv6

Ďalšie zadanie sa týka pridania **statickej cesty** ukazujúcej na *spätnoväzbovú slučku 0* na strane Zlína a zabezpečiť tak, aby tok dát prechádzal cez sieť 192.168.100.0/30 pre protokol IPv4 a 2001:DB8:FAC::2/130 pre protokol IPv6:

Tab. 21: Konfigurácia statického smerovania na spätnoväzbovú slučku 0 smerovača Zlín cez sieť 192.168.100.0/30 pre protokol IPv4 a 2001:DB8:FAC::2/130 pre protokol IPv6 [autor]

```
!Bratislava:
ip route 2.2.2.0 255.255.255.252 192.168.100.2
ipv6 route 2001:DB8:2::/64 2001:DB8:FAC::2
```

Po nastavení je možné opäť overovať výpisom **smerovacej tabuľky** pre statické cesty:

```
Bratislava#show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/30 is subnetted, 1 subnets
S       2.2.2.0 [1/0] via 192.168.100.2
Bratislava#show ipv6 route static
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
S   2001:DB8:2::/64 [1/0]
    via 2001:DB8:FAC::2
```

Obr. 38: Smerovacia tabuľka so statickou cestou cez 192.168.100.0/30 a 2001:DB8:FAC::/130 [autor]

3.6.5 Zlin: vytvorte predvolenú cestu ukazujúcu na spätnoväzbovú slučku 0 na strane Bratislavy, tak, aby tok dát prechádzal cez sieť 192.168.200.0/30 pre protokol IPv4 a 2001:DB8:FAD::/130 pre protokol IPv6. V smerovacej tabuľke by mal pribudnúť záznam 0.0.0.0.

Ďalšie zadanie sa týka pridania statickej cesty ukazujúcej na spätnoväzbovú slučku 0 na strane Zlina a zabezpečiť tak, aby tok dát prechádzal cez sieť 192.168.200.0/30 pre protokol IPv4 a 2001:DB8:FAD::/130 pre protokol IPv6:

Tab. 22: Konfigurácia statického smerovania na spätnoväzbovú slučku 0 smerovača Bratislava cez sieť 192.168.200.0/30 pre protokol IPv4 a 2001:DB8:FAD::2/130 pre protokol IPv6 [autor]

```
!Zlin:
ip route 0.0.0.0 0.0.0.0 192.168.200.1
ipv6 route ::/0 2001:DB8:FAD::1
```

Po nastavení je možné opäť overovať výpisom smerovacej tabuľky pre statické cesty:

```
Zlin#show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.200.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.200.1
Zlin#show ipv6 route static
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
S     ::/0 [1/0]
      via 2001:DB8:FAC::1
      via 2001:DB8:FAD::1
```

Obr. 38: Smerovacia tabuľka s predvolenou cestou cez 192.168.200.0/30 a 2001:DB8:FAD::/130 [autor]

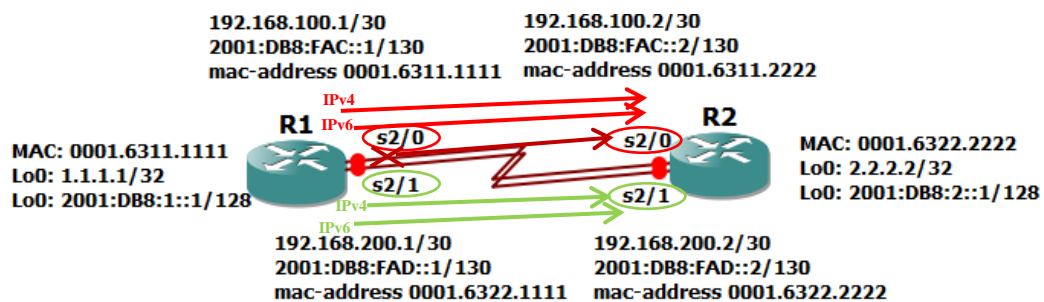
3.6.6 Bratislava: vytvorte záložnú statickú cestu ukazujúcu na spätnoväzbovú slučku 0 na strane Zlina s administratívnou vzdialenosťou 150, ktorá sa použije pri výpadku primárnej pre protokoly IPv4 a IPv6

Ďalšie zadanie sa týka pridania **záložnej statickej cesty** ukazujúcej na *spätnoväzbovú slučku 0* na strane Zlina a zabezpečiť tak, aby tok dát prechádzal cez záložnú linku v prípade výpadku *192.168.200.0/30* pre protokol *IPv4* a *2001:DB8:FAD::/130* pre protokol *IPv6*:

Tab. 23: Konfigurácia záložného smerovania na spätnoväzbovú slučku 0 smerovača Zlin cez sieť *192.168.200.0/30* pre protokol *IPv4* a *2001:DB8:FAD::2/130* pre protokol *IPv6* s administratívnou vzdialenosťou 150

```
!Bratislava:
ip route 2.2.2.0 255.255.255.252 192.168.200.2 150
ipv6 route 2001:DB8:2::/64 2001:DB8:FAD::2 150
!Logické zatvorenie sériového rozhrania Serial 0/0
inter Serial 0/0
shutdown
!no shutdown !znovuotvorenie portu a zavenie povôdných ciest 192.168.100.2 a 2001:DB8:FAC::2
```

Na Obr. 39 je vidieť **failover test**, v ktorom sa logicky zatvorí sériové rozhranie *Serial 2/0* a do smerovacej tabuľky sa zavedie novo pridaná záložná cesta s administratívnou vzdialenosťou 150. Po nastavení je možné opäť **overovať** výpisom smerovacej tabuľky



Obr. 39: Ilustrácia výpadku sériového rozhrania *Serial 2/0* a zavedenia záložnej cesty
[autor]

Nasledujúci Obr. 40 simuluje **testovanie** výpadku (logicky sa zatvorí sériové rozhranie *Serial 2/0*) a ukazuje možnosť kontroly zavedenia nových ciest do smerovacej tabuľky.

```

Bratislava#show ip route 2.2.2.2
Routing entry for 2.2.2.0/30
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
    * 192.168.100.2
      Route metric is 0, traffic share count is 1
Bratislava#show ipv6 route 2001:DB8:2::1
Routing entry for 2001:DB8:2::/64
  Known via "static", distance 1, metric 0
  Backup from "static [150]"
  Route count is 1/1, share count 0
  Routing paths:
    2001:DB8:FAC::2
      Last updated 01:45:31 ago

Bratislava#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Bratislava(config)#inter s2/0
Bratislava(config-if)#shutdown
Bratislava(config-if)#end
Bratislava#show ipv6 route 2001:DB8:2::1
*Mar 28 17:41:35.519: %SYS-5-CONFIG I: Configured from console by console
Bratislava#show ip route 2.2.2.2
*Mar 28 17:41:36.255: %LINK-5-CHANGED: Interface Serial2/0, changed state to administratively down
*Mar 28 17:41:37.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
Bratislava#show ip route 2.2.2.2
Routing entry for 2.2.2.0/30
  Known via "static", distance 150, metric 0
  Routing Descriptor Blocks:
    * 192.168.200.2
      Route metric is 0, traffic share count is 1
Bratislava#show ipv6 route 2001:DB8:2::1
Routing entry for 2001:DB8:2::/64
  Known via "static", distance 150, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2001:DB8:FAD::2
      Last updated 00:00:08 ago

```

Obr. 40: Failover testovanie a kontrola zavedenia nových ciest do smerovacej tabuľky [autor]

3.6.7 Zlín: Zmeň predvolenú cestu, tak aby bola v smerovacej ceste aj v prípade pádu rozhrania pre protokol IPv4

Ďalšie zadanie sa týka pridania predvolenej cesty ukazujúcej na spätnoväzbovú slučku 0 smerovača Bratislava a zabezpečiť tak, aby tok dát prechádzal cez sieť 192.168.100.0/30 pre protokol IPv4:

Tab. 24: Konfigurácia predvolenej cesty na spätnoväzbovú slučku 0 smerovača Bratislava cez sieť 192.168.100.0/30 pre protokol IPv4 [autor]

```

!Zlin:
ip route 0.0.0.0 0.0.0.0 192.168.100.1 permanent

```

Po nastavení je možné opäť overiť dané nastavenie zatvorením sériového rozhrania *Serial 2/0* a do **smerovacej tabuľky** sa zavedie novo pridaná záložná cesta s administratívnu vzdialenosť 150 len pre IPv6 a nasledujúci *Obr. 41* ponúka dôkaz nových statických ciest:

```

Zlin(config-if)#do show ip rou
*Mar 28 19:16:08.007: %LINK-5-CHANGED: Interface Serial2/0, changed state to adminis
tratively down
*Mar 28 19:16:09.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, cha
nged state to down
Zlin(config-if)#do show ip rou
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.200.1 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 192.168.200.1
      [1/0] via 192.168.100.1
      2.0.0.0/32 is subnetted, 1 subnets
C     2.2.2.2 is directly connected, Loopback0
      192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.200.0/30 is directly connected, Serial2/1
L     192.168.200.2/32 is directly connected, Serial2/1

Zlin(config-if)#do show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:
    * 192.168.200.1
      Route metric is 0, traffic share count is 1
      192.168.100.1, permanent
      Route metric is 0, traffic share count is 1
Zlin(config-if)#exi
Zlin(config)#no ip route 0.0.0.0 0.0.0.0 192.168.100.1 permanent
Zlin(config)#do show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:
    * 192.168.200.1
      Route metric is 0, traffic share count is 1





```

Obr. 41: Smerovacia tabuľka s predvolenou cestou cez 192.168.100.1 a 192.168.200.1 v prípade pádu rozhrania pre protokol IPv4 [autor]

V prípade testovania reálneho zaťaženia je vidieť pri zhodení linky, že sa stratí 4% paketov

Výsledné nastavenie smerovačov pre **konfigurácie** statickej cesty:

Tab. 25: Konfigurácia smerovačov R1 a R2 v Cisco IOS 15.2(4) S3 [autor]

R1	R2	Wireshark prim	Wireshark back
 R1.txt	 R2.txt	 s2-0.pcapng	 s2-1.pcapng

Pre konfiguráciu **rozhraní** virtuálnych liniek a nastavenie databázy užívateľov používame nasledujúce príkazy:

Tab. 26: Syntax aplikovaných príkazov pri konfigurácii DHCPv6 [autor]

	Syntax + Príkaz	Význam/Účel
Syntax príkazu:	router#show interfaces	Zobrazenie štatistík pre rozhrania na smerovači.
Syntax príkazu:	router (config)#ipv6 unicast-routing	Zasielanie IPv6 prenos z CEF na smerovači.
Syntax príkazu:	router (config)#ipv6 address IPv6 Address router(config-if)#ipv6 address 2001:DB8:CAFE:2::1/64	Nastavenie IPv6 adresy pre dané rozhranie s prefixom.
Syntax príkazu:	ip address IP Address router(config-if)# ip address 1.1.1.1 255.255.255.255	Nastavenie IPv4 adresy pre dané rozhranie.
Syntax príkazu:	Interface [type number] router(config)#interface Ethernet1/1	Vstup do konfiguračného rozhrania Ethernet1/1
Syntax príkazu:	switch# prefer dual-ipv4-and-ipv6 default	Aktivovanie šablóny pre koexistenciu IPv6 a IPv4
Syntax príkazu:	router#show ipv6 interface [brief] [type number] [prefix]	Zobrazenie stavu IPv6 pre rozhrania na smerovači
Syntax príkazu:	router(config-if)#ipv6 address autoconfig	Nastavenie SLAAC IPv6 adresy pre rozhranie.
Syntax príkazu:	ipv6 address ipv6 address router(config-if)# ipv6 address FE80::1 link-local	Nastavenie IPv6 linkovej adresy pre dané rozhranie.
Syntax príkazu:	ipv6 dhcp pool poolname router(config)# ipv6 dhcp pool cafe-test-luki	Vytvorenie mena DHCPv6 a vstup do konfig. režimu.
Syntax príkazu:	domain-name domain router(config-dhcpv6)# domain-name fai.utb.cz	Špecifikácia domény pre klienta
Syntax príkazu:	dns-server ipv6-address router(config-dhcpv6)# dns-server 2001:DB8:CAFE:2::DB01	Špecifikácia DNS servera pre klienta
Syntax príkazu:	ipv6 dhcp server [pool] rapid-commit router(config-if)#ipv6 dhcp server cafe-luki rapid-commit	Nastavenie rapid-commit procesu pre DHCPv6 server
Syntax príkazu:	router(config-if)#ipv6 dhcp client pd [pool] rapid-commit	Nastavenie rapid-commit procesu pre DHCPv6 klient
Syntax príkazu:	router(config-if)#ipv6 dhcp relay destination [prefix]	Nastavenie adresy DHCPv6 servera z relay agenta
Syntax príkazu:	router(config-if)# ipv6 nd other-config-flag	Nastavenie flagu pre stavový DHCPv6 RA správy

Syntax příkazu:	router(config-if)# ipv6 nd managed-config-flag	Nastavenie flagu pre stavový DHCPv6 RA správy
Syntax příkazu:	show ipv6 dhcp binding [ipv6-address] [vrf vrf-name] router# show ipv6 dhcp binding	Zobrazenie priradených IPv6 klientov DHCPv6 serv.
Syntax příkazu:	show ipv6 dhcp interface [type number] router# show ipv6 dhcp interface Eth1/0	Zobrazenie informácií rozhrania pre DHCPv6
Syntax příkazu:	show ipv6 interface [brief] [type number] [prefix] router# show ipv6 interface Eth1/0	Zobrazenie stavov rozhraní a ipv6 adres
Syntax příkazu:	router# show ipv6 dhcp pool	Zobrazenie nastavenia DHCP poolu IPv6 adres
Syntax příkazu:	router#debug ipv6 dhcp	Zobrazí hlavné informácie z ladenia pre DHCPv6.
Syntax příkazu:	router#debug ipv6 dhcp detail	Zobrazí detail. informácie z ladenia pre DHCPv6.
Syntax příkazu:	router#debug ipv6 dhcp database	Zobrazí ladenie informácie z databáze pre DHCPv6.
Syntax příkazu:	undebug all	Vypnutie všetkých ladenie oznámení na terminály.
Syntax příkazu:	show ip/ipv6 interface brief R1/R2# show ip/ ipv6 interface brief	Zobrazenie IP/IPv6 infor. pre dané rozhrania
Syntax příkazu:	show ip/ ipv6 route R1/R2# show ip/ ipv6 route	Zobrazenie smerovacej tabuľky pre IPv4 a IPv6.
Syntax příkazu:	ip route prefix mask {ip-address interface-type interface-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent track number] [tag tag] router#ip route 2.2.2.0 255.255.255.252 192.168.100.2	Nastavenie statickej cesty pre IPv4 a všetky možnosti
Syntax příkazu:	ipv6 route ipv6-prefix / prefix-length ipv6-address interface-type interface-number ipv6-address}} [administrative-distance] router#ipv6 route 2001:DB8:2::/64 2001:DB8:FAC::2	Nastavenie statickej cesty pre IPv6 a všetky možnosti
Syntax příkazu:	ip route prefix mask {ip-address interface-type interface-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent track number] [tag tag] router#ip route 0.0.0.0 0.0.0.0 192.168.100.1 permanent	Nastavenie predvolenej statickej cesty pre IPv4
Syntax příkazu:	ipv6 route ipv6-prefix / prefix-length ipv6-address interface-type interface-number ipv6-address}} [administrative-distance] router#ipv6 route ::/0 2001:DB8:FAD::1	Nastavenie predvolenej statickej cesty pre IPv6
Syntax příkazu:	ipconfig [/allcompartments] [/all] [/renew] [/release] PC>ipconfig	Zobrazenie nastavenia sieťového adaptéru
Syntax příkazu:	PC>tracert / R#tracert R1# traceroute 10.1.1.2	Zobrazenie cesty k cieľovej IP a dosiahnutý uzlom v
Syntax příkazu:	netstat [-a] [-e] [-n] [-o] [-r] [-s] [-p<Protocol>] R2(dhcp-config)# domain-name fai.utb.cz	Zobrazenie aktívneho sieťového spojenia a tabulu
Syntax příkazu:	ping [-t] [-a] [-n count] [-l size] [-f] [-r count] [-R] R2# ping 10.1.1.2	Overenie odozvy protistrany (ICMP)
Syntax příkazu:	copy running-config startup-config /write memory R2 (config-if)# # copy running-config startup-config	Uloženie aktuálneho nastavenia do NVRAM.

ZOZNAM POUŽITÉJ LITERTÚRY

- [1] LAMMLE, Todd. *CCNA: výukový průvodce*. 1. vydání. Překlad Jakub Goner. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
- [2] Cisco Networking Academy Course Catalog, [Online]. [cit. 2015-10-28].
Dostupné z :
www.cisco.com/web/learning/netacad/course_catalog/CCNAexploration.html.
- [3] *GNS3 / Graphical Network Simulator*. [Online]. [cit. 2015-10-28]. Dostupné z:
www.gns3.net.
- [4] ODOM, Wendell. *Cisco CCENT/CCNA ICND1 100-101 official cert guide, academic edition*. Academic edition. Indianapolis, IN: Cisco Press, 2013. ISBN 1587144859.
- [5] ODOM, Wendell. *Cisco CCNA routing and switching ICND2 200-101 official cert guide*. Indianapolis, Indiana: Cisco Press, 2013. ISBN 1587143739.
- [6] HUCABY, Dave. *CCNP routing and switching SWITCH 300-115 official cert guide*. Indianapolis, IN: Cisco press, 2015. ISBN 978-1-58720-560-6.
- [7] URBANČOK, Lukáš. *Technologie IPv6, její bezpečnost a simulace sítí s využitím GNS3*. Zlín, 2016. Diplomová práce. Fakulta aplikované informatiky - Univerzita Tomáše Bati ve Zlíně. Katedra počítačových a komunikačních systémů. Vedoucí kvalifikační práce Ing. Jiří Korbel, Ph.D.
- [8] SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AAA	Authentication, Authorization, and Accounting
ACL	Access-list = kontrolný zoznam = filter
C	Priamo pripojená cesta - Connected
CCNA	Cisco Certified Network Associate
CDP	Cisco Discovery Protocol- zhromažďovanie info o lokálne zariadení
CLI	command-line interface = rohranie príkazového riadku
DAD	detekcia duplicity adres (Duplicate Address Detection)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System – preklad názvov host'ov
E1/0	Ethernet 1/0
EXEC	Mód nad konfiguráciou, rozlišujúci práva USER-, PRIVILEGED-
GNS3	Graphical Network Simulator 3
ICMP	Internet Control Message Protocol – poskytovateľ služieb zpráv IP
IOS	Internetwork Operating System
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
Lo1	Spätnoväzbová slučka 1 (Loopback1)
MAC	L2 adresa, ktorá jednoznačne identifikuje fyzické pripojenie hostiteľa
multiaccess	Viacprístupový
NA	Neighbor advertisement
NDP	Neighbor Discovery Protocol
NS	Neighbor solicitation
NVRAM	Nonvolatile RAM – obsahuje platný startup-config používaný pri restate
OS	Operating System - operačný systém
OSI	Open Systems Interconnection- Cisco model 7 hierarchických vrstiev
payload	zaťaženie – samotné dáta v paketoch
R/S	Routing and Switching
RA	Router advertisement
RADIUS	Remote Authentication Dial-in User Service – server pre AAA
RS	Router solicitation
RSA	Rivest-Shamir-Adleman – šifrovací systém pre verejné kľúče
run-config	bežiacia konfigurácia
S	Statická cesta - Static
S2/1	Serial 2/1
SNMP	Simple Network Management Protocol – protokol pre správu siete
SSH	Secure Shell – zabezpečená relácia nad štandardným pripojením TCP/IP
TACACS+	Terminal Access Controller Access-Control System + protokol pre AAA
TTL	Time to Live – zamedzenie neobmedzenej životnosti paketov
UDP	User Datagram Protocol

VLAN	Virtuálna LAN - doména všesmerového vysielania
VPCS	Virtual PC Simulator
VTY	virtuálna linka pre správu/vzdialený prístup

ZOZNAM OBRÁZKOV

<i>Obr. 1: Ukážka jednoduchej a zložitejšej topológie a príklad IPv6 adresácie [autor].....</i>	<i>2</i>
<i>Obr. 2: Príklad pridelovania IPv6 adries a ukážka statickej alokácie v software GNS3 [7]</i>	<i>3</i>
<i>Obr. 3: Generovanie IPv6 adresy pre virtuálne PC1 [autor]</i>	<i>5</i>
<i>Obr. 4: Zobrazenie IPv6 adresy pre virtuálne PC2 a PC3 (vpcs dynamips) [autor].....</i>	<i>5</i>
<i>Obr. 5: Potvrdenie natvrdo priradenej IPv6 adresy pre rozhrania smerovačov R1a R2 [autor].....</i>	<i>5</i>
<i>Obr. 6: Testovanie dostupnosti susedného rozhrania smerovača R2 [autor].....</i>	<i>6</i>
<i>Obr. 7: Testovanie dostupnosti virtuálnej stanice PC2 zo smerovača R1 [autor].....</i>	<i>6</i>
<i>Obr. 8: Ukážka NDP protokolu z odchytených paketov medzi PC1 a R1 [autor]</i>	<i>7</i>
<i>Obr. 9: Ukážka paketu RS a RA pri hľadaní smerovača z PC1 [autor].....</i>	<i>8</i>
<i>Obr. 10: ICMPv6 informácie v správe RA od smerovača R1 [autor]</i>	<i>9</i>
<i>Obr. 11: Topológia pre test DHCPv4, IPv6 stavový a bezstavový DHCPv6 [autor]</i>	<i>11</i>
<i>Obr. 12: Proces pridelovania IP adries pomocou DHCP serveru [5][6]</i>	<i>12</i>
<i>Obr. 13: Objavovanie linkových adries susedov a duplicity [2][5]</i>	<i>13</i>
<i>Obr. 14: Štyri správy stavovej DHCPv6 medzi klientom a serverom [1][6]</i>	<i>14</i>
<i>Obr. 15: Zobrazenie nastavenia DHCP poolu IPv4 adries na smerovači R2 [autor]</i>	<i>17</i>
<i>Obr. 16: Zobrazenie štatistik DHCP poolu IPv4 adries [autor]</i>	<i>18</i>
<i>Obr. 17: Zobrazenie predvolenej brány (gateway) v smerovacej tabuľke [autor].....</i>	<i>18</i>
<i>Obr. 18: Ukážka zachyteného DHCP offer paketu s L2 a L3 broadcastu [autor]</i>	<i>19</i>
<i>Obr. 19: Zobrazenie bootp flagu a detail ACKNOWLEDGEMENT od servera [autor]</i>	<i>20</i>
<i>Obr. 20: Priradenie IPv4 adresy pre virtaul PC pomocou Unicast možnosti pre DHCP [autor]</i>	<i>21</i>
<i>Obr. 21: Kontrola priradených unicast IPv4 adries pomocou show ip dhcp binding [autor]</i>	<i>21</i>
<i>Obr. 22: Príklad dizajnu všetkých možností IPv6 adresácie s konfiguráciou na smerovači [autor]</i>	<i>23</i>
<i>Obr. 23: Nastavenie protokolu IPv6 (TCP/ICPv6) v operačnom systéme Windows [autor]</i>	<i>24</i>
<i>Obr. 24: Filtrovanie multicast pre všetky uzly na linke FF02::1 [autor]</i>	<i>24</i>
<i>Obr. 25: Nastavená IPv6 adresa pomocou SLAAC pomocou VPC [autor]</i>	<i>25</i>

<i>Obr. 26: RA správa, ktorá bola zachytená; flag ICMPv6 rozlišuje typ DHCPv6 [autor]</i>	<i>25</i>
<i>Obr. 27: Overenie poskytnutej IPv6 unicast adresy pomocou SLAAC [autor].....</i>	<i>26</i>
<i>Obr. 28: Ladenie bezstavového DHCPv6 na R4 po zatvorení a otvorení rozhrania Eth1/0 [autor].....</i>	<i>27</i>
<i>Obr. 29: Zachytené RA správy vo FLAG nastavení je nastavený Other configuration [autor]</i>	<i>28</i>
<i>Obr. 30: Povolenie používania ladenia pri spustení DHCPv6 [autor]</i>	<i>29</i>
<i>Obr. 31: Povolenie používania DHCPv6 pre získanie smerovateľných adries [autor]</i>	<i>30</i>
<i>Obr. 32: Ladenie správ pri stavovej DHCPv6 medzi klientom a serverom vid' Obr. 14.....</i>	<i>30</i>
<i>Obr. 33: Ladenie skráteného DHCPv6 rapid-commit procesu [autor]</i>	<i>32</i>
<i>Obr. 34: Odchytené pakety s DUID (id klient a server DHCPv6) [autor]</i>	<i>32</i>
<i>Obr. 35: Kontrola DHCPv6 na strane klienta so špecifickým DUID [autor].....</i>	<i>33</i>
<i>Obr. 36: GNS3 topológia z laboratórnej úlohy Ethernet pre overenie funkčnosti statického smerovania [autor]</i>	<i>35</i>
<i>Obr. 37: Testovanie priradených IPv4 a IPv6 pre rozhrania [autor]</i>	<i>39</i>
<i>Obr. 38: Smerovacia tabuľka so statickou cestou cez 192.168.100.0/30 a 2001:DB8:FAC::/130 [autor]</i>	<i>40</i>
<i>Obr. 39: Ilustrácia výpadku sériového rozhrania Serial 2/0 a zavedenia záložnej cesty [autor]</i>	<i>42</i>
<i>Obr. 40: Failover testovanie a kontrola zavedenia nových ciest do smerovacej tabuľky [autor]</i>	<i>43</i>
<i>Obr. 41: Smerovacia tabuľka s predvolenou cestou cez 192.168.100.1 a 192.168.200..1 v prípade pádu rozhrania pre protokol IPv4 [autor].....</i>	<i>44</i>
<i>Obr. 42: Testovanie výpadku rozhrania S2/0 a zavedenia záložnej IPv6 cesty pri zaťažení [autor]</i>	<i>45</i>
<i>Obr. 43: Testovanie výpadku rozhrania S2/0 a zavedenia záložnej IPv6 cesty pri zaťažení [autor]</i>	<i>45</i>

ZOZNAM TABULIEK

<i>Tab. 1: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]</i>	<i>4</i>
<i>Tab. 2: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]</i>	<i>9</i>
<i>Tab. 3: Syntax aplikovaných príkazov a vysvetlenie významu pri konfigurácii DHCPv4 [autor].....</i>	<i>16</i>
<i>Tab. 4: Laboratórna úloha DHCP súkromná kancelária- Posledná zmena:2/18/2016 [autor]</i>	<i>17</i>
<i>Tab. 5: Show príkazy overujúce DHCP nastavenie a DHCPv4 konfigurácie [autor]</i>	<i>22</i>
<i>Tab. 6: Vytvorenie sumarizácie ciest na sériovom rozhraní S0/0 na smerovači MARS [autor]</i>	<i>22</i>
<i>Tab. 7: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]</i>	<i>22</i>
<i>Tab. 8: Nastavenie SLAAC na SW1 a zobrazenie nastavenia PC1 [autor]</i>	<i>24</i>
<i>Tab. 9: Nastavenie bezstavového DHCPv6 na R3 a R4 a zobrazenie nastavenia DHCPv6 [autor].....</i>	<i>26</i>
<i>Tab. 10: Nastavenie ladenie bezstavového DHCPv6 na R3 a R4 [autor].....</i>	<i>27</i>
<i>Tab. 11: Overenie nastavenia bezstavového DHCPv6, kde sa neukladá stav IPv6 adres [autor]</i>	<i>28</i>
<i>Tab. 12: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]</i>	<i>29</i>
<i>Tab. 13: Nastavenie DHCPv6 na R1a R2 [autor]</i>	<i>31</i>
<i>Tab. 14: Konfigurácia smerovačov R1, R2 a R5 v Cisco IOS 15.2(4) S3 [autor].....</i>	<i>33</i>
<i>Tab. 15: Nastavenie koexistencie IPv4 a IPv6 protokolu [autor]</i>	<i>34</i>
<i>Tab. 16: Nastavenie SLAAC IPv6 adresy pre rozhranie [autor]</i>	<i>34</i>
<i>Tab. 17: Nastavenie rapid-commit procesu v stavovom DHCPv6 [autor]</i>	<i>34</i>
<i>Tab. 18: Prvotná konfigurácia IPv4 a IPv6 adres a povolenie IPv6 smerovania [autor]</i>	<i>38</i>
<i>Tab. 19: Konfigurácia IPv4 a IPv6 spätnoväzbových slučiek pre všetky rozhrania [autor]</i>	<i>39</i>
<i>Tab. 20: Konfigurácia IPv4 a IPv6 spätnoväzbových slučiek pre všetky rozhrania [autor]</i>	<i>39</i>
<i>Tab. 21: Konfigurácia statického smerovania na spätnoväzbovú slučku 0 smerovača Zlin cez sieť 192.168.100.0/30 pre protokol IPv4 a 2001:DB8:FAC::2/130 pre protokol IPv6 [autor]</i>	<i>40</i>

<i>Tab. 22: Konfigurácia statického smerovania na spätnoväzbovú slučku 0 smerovača Bratislava cez sieť 192.168.200.0/30 pre protokol IPv4 a 2001:DB8:FAD::2/130 pre protokol IPv6 [autor]</i>	<i>41</i>
<i>Tab. 23: Konfigurácia záložného smerovania na spätnoväzbovú slučku 0 smerovača Zlin cez sieť 192.168.200.0/30 pre protokol IPv4 a 2001:DB8:FAD::2/130 pre protokol IPv6 s administratívnou vzdialenosťou 150.....</i>	<i>42</i>
<i>Tab. 24: Konfigurácia predvolenej cesty na spätnoväzbovú slučku 0 smerovača Bratislava cez sieť 192.168.100.0/30 pre protokol IPv4 [autor]</i>	<i>43</i>
<i>Tab. 25: Konfigurácia smerovačov R1 a R2 v Cisco IOS 15.2(4) S3 [autor]</i>	<i>46</i>
<i>Tab. 26: Syntax aplikovaných príkazov pri konfigurácii DHCPv6 [autor]</i>	<i>46</i>