UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Sbírka řešených úloh na konfiguraci IPv6

Richard Matula

Bakalářská práce
2014

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Richard Matula**
Osobní číslo:	**I11128**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Sbírka řešených úloh na konfiguraci IPv6**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je podrobně představit principy protokolu IPv6 a navrhnout minimálně 6 řešených úloh na konfiguraci směrované sítě s protokolem IPv6. Práce bude obsahovat sadu podrobně řešených a vysvětlených úloh na směrování protokolu IPv6 s využitím statického a dynamického směrování.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

MCFARLAND, Shannon, Rus HEALY a Naren MEHTA. IPv6: kompletní průvodce nasazením v podnikových sítích. Vyd. 1. Brno: Computer Press, 2011, 368 s. Samostudium. ISBN 978-80-251-3684-3.
ODOM, Wendell, Rus HEALY a Naren MEHTA. Směrování a přepínání sítí: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009, 879 s. Samostudium. ISBN 978-80-251-2520-5.
LOSHIN, Pete, Rus HEALY a Naren MEHTA. IPv6 theory, protocol, and practice: autorizovaný výukový průvodce. 2nd ed. San Francisco: Morgan Kaufmann, 2004, xxiv, 536 s. Samostudium. ISBN 15-586-0810-9.

Vedoucí bakalářské práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

Datum zadání bakalářské práce: **20. prosince 2013**
Termín odevzdání bakalářské práce: **9. května 2014**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2014

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 9. 5. 2014 Richard Matula

Poděkování

Na tomto místě bych chtěl v prvé řadě poděkovat panu Mgr. Josefu Horálkovi, Ph. D. za ochotu a cenné rady při tvorbě této práce. Dále bych chtěl poděkovat své rodině a přítelkyni za podporu při mých studiích a za pomoc při zpracování tohoto díla.

Anotace

Cílem práce je podrobně představit principy protokolu IPv6 a navrhnout minimálně 6 řešených úloh na konfiguraci směrované sítě s protokolem IPv6. Práce bude obsahovat sadu podrobně řešených a vysvětlených úloh na směrování protokolu IPv6 s využitím statického a dynamického směrování.

Klíčová slova

IPv6, směrování, konfigurace, Internet Protocol

Title

Collection of solved problems on the configuration of IPv6.

Annotation

The aim of the thesis is to present the principles of IPv6 protocol and to propose at least 6 solved tasks to configuration of a routed network with IPv6. The thesis will include a set of detailed solved and explained tasks on the routing protocol IPv6 using static and dynamic routing.

Keywords

IPv6, routing, configuration, Internet Protocol

Obsah

Seznam zkratek

ARPANET	Advanced Research Projects Agency Network
BGP	Border Gateway Protocol
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EUI	Extended Unique Identifier
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
IGP	Interior Gateway Protocol
IPv4	Internet Protocol verze 4
IPv6	Internet Protocol verze 6
ISP	Internet Service Provider
ISO/OSI	International Standards Organization / Open System Interconnection
NAT	Network Address Translation
NAT-PT	Network Address Translation – Protocol Translation
OSPF	Open Shortest Path First
RAM	Random Access Memory
RFC	Request for Comments
RIP	Routing Information Protocol
SLAAC	Stateless Address Autoconfiguration
QoS	Quality of Service
VLSM	Variable-Length Subnet Mask

Seznam obrázků

Seznam tabulek

Rešerše

IPv6. Protokol, o kterém bylo od už začátku pokládáno mnoho spekulativních otázek, je momentálně čím dál více rozebírané téma v oboru počítačových sítí. Hodně odborníků, ale i amatérů s tímto zájmem, se začalo touto problematikou zabývat a vyšel nesporně velký počet literatury a článků. Z řad českých spisovatelů mě zaujala kniha IPv6 od autora Pavla Satrapy a dále, už ale cizojazyčné knihy, Understanding IPv6 a IPv6 Theory, Protocol and Practise. Hodně informací se dalo také čerpat z dokumentů RFC.

Z těchto pramenů se mi také podařilo získat velké množství informací z článků na internetu. Například na stránkách ipv6.cz, v internetových magazínech lupa.cz a abclinuxu.cz v rubrice Sítě. Webová stránka test-ipv6.com představuje pohodlný způsob, jak zjistit, zda je zařízení schopno pracovat s IPv6, nebo v jaké míře.

Také jsem měl možnost nahlédnout do bakalářských a diplomových prací mých starších kolegů pod vedením mého vedoucího práce pana doktora Horálka, dále pana inženýra Drvoty z dopravní fakulty a pana inženýra Horáka z fakulty ekonomicko-správní.

Bakalářskou práci na toto téma jsem se rozhodl psát z toho důvodu, že mě problematika počítačových sítí zajímá a chtěl jsem se dozvědět něco více o protokolu IPv6. Tato práce se tedy nebude zabývat pouhým popisem protokolu a metod směrování, nýbrž i praktickou ukázkou na toto téma doloženou v příloze tohoto dokumentu. Dalo by se říci, že je práce určená pro odborníky, ale např. také pro laiky, kteří se o tomto tématu chtějí něco dozvědět nebo rozšířit své znalosti.

Úvod

V době, kdy ARPANET položil základy Internetu, se nevědělo, jaký bude nárůst uživatelů za pár let, a že velký rozmach této sítě bude znamenat problémy pro mnohé organizace zabývající se Internetovými standardy s řešením nedostatku adres. Bohužel tento nedostatek pro síť původně vymyšlenou pro experimentální účely nastal.

To sice bylo možné dočasně vyřešit mechanismy CIDR a NAT, ale definitivním řešením bylo nasazení protokolu IPv6. Tento protokol položil základní kámen pro nový typ datové komunikace. Cesta k tomuto řešení ale nebyla jednoduchá kvůli vzájemné nekompatibilitě protokolu s jeho předchůdcem.

Internet Protocol verze 6, neboli podle původního názvu IPng (IP next-generation), je, jak již název napovídá, Internetový protokol nové generace, který má oproti svému předchůdci IPv4 spoustu výhod. Je to nastupující protokol a důvodů k jeho zavedení je spousta, včetně výše uvedeného nedostatku adresního prostoru.

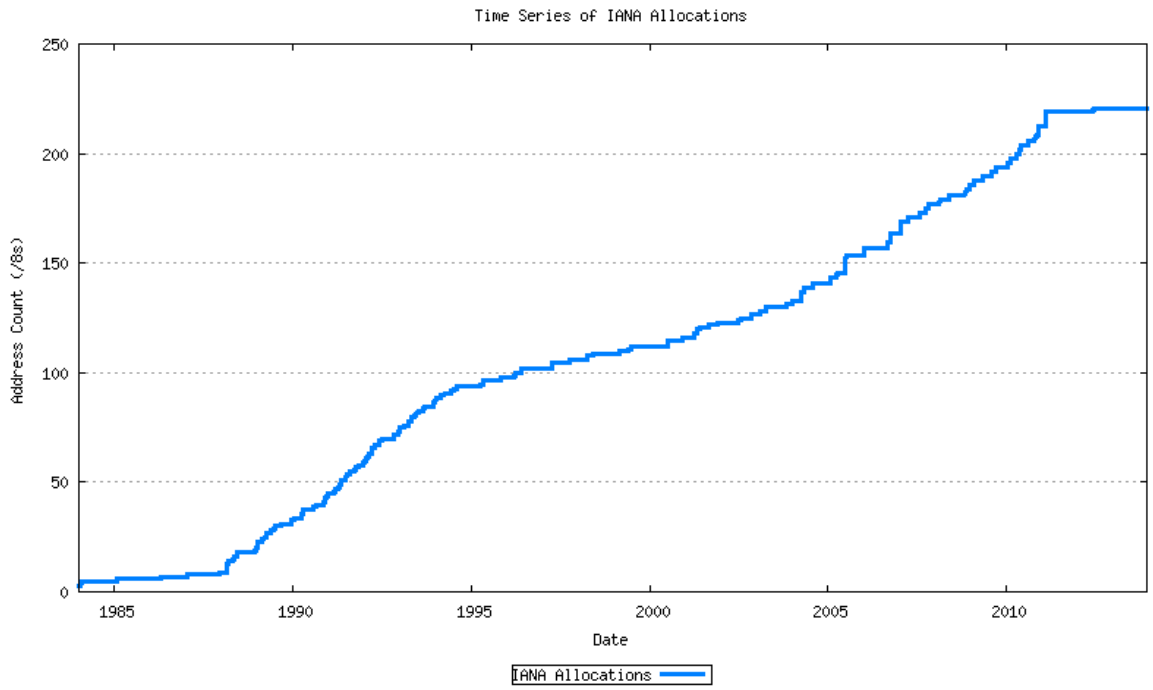
Bakalářská práce je rozdělena do dvou částí. První část se zabývá protokolem IPv6 po teoretické stránce, zatímco druhá po praktické – návrh šesti řešených úloh na směrování s podporou IPv6.

První kapitola se zabývá bližším popisem protokolu – specifické zápisy adres pro protokol IPv6, typy adres, hlavička paketu a konfigurací protokolu. Druhá kapitola poukazuje na jeden nedostatek protokolu IPv6, a to zpětnou kompatibilitu s IPv4, která musí být řešena přechodovými mechanismy. Třetí a čtvrtá kapitola už přibližuje čtenáři záměr této práce, a to směrovací algoritmy a druhy směrování v tomto protokolu. Pátá kapitola nabízí samotný návrh řešení úloh na směrování. Poslední kapitola se snaží shrnout výše uvedené kapitoly a uzavřít tak tuto bakalářskou práci.

1 Popis protokolu

Tak jako každý automobil musí mít unikátní SPZ značku, musí mít i každý počítač v síti jednoznačnou IP adresu. Tento fakt samozřejmě u Internetu neplatí pro technologii překladu adres (NAT) protokolu IPv4, ale u adres typu IPv6 tomu tak je – kvůli jeho již dostačujícímu rozsahu. Adresy jsou stejně jako u IPv4 přiřazovány síťovým rozhraním – to znamená, že počítač může komunikovat prostřednictvím různých IP adres.

IPv6 vznikl na počátku 90. let 20. století a jeden z důvodů jeho vzniku bylo nastávající vyčerpání adres IPv4. U jeho vzniku stáli především pánové Steven Deering a Robert Hinden, kteří vydali v roce 1995 dokument RFC 1883 (Hinden a Deering, 1995). Protokol pracuje na 3. (síťové) vrstvě ISO/OSI modelu a jeho specifikace je detailně popsána v RFC 2460 (Hinden a Deering, 1998) a adresovací architektura v RFC 4291 (Hinden a Deering, 2006). „Podle RFC 6540 (George et al., 2012) je jeho podpora povinná ve všech implementacích IP, a to v kvalitě přinejmenším srovnatelné s IPv4.“ (Satrapa, 2012) Struktura hlavičky a adresy protokolu byly přepracovány a mnohá funkcionalita, která byla u IPv4 jen doplňkem, je již v IPv6 standardem. Vzhledem k tomu, že IPv6 adresa zabírá 128b (IPv4 pouze 32b), nabízí větší adresní prostor – konkrétně $3{,}4*10^{38}$ adres. Podle Satrapy (2011, s. 21) je to číslo natolik dostačující, že každý počítač, hodinky, lednička či další zařízení bude mít svou vlastní, celosvětově jednoznačnou IP adresu.



Obrázek 1 – Spotřeba IPv4 adres [převzato z http://www.potaroo.net/tools/ipv4/]

Důvod vzniku nebyl jenom nedostatek adresního prostoru, ale zejména tyto následující požadavky: (Satrapa, 2011, s. 17)

- rozsáhlý adresní prostor, který vystačí pokud možno navždy,
- tři druhy adres: individuální (unicast), skupinové (multicast) a výběrové (anycast),
- jednotné adresní schéma pro Internet i vnitřní sítě,
- hierarchické směrování v souladu s hierarchickou adresací,
- zvýšení bezpečnosti (zahrnout do IPv6 mechanismy pro šifrování, autentizaci a sledování cesty k odesílateli),
- podpora služby se zajištěnou kvalitou,
- optimalizace pro vysokorychlostní směrování,
- automatická konfigurace (pokud možno plug and play),
- podpora mobility (přenosné počítače apod.),
- hladký a plynulý přechod z IPv4 do IPv6.

1.1 Zápis adresy a prefixu v IPv6

IPv6 adresa zabírá oproti svému předchůdci 4x větší prostor, a to má za následek také větší (delší) adresu a její specifický zápis. Zápis adresy podléhá pravidlům dokumentu RFC 4291 (Hinden a Deering, 2006). Adresa obsahuje místo původních 4 skupin číslic 8 bloků, které jsou odděleny dvojtečkami. Hlavní rozdíl oproti IPv4 je ten, že IPv6 adresa je zapsána v šestnáctkové, tedy hexadecimální soustavě, nikoli v soustavě desítkové. Příklad IPv6 adresy:

2001:0073:1d21:0016:02dc:22ff:fec9:0cc6/64

Prefix

Číslo v adrese uvedené za lomítkem udává tzv. délku prefixu, což označuje adresu sítě. Tento fakt tedy intuitivně značí počet bitů adresy (zleva), které do prefixu patří. Každý typ adresy má svůj prefix, podle kterého je její druh lehce identifikovatelný. Tento způsob zápisu je převzat z mechanismu CIDR protokolu IPv4. Detailnější popis přidělení prefixů je popsán v kapitole 1.2.4 Globální individuální adresy.

Zkracování adres

Pokud adresa obsahuje nuly na specifické pozici, pak je některé možno vynechat. Například úvodní nuly v každé skupině:

2001:73:1d21:16:2dc:22ff:fec9:cc6

Pokud jsou v bloku 4 nuly, lze tyto nuly taktéž vynechat – nahradit znakem „::“ (čtyřtečka):

2001:0073:0000:0000:0000:2dfe:ff02:ce12

2001:73::2dfe:ff02:cd12

Ovšem při zápisu typu:

2001:0:0:0:ff12:0:0:cd12

lze tyto nuly vynechat pouze jednou – kvůli jednoznačnosti zápisu:

2001::ff12:0:0:cd12 nebo 2001:0:0:0:ff12::cd12,

nikoli však 2001::ff12::cd12.

Jelikož je kombinací zápisu IPv6 adres spousta, například záměna malých a velkých písmen nebo vynechávání nul, byla v RFC 5952 (Kawamura a Kawashima, 2010) definována pravidla, podle kterých by měla všechna zařízení na výstupu dostat adresu ve stejném formátu. Zařízení by tedy měla podporovat všechny vstupní formáty, ale jako výstup pouze formát podle této normy (tj. v kanonickém tvaru). (Satrapa, 2011, s. 56–58; 2008a; Lammle, 2010, s. 722–723)

1.2 Typy adres

Jak již bylo uvedeno výše, protokol IPv6 vylepšuje protokol IPv4. Proto nabízí kromě jednosměrových a vícesměrových adres také adresy výběrové, avšak adresy všesměrové (broadcast) byly vyloučeny a nahrazeny adresami skupinovými. Základní typy adres v IPv6 jsou:

- individuální (unicast),
- skupinové (multicast),
- výběrové (anycast).

1.2.1 Individuální (unicast)

Adresy tohoto typu jsou doručeny pouze jednomu rozhraní, například komunikace klienta se serverem, nebo spoj klient - klient.

1.2.2 Skupinové (multicast)

Tyto adresy slouží pro adresování skupin počítačů či zařízení. Pro tento druh adres je vyhrazena formátovací předpona (skupina nejvyšších bitů adresy) na hodnotu FF. Při odeslání dat na tuto adresu musí být odeslána na všechna zařízení v této skupině. Proto se v některých literaturách také označují jako adresy typu 1:N.

1.2.3 Výběrové (anycast)

Výběrové adresy pracují na stejném principu jako adresy skupinové, jen s tím rozdílem, že se požadavku na zpracování paketu ujme zpravidla nejbližší síťové rozhraní.

1.2.4 Globální individuální

Ovšem tu největší část adres tvoří tzv. **globální individuální adresy**. Je to typ adres podobný IPv4 a nejdůležitějším faktem je, že tyto adresy jsou celosvětově unikátní. S tímto druhem adres se uživatel setká nejčastěji. Tyto adresy jsou zatím určeny prefixem 2000::/3. V RFC 3587 (Hinden, Deering a Nordmark, 2003) jsou definovány takto:

- první 3 bity – pevný prefix 001,
- dalších 45 bitů – globální směrovací prefix,
- dalších 16 bitů – číslo podsítě,
- posledních 64 bitů – identifikátor rozhraní.

Veškerý adresní prostor má na starosti organizace IANA, která dohlíží na přidělování IP adres. Globální směrovací prefix určuje koncovou síť a je určen ISP a kontinentálním registrátorem. Tyto prefixy jsou přidělovány tak, aby byla zajištěna agregace směrování a zmenšení velikosti směrovacích tabulek. ISP dále přidělí prefixy dlouhé /48 koncovým zákazníkům a ti už si posledních 64 bitů rozdělí pro vlastní potřeby.

1.2.5 Lokální

Dalším neméně důležitým typem jsou **lokální adresy.** Tak jako má protokol IPv4 k dispozici privátní adresy, má IPv6 výše zmíněné adresy lokální. Tyto adresy už nejsou celosvětově jedinečné, to znamená, že jsou přidělovány na úrovni LAN sítí. V některých literaturách se lze setkat s termínem adresy s omezeným dosahem.

Lokální linkové

Tyto adresy začínají prefixem fe80::/10 a jsou jedinečné v rámci jednoho ethernetového segmentu. Skládají se z prefixu a 64bitového identifikátoru rozhraní (EUI-64). Používají se ke sdílení dat po místní síti a u automatické konfigurace.

Lokální místní

Dalším, dnes již zamítnutým druhem adres, jsou adresy lokální místní. Tento typ představoval jakési „IPv4 privátní adresy“ v IPv6. Tyto adresy lze poznat podle prefixu fec0::/10, avšak byly kvůli jejich komplikovanosti normou RFC 3879 (Huitema a Carpenter, 2004) zavrženy.

Unikátní lokální

Nástupcem adres místních jsou tzv. lokální unikátní adresy. Označují se prefixem fc00::/7 a následuje bitový příznak L. (Satrapa, 2011, s. 55–79; 2008a; Lammle, 2010, s. 724–725)

1.2.6 Speciální

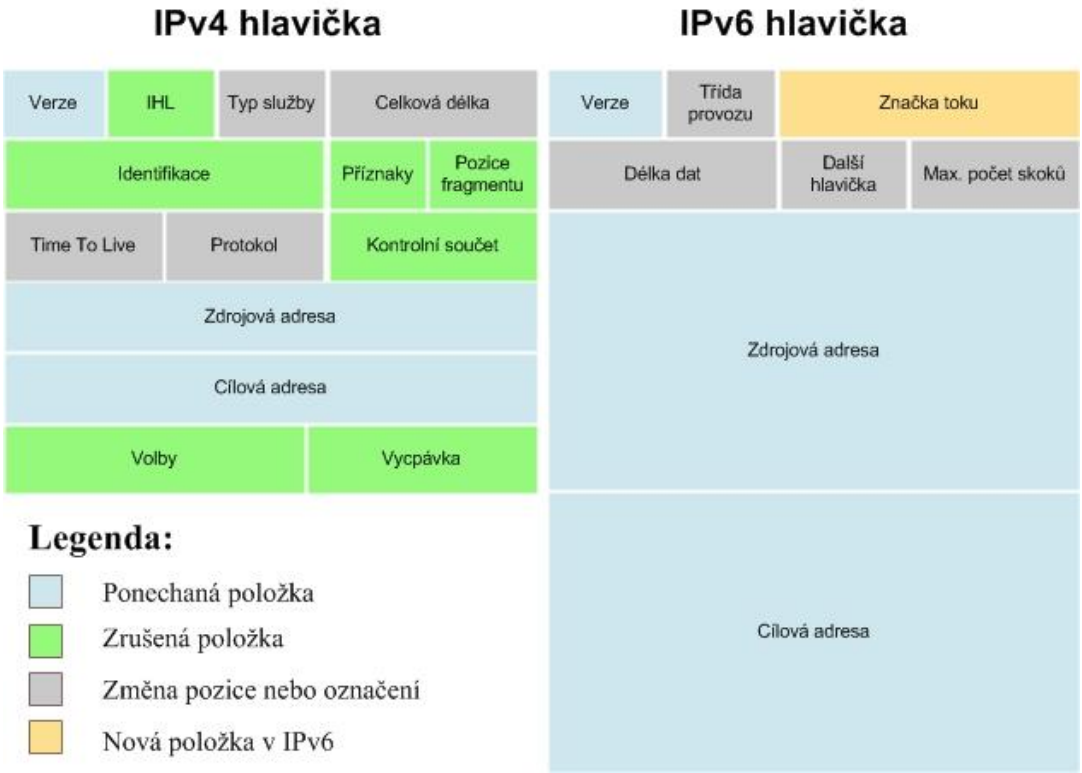
Protokol IPv6 taktéž definuje následující speciální adresy. (Satrapa, 2008a)

Tabulka 1 – Speciální druhy adres

prefix	význam
::/128	nedefinovaná adresa
::1/128	lokální smyčka (loopback)
fc00::/7	unikátní individuální lokální adresa
fe80::/10	individuální lokální adresy
ff00::/8	skupinové adresy
2001:db8::/32	dokumentační prefix – pro fiktivní adresy v dokumentech (RFC 3849) (Huston, Lord a Smith, 2004)
ff0X::db8:0:0/96	dokumentační prefix pro skupinové adresy (RFC 6676) (Venaas et al., 2012)

1.3 Hlavička IPv6

Datagram IPv6 protokolu obsahuje nejprve hlavičku a následně přenášená data. Oproti záhlaví IPv4 ovšem došlo ke značnému přepracování. IPv4 hlavička má proměnlivou velikost, IPv6 konstantní – 40B (z toho 32B zabírají adresy odesílatele a příjemce) – a obsahuje pouze nejnutnější informace, případné další doplňující nebo nepovinná data se přenáší v next header. Specifikace IPv6 hlavičky je obsáhle popsána v RFC 2460 (Hinden a Deering, 1998). (Satrapa, 2011, s. 35–37; 2008b; Loshin, 2004, s. 126–132)

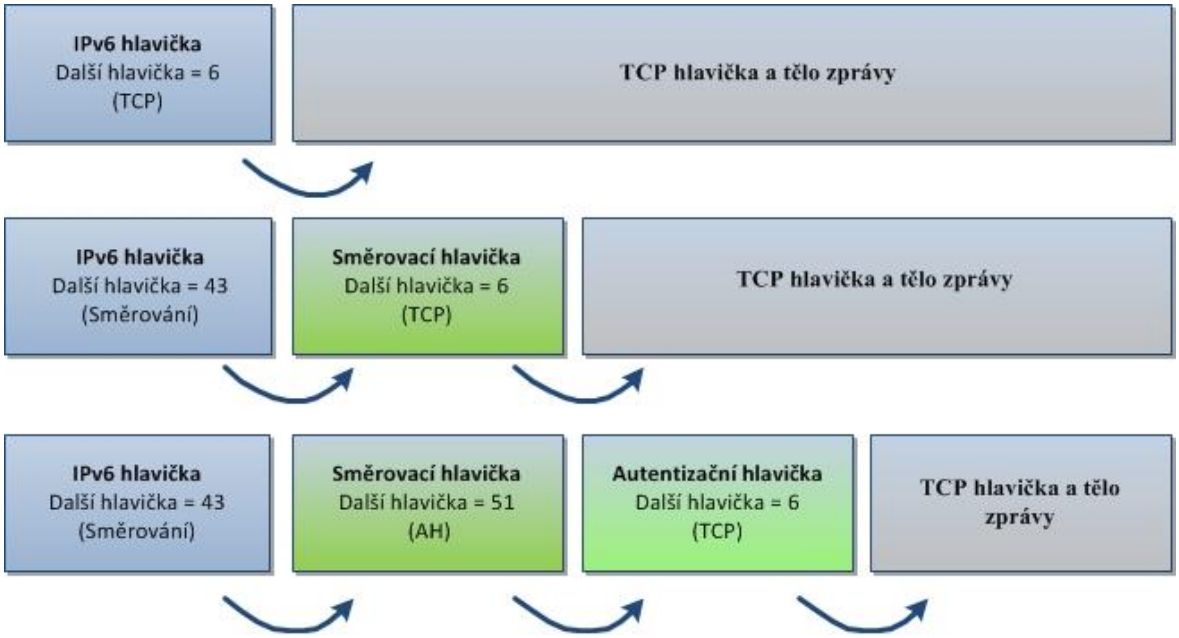


Obrázek 2 – Srovnání IPv4 a IPv6 hlaviček [vytvořeno autorem, převzato z lupa.cz]

IPv6 hlavička obsahuje následující pole:

- **Verze (Version) –** identifikuje verzi protokolu, zde 6.
- **Třída provozu (Traffic class) –** priorita datagramu, tato položka se stará také o QoS.
- **Značka toku (Flow label) –** „Koncepce toku je novinkou v IPv6 a stejně jako třída provozu zatím není přesně definována. V zásadě by jako tok měl být označován proud datagramů se společnými vlastnostmi (odesilatel, adresát, požadavky na vlastnosti spojení). Prostřednictvím identifikátoru (značky) směrovač rychle rozpozná, že datagram je součástí určitého toku, což mu usnadní rozhodování o jeho dalším osudu (bude s ním naloženo stejně, jako s předchozími členy téhož toku).“ (Satrapa, 2011, s. 36)
- **Délka dat (Payload length) –** určuje velikost datagramu, respektive počet bajtů jdoucích za standardní hlavičkou, základní hlavička se do této délky nepočítá.
- **Další hlavička (Next header) –** Jelikož je IPv6 hlavička stručná a občas je potřeba přenášet další informace, vznikla tzv. další hlavička, která zřetězuje informace rozšiřujících hlaviček.
- **Max. počet skoků (Hop limit) –** je to maximální počet průchodů datagramu sítí, každý směrovač tuto hodnotu sníží o jedničku, a když je hodnota nulová, tento datagram zahodí a pošle odesílateli ICMPv6 hlášení. U protokolu IPv4 toto obstarával TTL (Time To Live).
- **Zdrojová a cílová adresa (Source and destination address) –** adresy zabírají vzhledem ke své velikosti 80% hlavičky.

Koncept řetězení rozšiřujících hlaviček popisuje podrobněji obr. 3.



Obrázek 3 – Koncept řetězení rozšiřujících hlaviček [vytvořeno autorem, převzato z lupa.cz]

Přehled rozšiřujících hlaviček a jejich hodnot zobrazuje tabulka 2. (Satrapa, 2008b)

Tabulka 2 – Přehled rozšiřujících hlaviček

Popis	Hodnota	Informace
Volby pro všechny	0	informace zajímavé pro každého po cestě (např. upozornění směrovače, že paket nese data, která by jej mohla zajímat)
Směrování	43	datagram musí projít předepsanou cestou
Fragmentace	44	při fragmentaci paketu nese informace nutné pro jeho složení do původní podoby
Šifrování obsahu (ESP)	50	obsah datagramu je zašifrován, ESP hlavička nese odkaz na parametry pro dešifrování
Autentizace (AH)	51	data pro ověření totožnosti odesilatele a původnosti obsahu
Poslední hlavička	59	nic dalšího nenásleduje
Volby pro cíl	60	informace určené příjemci datagramu (např. domácí adresa mobilního uzlu)
Mobilita	135	pro potřeby komunikace s mobilními zařízeními

Typ nesených dat uvádí tabulka 3. (úplnou specifikaci popisuje stránka http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml)
(Protocol Numbers, 1994)

Tabulka 3 – Typ nesených dat rozšiřující hlavičky

Hodnota	Protokol
6	TCP
8	EGP
9	IGP

Hodnota	Protokol
17	UDP
46	RSVP
47	GRE
58	ICMP

1.3.1 Směrovací hlavička

Vzhledem k tomu, že tato práce má za úkol přiblížit čtenáři principy směrování a jeho praktické využití, je důležité detailněji popsat jednu z rozšiřujících hlaviček, a to hlavičku směrovací.

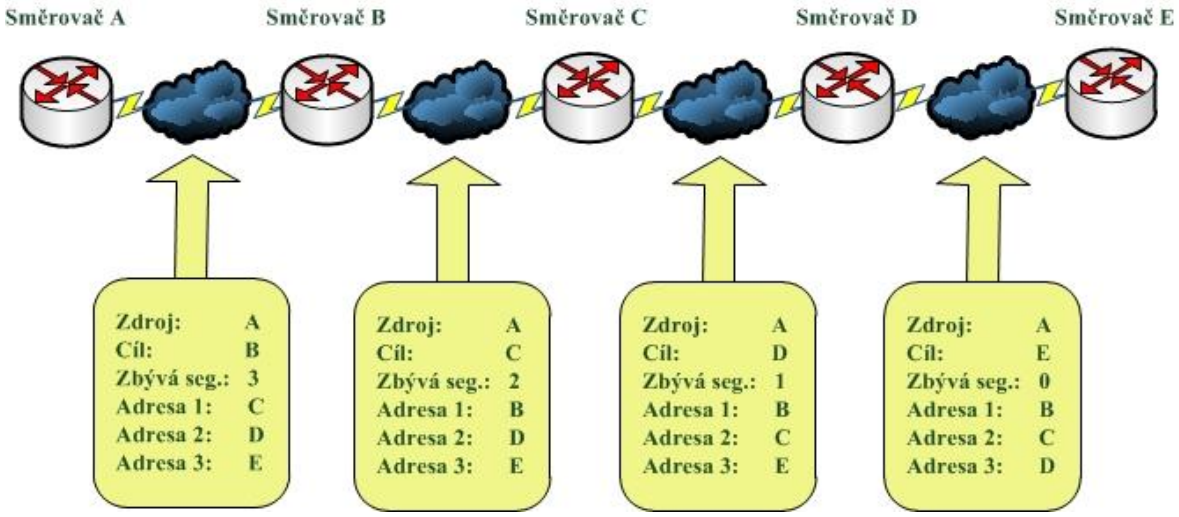
„This header causes the packet to visit specific nodes, specified in the header, on its route to its destination. The initial destination address of the IPv6 header is not the same as the ultimate destination of the packet, but rather the first address in the list contained in the Routing Header. When that node receives the packet, it processes the IPv6 header and the Routing Header and resends the packet to the second address listed in the Routing Header. This process continues until the packet reaches its ultimate destination.“ (Loshin, 2004, s. 133)

Tato hlavička způsobí, že paket projde určenými uzly k cíli specifikovanými v hlavičce. Původní cílová adresa IPv6 hlavičky není stejná jako koncová adresa paketu, ale spíše první adresa v seznamu směrovací hlavičky. Když uzel obdrží paket, zpracuje IPv6 záhlaví a směrovací záhlaví a přepošle paket na druhou adresu v seznamu směrovacích hlaviček. Tento proces pokračuje, dokud se paket nedostane do konečného cíle. (volně přeloženo autorem)

V současné době jsou definovány 2 typy směrovací hlavičky:

- Typ 0 – Hlavička obsahuje předem určené body, kterými má paket projít a čítač, určující kolik adres ještě zbývá projít do cíle. Podle RFC 5095 (Abley, Savola a Neville-Neil, 2007) je ale tento typ zavržen z důvodu nebezpečí jeho zneužití (paket je možno plně naplnit adresami aby dlouze koloval sítí a zahlcoval tak linky).
- Typ 2 – „Typ 2 byl definován speciálně pro mobilitu. De facto se jedná o silné zjednodušení obecnějšího typu 0. Když je mobilní uzel na cestách, má kromě své původní pevné adresy i adresu dočasnou, jež se mění podle sítě, ve které se právě nachází. Pokud přechází mezi buňkami, může se dočasná adresa během komunikace měnit. Aby nebyla narušena komunikace běžících programů, používá pro ni svou trvalou, tak zvanou domácí adresu. Jeho partner pomocí směrovací hlavičky typu 2 stanoví, že koncovou adresou je pevná adresa mobilního uzlu, ale má se nejprve dopravit na jeho dočasnou adresu. Čili datagram je dopraven na aktuální dočasnou adresu, tam se postupem podobným směrování typu 0 nahradí cílová adresa hodnotou ze směrovací hlavičky a vyšším komunikačním vrstvám se data doručí, jako by

přišla na trvalou adresu. Směrovací hlavička typu 2 proto umožňuje uložit jen jedinou adresu (domácí adresu mobilního uzlu, jemuž je datagram určen). To výrazně omezuje její zneužitelnost.“ (Satrapa, 2011, s. 45)



Obrázek 4 – Princip změn informací ve směrovací hlavičce typu 0 [vytvořeno autorem, převzato z Satrapa, 2011, s. 44]

Obrázek 5 – Rozšiřující hlavička směrování typu 0 [vytvořeno autorem, převzato z Satrapa, 2011, s. 44]

1.4 Konfigurace protokolu

„One of the most useful aspects of IPv6 is its ability to automatically configure itself, even without the use of an address configuration protocol such as DHCPv6. An IPv6 host can automatically configure a link-local address for each interface.“ (Davies, 2012, s. 205)

Jedním z nejvíce užitečných aspektů IPv6 je jeho schopnost sám se automaticky nakonfigurovat, a to i bez použití adresního konfiguračního protokolu DHCPv6. Hostitel IPv6 může automaticky nakonfigurovat link-local adresy pro každé rozhraní. (volně přeloženo autorem)

Protokol IPv6 tedy lze konfigurovat těmito způsoby:

- automatickou konfigurací,
    - stavovou,
    - bezstavovou,
- ruční konfigurací.

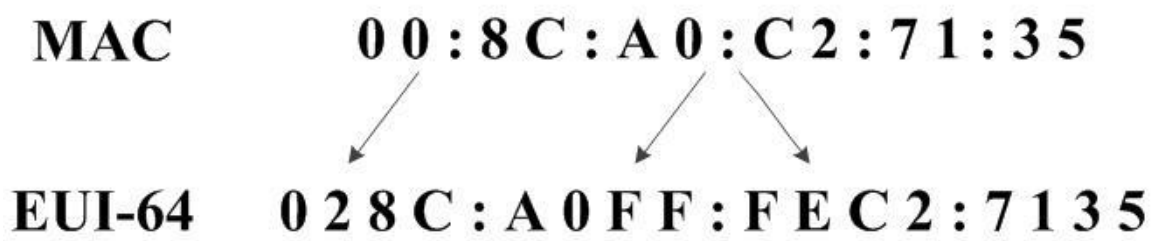
1.4.1 Autokonfigurace

- **Stavová autokonfigurace** – základem je DHCPv6 server definovaný v RFC 3315 (R. Droms et al., 2003), který přijímá požadavky o přidělení adresy od připojeného zařízení.

- **Bezstavová autokonfigurace** – funguje na principu objevování sousedů a probíhá tak, že směrovač po náhodném časovém intervalu posílá oznamovací zprávy obsahující prefix dané sítě, připojené zařízení si vezme tento prefix a připojí k němu náhodně vygenerovaný 64bitový identifikátor rozhraní. Tento typ konfigurace je někdy označován také jako SLAAC (Stateless Address Autoconfiguration) a je definován v RFC 2462 (Thomson a Narten, 1998). (Satrapa, 2011, s. 119)

1.4.2 Ruční konfigurace

Protokol lze taktéž konfigurovat ručně. Vychází se z předpokladu, že každé zařízení má svou jedinečnou MAC adresu, ze které se pak IPv6 adresa sestavuje. Tato část, spolu se vsuvkou FF:FE pak představuje tzv. identifikátor rozhraní, který zabírá polovinu délky adresy, tedy 64 bitů. Tato metoda konfigurace se nazývá EUI-64 a výsledná adresa se skládá z ručně zadaného prefixu a hostitelské části podle výpočtu uvedeného výše. Dále musí být věnována pozornost tomu, jestli chceme adresu globálně jednoznačnou nebo lokální. V prvním případě musí být druhý bit v adrese nenulový, v druhém případě musí nabývat hodnoty 0. (Satrapa, 2011, s. 61–62)



Obrázek 6 – Vytvoření identifikátoru rozhraní [vytvořeno autorem, převzato z ipv6.cz]

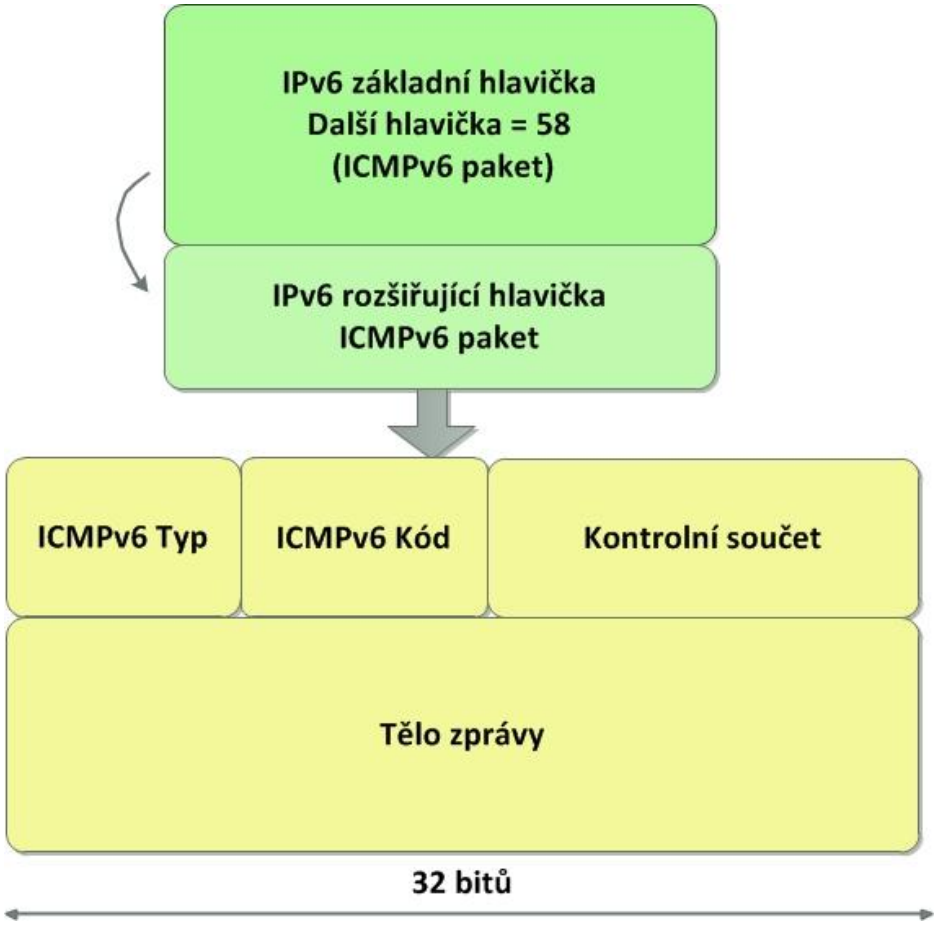
1.5 Ověření konfigurace – využití ICMPv6

„Internet Control Message Protocol (ICMP) je režijním protokolem Internetu. Slouží k ohlašování chybových stavů, testování dosažitelnosti a všeobecně k výměně některých provozních informací. Jeho implementace je povinná v každém zařízení podporujícím IP. Skutečnost, že IP datagram nese ICMP zprávu, signalizuje hodnota 58 v položce Další hlavička.“ (Satrapa, 2011, s. 97)

„Protokol IPv4 využívá ICMP k mnoha účelům, jak např. přenos chybových zpráv typu nedosažitelnosti cíle a funkcím pro řešení potíží typu příkazů Ping a Traceroute. Protokol ICMPv6 tyto služby poskytuje i nadále, ale na rozdíl od svého předchůdce není verze 6 implementována jako samostatný protokol vrstvy 4. Jedná se o integrovanou součást protokolu IPv6 a přenáší se za základní hlavičkou protokolu IPv6 jako rozšiřující hlavička.“ (Lammle, 2010, s. 729) Jako většina protokolů je také popsán v normě RFC, konkrétně v RFC 4443 (Conta, Deering a M. Gupta, 2006).

ICMP hlavička obsahuje následující pole: (Satrapa, 2011, s. 97)

- **Typ –** indikuje druh zprávy, v případě chybových zpráv je nejvyšší bit 0, u informačních zpráv je pak nastaven na hodnotu 1.
- **Kód –** blíže specifikuje typ.
- **Kontrolní součet –** slouží pro kontrolu paketu.
- **Tělo zprávy –** nese buďto specifickou informaci o typu, nebo je pole prázdné.



Obrázek 7 – ICMPv6 hlavička [vytvořeno autorem, převzato z cisco.com]

Zprávy ICMP protokolu jsou rozděleny do dvou tříd: (Satrapa, 2011, s. 99–101)

- **chybové (typ leží v intervalu 0 – 127):**
  - 1 – nedosažitelnost cíle,
  - 2 – paket příliš velký,
  - 3 – expirace životnosti paketu (došlo postupným snižováním Max. Hop na hodnotu 0),
  - 4 – problém s parametry,
- **informační (typ leží v intervalu 128 – 255), je jich více, zde pouze nejdůležitější:**
  - echo (echo request – 128, echo reply – 129),
  - informace o uzlu (ICMP Node Information Query – 139, ICMP Node Information Reply – 140).

Dostupnost zařízení můžeme například ověřit následujícími příkazy:

- ping – slouží pro zkontrolování, zda je cílová adresa dostupná, zobrazuje tedy, zda koncové zařízení odpovědělo a s jakým zpožděním,
- tracert – používá se k analýze sítě, vypisuje seznam směrovačů, přes který paket do cíle prošel.

2 Kooperace sítí s protokoly IPv4 a IPv6

Jak již bylo výše avizováno, největší nevýhoda protokolu IPv6 je kompatibilita s jeho předchůdcem. Vzhledem k faktu, že stále převládají sítě fungující na IPv4 a že přechod k IPv6 není možné realizovat okamžitě, se tento problém musí řešit tzv. přechodovými mechanismy. Těchto mechanismů je celá řada, lze je rozdělit do těchto skupin:

- dual stack,
- tunelování,
- překladače.

2.1 Dual stack

Dual stack, nebo též v překladu dvojí zásobník je mechanismus, který na každé stanici a směrovači implementuje jak IPv6 tak IPv4. Tato metoda je však složitější na správu z důvodu administrativy obou protokolů.

2.2 Tunelování

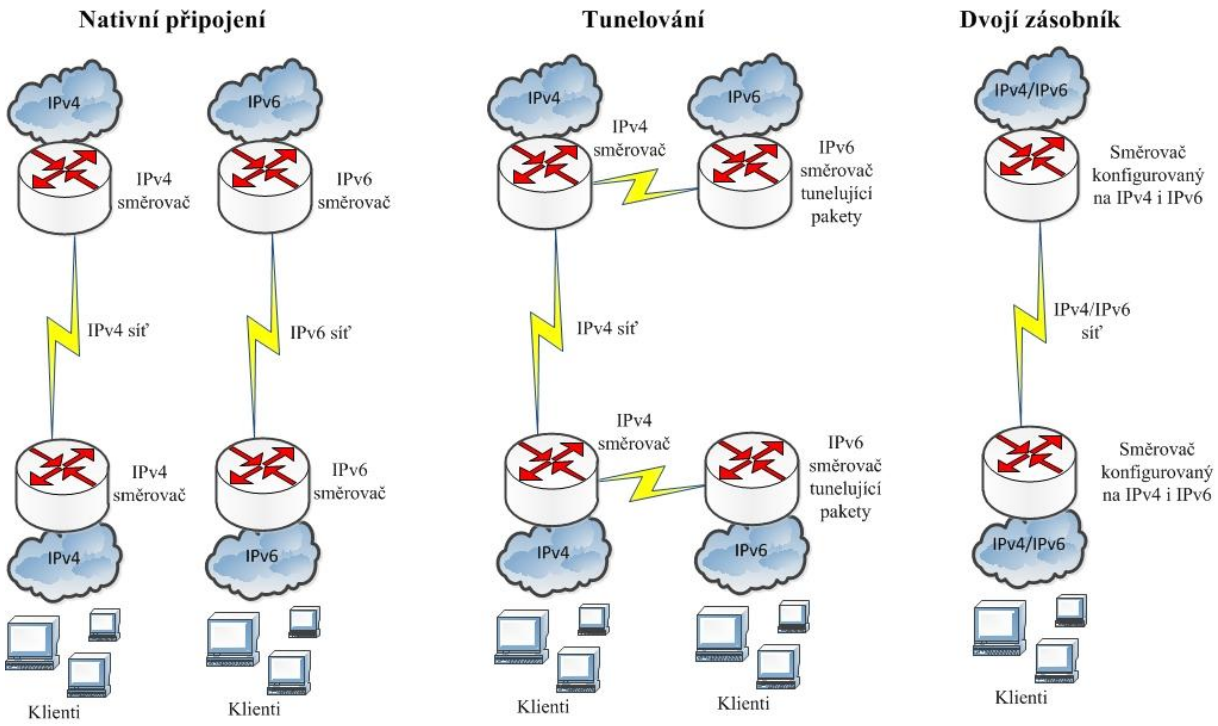
Proces tunelování funguje tak, že se IPv6 datagram zabalí jako data do IPv4 datagramu, pošle IPv4 sítí a koncový směrovač jej rozbalí a posílá dál, teď už do IPv6 sítě. Aby směrovač poznal, že IPv4 datagram nese data vyššího protokolu, je v jeho hlavičce v položce Protokol uvedena hodnota 41.

Zástupce technologie tunelování spolu s jejich RFC definicemi uvádí tabulka 4.

Tabulka 4 – Druhy tunelů

Typ tunelu	Dokument
6to4	RFC 3056 (Carpenter, 2001)
6over4	RFC 2529 (Carpenter a Jung, 1999)
ISATAP	RFC 5214 (Templin, Gleeson a Thaler, 2008)
Teredo	RFC 4380 (Huitema, 2006)

Další metodou je intuitivně i metoda nativní, která sice není přechodovým mechanismem, ale stojí za zmínku. Vypadá tak, že zařízení pracující na určitém typu protokolu je připojeno k odpovídající síti (se stejným protokolem). Předchozí tři metody tedy ilustruje následující obrázek.



Obrázek 8 – Druhy přenosu dat IPv4/IPv6 sítěmi [vytvořeno autorem, převzato z us.ntt.net]

2.3 Překladače

Je-li na jedné straně zařízení podporující pouze IPv4 a na druhé straně zařízení pracující pouze s novějším typem, je potřeba překladač. Translátor jednoduše překládá síťový provoz z IPv6 do starší verze a naopak, například pro komunikaci IPv6 klienta s IPv4 serverem. Tato technologie už nemá tolik zástupců, jako příklad lze uvést NAT-PT, který byl zavržen a nahrazen novějším NAT64 definovaným v RFC 6146 (Bagnulo, Matthews a Beijnum, 2011).

Při popisování přechodových mechanismů bylo čerpáno z (Davies, 2012, s. 283–299) a (Satrapa, 2011, s. 251–283).

3 Statické směrování s využitím IPv6

Statické směrování je vhodné využít při menších velikostech sítě. Základní funkčnost směrování obstarává směrovací tabulka. Ta poskytuje informace o tom, kam se má daný paket poslat. Je to tedy v podstatě datová struktura zapouzdřující atributy: (Směrovací tabulka IPv6, 2011)

- prefix sítě,
- rozhraní nebo adresa odchozího paketu,
- hodnota určující trasu, která se použije při více stejných prefixech,
- doba životnosti trasy a způsob jejího stárnutí,
- informace, zda má být trasa publikována (ve zprávách směrovače),
- typ trasy.

Do směrovacích tabulek se u statického směrování záznamy o trasách přidávají ručně. Ovšem při změně topologie sítě se tabulky automaticky neaktualizují. Statické směrování u IPv6 je podobné jako u IPv4. Na Cisco směrovači bychom mohli přidat trasu např. takto:

```
ipv6 route [cílová síť] [ipv6 rozhraní nebo next hop]
```

3.1 Vyhledávací proces

Než se dozvíme o principu hledání cest u protokolu IPv6, je dobré vědět, jak je tato činnost prováděna u jeho předchůdce.

Vyhledávací proces (nebo též anglicky lookup process) je činnost, která využívá hierarchické struktury směrovací tabulky a dokáže tak rychle vyhledat trasu a efektivně směrovat pakety.

V IPv4 se rozlišují 4 úrovně cest: (Online kurikulum CCNA Exploration – CCNA R&S: Routing and Switching Essentials, 2013)

- Ultimátní trasa – je položka směrovací tabulky, která obsahuje buď next-hop IPv4 adresy, popř. výstupní rozhraní, anebo přímo připojenou linku, dynamicky naučenou cestu nebo místní cestu.
- Level 1 trasa – je trasa se stejnou nebo menší třídní maskou adresy, dále se dělí na:
    - Síťovou trasu (Network route) – trasa, jejíž maska sítě je rovna masce sítě příslušné třídy (třída A, B nebo C).
    - Supernet trasa – je to adresa s maskou menší než třídní maska.

    - Výchozí cesta (Default route) – statická cesta s adresou 0.0.0.0/0.

- Level 1 trasa rodiče (Level 1 parent route) – je to trasa, která obsahuje podsítě.
- Level 2 trasa potomka (Level 2 child route) – je trasa, která je podsítí třídní adresy sítě, tedy rodičovské trasy.

Směrovač má tedy pro tento doraziví paket za úkol vyhledat nejlepší trasu. Tento proces probíhá takto: (Online kurikulum CCNA Exploration – CCNA R&S: Routing and Switching Essentials, 2013)

1. Nejprve se prohledají ultimátní trasy, pokud není nalezena shoda, směrovač pokračuje krokem 2.
2. Směrovač prohledá level 1 cesty a jde na další krok.
3. Pokud má k dispozici záznam o trase potomka, předá paket na příslušné rozhraní nebo adresu. Jestliže ani zde není shoda, pokračuje krokem 4.
4. Když je nalezena supernet trasa nebo výchozí trasa, směrovač použije ji.
5. Pokud nebyla nalezena žádná shoda, je paket zahozen.

Záměrem při vývoji IPv6 bylo vytvořit beztřídní protokol, proto u IPv6 odpadá starost s vyhledáváním tras, jako tomu bylo u IPv4 (všechny trasy jsou ultimátní). K tomu, aby směrování mohlo fungovat, je ale potřeba vyhledávací proces i u IPv6. Využívá se při tom hierarchického směrování, kdy se do směrovacích tabulek dostávají pouze agregované prefixy sítí. Čím blíže je tedy datagram k cíli, tím delší prefixy obsahují v záznamech směrovací tabulky. (Satrapa, 2011, s. 141)

„Když má daný stroj předat datagram, vyhledá ve své směrovací tabulce všechny záznamy, jejichž cíl odpovídá cílové adrese datagramu. Může jich být několik s různou délkou prefixů (například prefix ::/0 odpovídá libovolné adrese, implicitní směrovací záznam bude proto pokaždé zařazen mezi kandidáty). Z nich vybere ten, jehož prefix je nejdelší, a datagram odešle podle údajů v něm obsažených.“ (Satrapa, 2011, s. 140)

4 Dynamické směrování s využitím IPv6

Dále lze mimo statického směrování využít směrování dynamické. Používá se u větších sítí z důvodu usnadnění jejich správy, ale předpokládá hlubší znalosti systému tohoto směrování. Jako nevýhoda se jeví především větší nároky na procesor a RAM paměť směrovače. Dynamické směrování ale odstraňuje nevýhodu statiky reagováním na změny v topologii sítě aktualizací směrovací tabulky a při výpadku linky se stará o vyhledání náhradní linky. K tomuto účelu slouží směrovací protokoly.

Směrovací protokoly lze rozdělit na 2 druhy:

- **IGP** – slouží pro výměnu informací v rámci jednoho autonomního systému (AS). „Autonomní systém je tvořen skupinou sítí, které mají jednotnou správu a směrovací politiku. Například běžný poskytovatel Internetu má přidělen svůj autonomní systém, do nějž patří jeho vlastní páteřní síť a sítě zákazníků k ní připojené.“ (Satrapa, 2011, s. 141)

- **EGP** – používají se pro komunikaci mezi různými autonomními systémy.

Příkladem EGP protokolu je BGP (Border Gateway Protocol, pro IPv6 je to BGP+), dále se tato práce zabývá pouze protokoly IGP.

Podle principu funkčnosti se dále směrovací protokoly rozdělují na:

- **typu vektor vzdálenosti** – „Protokoly s vektorem vzdáleností (distance-vector protocol) hledají nejlepší cestu do vzdálené sítě na základě vzdálenosti. Každý průchod paketu směrovačem se označuje jako přeskok (hop). Trasa do sítě, která obsahuje nejnižší počet přeskoků, je považována za optimální. Vektor udává směr do vzdálené sítě. Mezi protokoly s vektorem vzdáleností patří protokoly RIP i IGRP. Přímo připojeným sousedům odesílají celou směrovací tabulku.“ (Lammle, 2010, s. 387)

- **typu stav linky** – „V případě protokolů se stavem linky (link-state protocol), které se také označují jako protokoly algoritmu nejkratší cesty (shortest-path-first protocol), vytváří každý směrovač tři samostatné tabulky. Jedna z těchto tabulek sleduje přímo připojené sousedy, druhá určuje topologii celé datové sítě a třetí slouží jako směrovací tabulka. Směrovače se stavem linky mají o datové síti více informací než směrovače, které pracují se směrovacím protokolem s vektorem vzdáleností. OSPF je směrovací protokol IP, který se jednoznačně řadí do kategorie protokolů se stavem linky. Tyto protokoly odesílají všem ostatním směrovačům v síti aktualizace se stavem svých vlastních linek.“ (Lammle, 2010, s. 387)

4.1 RIPng

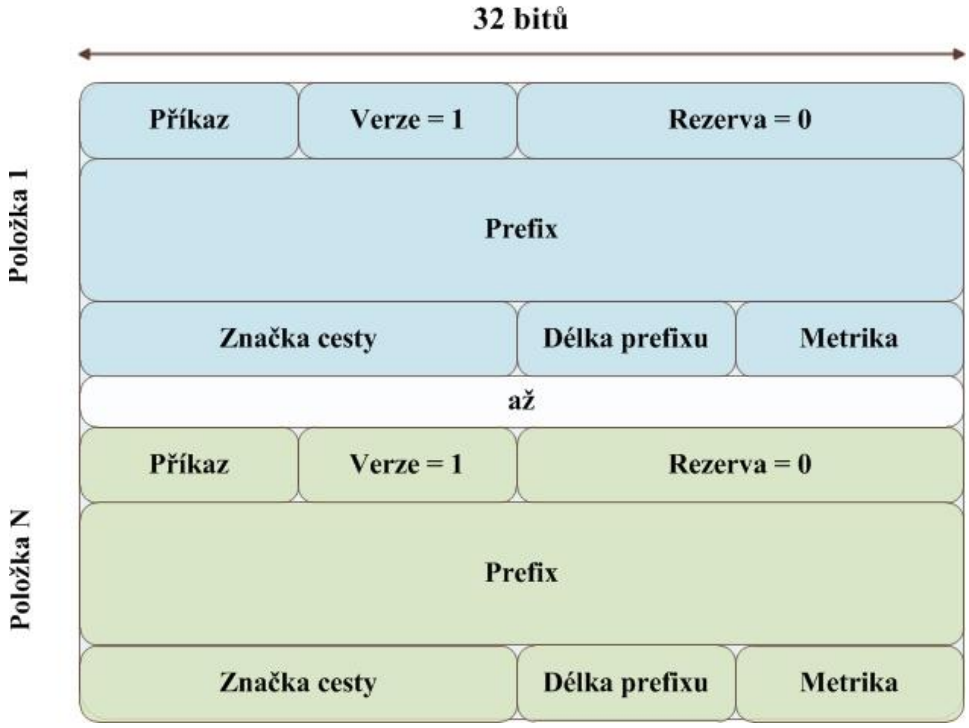
RIPng (Routing Information Protocol next generation) je směrovací protokol typu vektor vzdálenosti. Řadí se mezi nejstarší směrovací protokoly vůbec a jeho specifikace je popsá-

na v RFC 2080 (Malkin a Minnear, 1997). Mezi výhody protokolu RIP patří jeho snadná spravovatelnost, ale je použitelný jen v menších sítích. Maximální vzdálenost je patnáct přeskoků, přičemž při šestnácti a více je zařízení považováno za nedostupné. Za zmínku také stojí, že RIPng vychází z protokolu RIPv2, jen s tím rozdílem, že pracuje s IPv6 adresami.

Směrovací tabulka musí pro potřeby RIPng ke každému cíli obsahovat následující údaje: (Satrapa, 2011, s. 143)

- prefix cíle (jeho hodnotu a délku),
- metriku odpovídající celkové ceně cesty,
- adresu dalšího směrovače na cestě (komu má předávat datagramy směřující k tomuto cíli),
- příznak změny (zda se v poslední době změnila),
- časovače: dobu platnosti a likvidační interval.

Směrovače po startu začnou odesílat směrovací informace, obsahující mj. i délku cesty k cílovému zařízení (vypočtenou z ceny linek a směrovačů). Protokol pracuje tak, že každých 30 sekund odesílá tyto informace z vlastní směrovací tabulky všem zařízením jako multicast na adresu ff02::9. Odesílání zprávy může vyvolat i jiný podnět, např. změna v síti nebo odpověď na požadavek od souseda. Proces směrování tedy funguje tak, že se směrovač snaží vybrat trasu s nejkratší cestou k cíli.



Obrázek 9 – Formát zprávy RIPng [vytvořeno autorem, převzato z Satrapa, 2011, s. 144]

Jak je vidět z obrázku 9, zpráva obsahuje následující údaje:

- Verze – identifikuje verzi protokolu, zde 1.
- Příkaz – v současnosti jsou pouze 2 příkazy, a to požadavek a odpověď nebo aktualizace.
- Prefix a délka prefixu – určuje cíl položky.
- Metrika – neboli vzdálenost k cíli.
- Značka cesty – slouží k rozlišení mezi cestami z ostatních směrovacích protokolů.

4.2 EIGRPv6

Dalším z IGP protokolů je EIGRPv6 (Enhanced Interior Gateway Protocol version 6). EIGRP je proprietární protokol společnosti Cisco, který rozšiřuje starší protokol IGRP. Na základě algoritmu DUAL (Diffused Update Algorithm) počítá nejkratší cestu k cíli, díky čemuž se vyznačuje velmi rychlou konvergencí. Protokol posílá pouze částečné aktualizace, tedy jen takové, které se změnily. Díky tomu efektivněji využívá šířku pásma.

„Protokol EIGRP se někdy označuje jako hybridní směrovací protokol, protože se vyznačuje vlastnostmi jak protokolů s vektorem vzdáleností, tak protokolů se stavem linky. Protokol EIGRP například neodesílá pakety se stavem linky jako protokol OSPF. Místo toho odesílá tradiční aktualizace s vektorem vzdáleností, které obsahují informace o sítích spolu s náklady na jejich dosažení z pohledu zveřejňujícího směrovače. Protokol EIGRP má také vlastnosti protokolu se stavem linky – při spuštění synchronizuje směrovací tabulky mezi sousedními směrovači a poté odesílá konkrétní aktualizace pouze při změnách topologie. Díky tomu je protokol EIGRP vhodný pro velmi velké sítě. Protokol EIGRP má maximální počet přeskoků 255 (výchozí hodnota je nastavena na 100).“ (Lammle, 2010, s. 422)

V protokolu EIGRP existují následující druhy paketů:

- Hello – Je posílán jako multicast na adresu FF02::10 a slouží k identifikaci sousedů.
- Update – Multicast, pomocí těchto paketů si soused sestavuje topology table.
- Acknowledgement – Potvrzuje přijetí update, reply nebo query paketu. Jsou posílány jako unicast.
- Query a Reply – Jsou odesílány v případě přepnutí zařízení do aktivního stavu. Dotazy (Query) jsou multicastové, kdežto odpovědi na ně (Reply) jsou unicastového typu.

Protokol si udržuje 2 tabulky, a to:

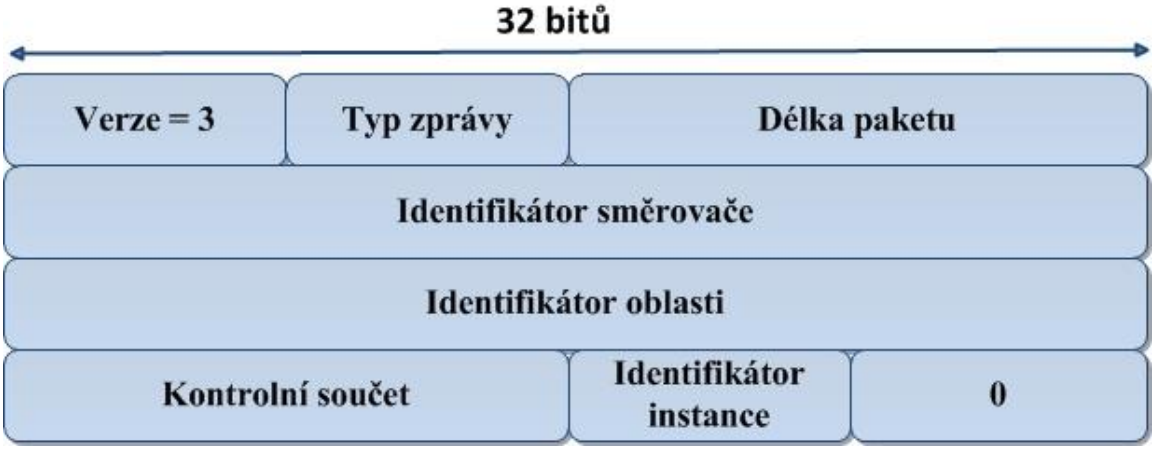
- Tabulku sousedů (Neighbor Table) – v této tabulce jsou uložené informace o sousedech.
- Tabulku topologie (Topology Table) – tato tabulka se plní na základě činnosti algoritmu DUAL a obsahuje informace, podle kterých vytváří směrovací tabulku.

EIGRP zavádí ještě další 2 pojmy, a to možný následník (feasible successor) a následník (successor). Možný následník je trasa, která je považována za záložní (její oznámená vzdálenost je menší než pravděpodobná vzdálenost). Druhý typ je považován za nejlepší trasu k cíli, je vybírán z možných následníků a ukládá se do směrovací tabulky.

4.3 OSPFv3

Mezi zástupce protokolů se stavem linky se jednoznačně řadí OSPFv3 (Open Shortest Path First version 3). Tento je popsán v dokumentu RFC 5340 (Coltun et al., 2008), který je upraven pro použití IPv6 a vychází z protokolu OSPFv2 definovaného v RFC 2328 (Moy, 2008). Výhody tohoto protokolu jsou rychlá konvergence a schopnost pracovat s rozsáhlejšími sítěmi.

Směrovač zpočátku začne posílat tzv. Hello paket, kterým zjistí sousedy ve svém okolí. Protokol pak pracuje na principu, že každý router udržuje kompletní mapu celé sítě (respektive jednoho autonomního systému), tzv. Link State Database, podle které pak provádí výpočet nejkratších cest (z názvu − Shortest Path First). Směrovací tabulka se tedy plní aplikováním tohoto algoritmu, kterému se také říká Dijkstrův algoritmus a tzv. zaplavováním (angl. flooding), kdy každý směrovač při změně v topologii posílá svojí databázi všem směrovačům v okolí. Konvergence síť dosáhne tehdy, když všechny směrovače odeslaly LSA (Link State Advertisement) paket a mají shodnou databázi. Směrovače mají úplný přehled o celé síti, na rozdíl od protokolů typu vektor vzdálenosti, kdy mají směrovače pouze informace, kudy mají daný paket do cílové sítě poslat.



Obrázek 10 – Hlavička OSPF zprávy [vytvořeno autorem, převzato z Satrapa, 2011, s. 153]

Položku Typ zprávy pak popisuje podrobněji následující tabulka. (Satrapa, 2011, s. 153)

Tabulka 5 – Typy OSPF zpráv

Typ	Název	Význam
1	Hello	zjištění okolních směrovačů
2	Popis databáze	shrnuje obsah databáze
3	Žádost o stav linky	požaduje LSA
4	Aktualizace stavu linky	aktualizace databáze (posílá LSA)
5	Potvrzení stavu linky	potvrzuje aktualizaci

Vzhledem k tomu, že protokol OSPF podporuje opravdu velké sítě, lze tyto sítě navíc rozdělit do tzv. oblastí, které rozdělují autonomní systém na části. V těchto oblastech pak pracují jednotlivé instance tohoto algoritmu a tím se zvyšuje výkon – směrovače neposílají aktualizační pakety do celé sítě, ale jen do své oblasti.

Poznatky o dynamickém směrování byly čerpány především ze (Satrapa, 2011, s. 139–156), dále z (Lammle, 2010, s. 729–732) a (Loshin, 2004, s. 235–253).

5 Návrh řešení úloh na směrování

Dostáváme se k praktické části bakalářské práce, kde si můžeme v praxi osvojit své dosavadní teoretické poznatky. Pro praktickou ukázku principů IPv6 byl zvolen nástroj Cisco Packet Tracer, konkrétně ve verzi 6.0.1, který dokáže efektivně odsimulovat reálnou počítačovou síť. Aby bylo ale vůbec možné s IPv6 na Cisco směrovači pracovat, je potřeba ho zapnout (implicitně je vypnutý). To se provede příkazem

```
ipv6 unicast-routing.
```

5.1 Autokonfigurace

V této úloze byla zvolena jednoduchá topologie, ale pro demonstrační účely bohatě stačí. Počítače dostanou od směrovače informaci o adrese místní sítě a ti si pak vytvoří na základě modifikovaného EUI-64 svoji adresu.

5.2 Statické směrování

Tento a následující příklady budou z důvodu lepší přehlednosti předváděny na stejné topologii, jen vždy samozřejmě s jinou konfigurací. Opírají se o znalosti bezstavové konfigurace předvedené v první podkapitole tohoto bloku a ukazují v praxi principy směrování na různých protokolech. U statického směrování není konfigurace nikterak složitá. Směrovací tabulka obsahuje pouze ty trasy, které jsme ručně přidali. Tabulka se u protokolu IPv6 zobrazí příkazem

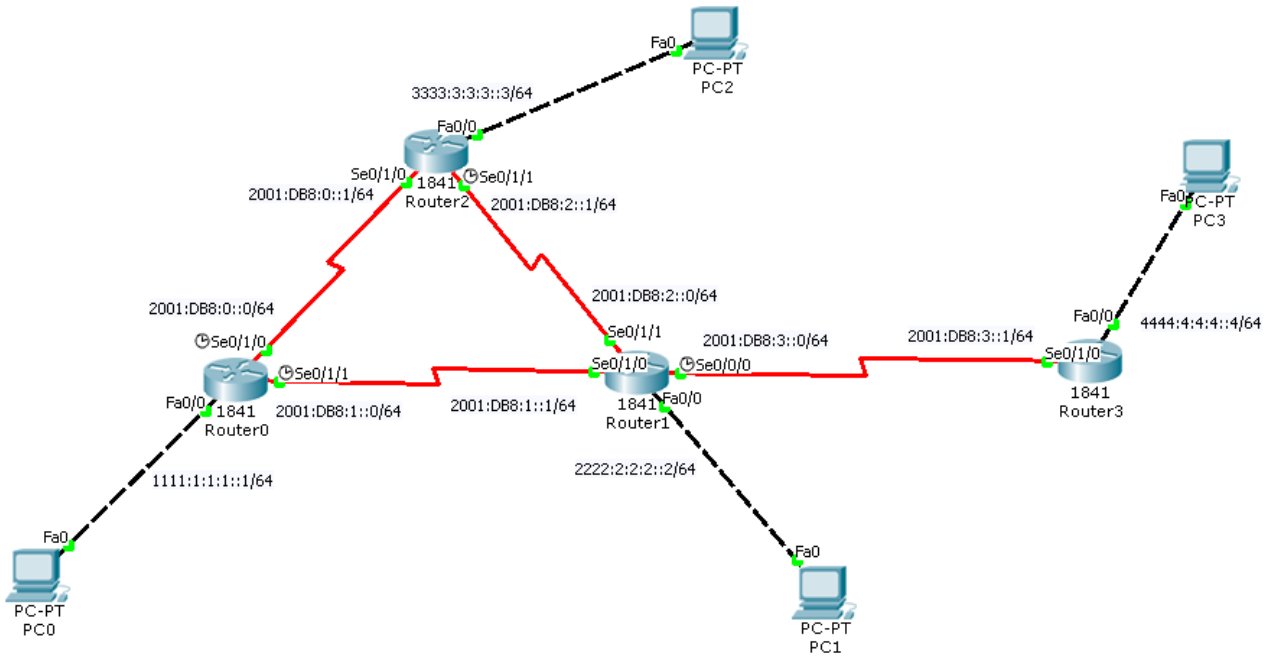
```
show ipv6 route
```

a obsahuje kódy, podle kterých poznáme druh protokolu, který se o přidání trasy postaral.

Přidání trasy obstará příkaz

```
ipv6 route adresa/prefix next-hop nebo odchozí rozhraní.
```

Topologii, ze které vychází úlohy na směrování, ilustruje následující obrázek.



Obrázek 11 – Testovací topologie sítě

Když chce počítač ze sítě 1111:1:1:1::/64 komunikovat například s hostem ze sítě 4444:4:4:4::/64, posílá paket na výchozí bránu, tedy ke směrovači 0. Ten má ve své tabulce, jak je vidno z následujícího obrázku, informaci o tom, že paket pro koncovou síť má předat na adresu 2001:DB8:1::1, což je příchozí rozhraní od našeho směrovače 0. Následník zase prohledá svojí tabulku a zjišťuje, že paket musí poslat ještě dál. Na koncovém směrovači už ale směrovací tabulka obsahuje údaj o přímo připojené síti 4444:4:4:4::/64 a posílá tedy paket na rozhraní jemu odpovídající.

Na následujícím obrázku si můžeme všimnout kódů na začátku každého řádku směrovací tabulky. Zde pár nejdůležitějších:

- C – přímo připojené zařízení.
- S – trasa přidaná ručně.
- R – trasu přidal protokol RIP.
- O – tato trasa byla přidána pomocí protokolu OSPF.
- D – přidání této trasy zajistil protokol EIGRP.

```
Router#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   1111:1:1:1::/64 [0/0]
     via ::, FastEthernet0/0
L   1111:1:1:1::1/128 [0/0]
     via ::, FastEthernet0/0
C   2001:DB8::/64 [0/0]
     via ::, Serial0/1/0
L   2001:DB8::/128 [0/0]
     via ::, Serial0/1/0
C   2001:DB8:1::/64 [0/0]
     via ::, Serial0/1/1
L   2001:DB8:1::/128 [0/0]
     via ::, Serial0/1/1
S   2222:2:2:2::/64 [1/0]
     via 2001:DB8:1::1
S   3333:3:3:3::/64 [1/0]
     via 2001:DB8::1
S   4444:4:4:4::/64 [1/0]
     via 2001:DB8:1::1
L   FF00::/8 [0/0]
     via ::, Null0
Router#
```

Obrázek 12 – Směrovací tabulka u statického směrování

5.3 RIPng

Po statickém směrování se dostáváme k protokolu RIPng, tedy ke směrování dynamickému. Když chceme pracovat s IPv6 musíme ho samozřejmě zapnout. Stejně tak to platí u protokolu RIPng i dalších následujících. U RIPng se tedy zapnutí spolu s nastavením identifikátoru provede příkazem

`ipv6 router rip` *`název`*,

ale tím práce nekončí. Dále je nutné u každého rozhraní v budoucí dynamicky směrované síti tento protokol povolit. To zařídí příkaz

`ipv6 rip` *`název`* `enable`.

V ořezaném výpisu lze vidět nastavení směrovače číslo 1. Ve spodní části výpisu se RIPng protokolu nastaví název, čímž se také zapne, a pak přímo v nastavení jednotlivých rozhraní povolí.

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2222:2:2:2::2/64
 ipv6 rip test enable
 ipv6 address autoconfig
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 ipv6 address 2001:DB8:1::1/64
 ipv6 rip test enable
 ipv6 enable
!
interface Serial0/0/1
 no ip address
 ipv6 address 2001:DB8:2::/64
 ipv6 rip test enable
 ipv6 enable
!
interface Serial0/1/0
 no ip address
 ipv6 address 2001:DB8:3::/64
 ipv6 rip test enable
 ipv6 enable
 clock rate 64000
!
interface Serial0/1/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ipv6 router rip test
```

Obrázek 13 – Ořezaný výpis ze směrovače s protokolem RIPng

Po konfiguraci celé sítě si můžeme funkci protokolu ověřit například výpisem směrovací tabulky. V hranatých závorkách je jako první uvedena administrativní vzdálenost (zde u RIPng 120) a jako druhá metrika, která značí počet přeskoků do cílové destinace. Poté už následuje link-local adresa nebo rozhraní, na které se paket přeposílá.

```
Router#sh ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   1111:1:1:1::/64 [120/2]
     via FE80::2E0:8FFF:FE0D:5501, Serial0/0/0
R   2001:DB8::/64 [120/2]
     via FE80::206:2AFF:FE24:4E02, Serial0/0/1
     via FE80::2E0:8FFF:FE0D:5501, Serial0/0/0
C   2001:DB8:1::/64 [0/0]
     via ::, Serial0/0/0
L   2001:DB8:1::1/128 [0/0]
     via ::, Serial0/0/0
C   2001:DB8:2::/64 [0/0]
     via ::, Serial0/0/1
L   2001:DB8:2::/128 [0/0]
     via ::, Serial0/0/1
C   2001:DB8:3::/64 [0/0]
     via ::, Serial0/1/0
L   2001:DB8:3::/128 [0/0]
     via ::, Serial0/1/0
C   2222:2:2:2::/64 [0/0]
     via ::, FastEthernet0/0
L   2222:2:2:2::2/128 [0/0]
     via ::, FastEthernet0/0
R   3333:3:3:3::/64 [120/2]
     via FE80::206:2AFF:FE24:4E02, Serial0/0/1
R   4444:4:4:4::/64 [120/2]
     via FE80::210:11FF:FE80:3001, Serial0/1/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Obrázek 14 – Výpis směrovací tabulky u protokolu RIPng

Další příkaz slouží k ověření použitých protokolů a rozhraní, pro které je na směrovači protokol aktivován. Jeho použití ilustruje následující obrázek.

```
Router#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static
IPv6 Routing Protocol is "rip test"
  Interfaces:
    FastEthernet0/0
    Serial0/0/0
    Serial0/0/1
    Serial0/1/0
```

Obrázek 15 – Výpis protokolů na směrovači 1

Při komunikaci počítače 0 s hostem 3 je paket poslán na směrovač 0, který pak má v tabulce uvedenou síť 4444:4:4:4::/64 s metrikou 3, zde v tabulce tedy cesta s nejmenším počtem přeskoků do cílové sítě. Posílá tedy paket na rozhraní příslušné dané cestě a další směrovač zpracuje paket stejným způsobem. Směrovač 3 už má tuto síť přímo připojenou a posílá paket příslušnému počítači.

5.4 EIGRPv6

Trochu složitější situace je u protokolu EIGRPv6. Zde je nutné z důvodu jednoznačného určení směrovače v síti zadat příkaz určující jeho ID. To se musí stát ještě před samotnou konfigurací směrování. Do konfiguračního režimu protokolu EIGRPv6 se dostaneme příkazem

```
ipv6 router eigrp název,
```

a zde pomocí příkazu

```
router-id adresa v IPv4 tvaru
```

nastavíme samotný identifikátor směrovače. Pak už stačí jen instanci EIGRP zapnout pomocí známého příkazu

```
no shutdown
```

a dále podobným postupem jako u RIPng nastavit rozhraní, u kterých chceme, aby byla v dynamicky směrované síti. Příkaz, kterým toto provedeme je uveden níže.

```
ipv6 eigrp název
```

Při výpise směrovací tabulky vidíme u dynamicky naučených tras v hranaté závorce hodnoty administrativní vzdálenosti a metriky. Směrovací tabulku, tabulku topologie a tabulku sousedů na směrovači 1 znázorňují následující obrázky.

```
Router#show ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
D   1111:1:1:1::/64 [90/2172416]
     via FE80::2E0:8FFF:FE0D:5501, Serial0/0/0
D   2001:DB8::/64 [90/2681856]
     via FE80::2E0:8FFF:FE0D:5501, Serial0/0/0
     via FE80::206:2AFF:FE24:4E02, Serial0/0/1
C   2001:DB8:1::/64 [0/0]
     via ::, Serial0/0/0
L   2001:DB8:1::1/128 [0/0]
     via ::, Serial0/0/0
C   2001:DB8:2::/64 [0/0]
     via ::, Serial0/0/1
L   2001:DB8:2::/128 [0/0]
     via ::, Serial0/0/1
C   2001:DB8:3::/64 [0/0]
     via ::, Serial0/1/0
L   2001:DB8:3::/128 [0/0]
     via ::, Serial0/1/0
C   2222:2:2:2::/64 [0/0]
     via ::, FastEthernet0/0
L   2222:2:2:2::2/128 [0/0]
     via ::, FastEthernet0/0
D   3333:3:3:3::/64 [90/2172416]
     via FE80::206:2AFF:FE24:4E02, Serial0/0/1
D   4444:4:4:4::/64 [90/2172416]
     via FE80::210:11FF:FE80:3001, Serial0/1/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Obrázek 16 – Směrovací tabulka u EIGRPv6

```
Router#show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H   Address                 Interface       Hold  Uptime    SRTT   RTO  Q  Seq
                                            (sec)           (ms)       Cnt Num
0   Link-local address:     Se0/0/0          14   00:13:24  40     1000  0   12
    FE80::2E0:8FFF:FE0D:5501
1   Link-local address:     Se0/1/0          12   00:13:22  40     1000  0   17
    FE80::210:11FF:FE80:3001
2   Link-local address:     Se0/0/1          13   00:13:20  40     1000  0   18
    FE80::206:2AFF:FE24:4E02
```

Obrázek 17 – Tabulka sousedů u EIGRPv6

```
Router#show ipv6 eigrp topology
IPv6-EIGRP Topology Table for AS 1/ID(2.2.2.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 2222:2:2:2::/64, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 2001:DB8:3::/64, 1 successors, FD is 2169856
         via Connected, Serial0/1/0
P 2001:DB8:1::/64, 1 successors, FD is 2169856
         via Connected, Serial0/0/0
P 1111:1:1:1::/64, 1 successors, FD is 2172416
         via FE80::2E0:8FFF:FE0D:5501 (2172416/28160), Serial0/0/0
P 2001:DB8::/64, 2 successors, FD is 2681856
         via FE80::2E0:8FFF:FE0D:5501 (2681856/2169856), Serial0/0/0
         via FE80::206:2AFF:FE24:4E02 (2681856/2169856), Serial0/0/1
P 3333:3:3:3::/64, 1 successors, FD is 2172416
         via FE80::206:2AFF:FE24:4E02 (2172416/28160), Serial0/0/1
P 2001:DB8:2::/64, 1 successors, FD is 2169856
         via Connected, Serial0/0/1
P 4444:4:4:4::/64, 1 successors, FD is 2172416
         via FE80::210:11FF:FE80:3001 (2172416/28160), Serial0/1/0
```

Obrázek 18 – Tabulka topologie u EIGRPv6

5.5 OSPFv3

Jako další příklad v praktické části je využití dynamického směrování pomocí OSPFv3. Stejně jako u každého jiného protokolu musíme nejdříve nastavit identifikátor (název) a tím i protokol zapnout. U OSPFv3 se to provede příkazem

`ipv6 router ospf` *`název`*,

přičemž musíme opět nastavit identifikátor směrovače. Ten se nastaví v režimu konfigurace protokolu, do kterého jsme se přepnuli předchozím příkazem. Potom už stačí v konfiguraci rozhraní tento protokol zapnout, nesmíme ovšem zapomenout na koncept oblastí, které OSPF zavádí. Konfiguraci OSPFv3 na zařízení znázorňuje následující příkaz.

`ipv6 ospf` *`název`* `area` *`číslo oblasti`*

Při pohledu do směrovací tabulky můžeme vidět u OSPF tras v závorkách administrativní vzdálenost (zde 110) a metriku, někdy označovanou také jako cenu.

```
Router#sh ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O   1111:1:1:1::/64 [110/65]
     via FE80::2E0:8FFF:FE0D:5501, Serial0/0/0
O   2001:DB8::/64 [110/128]
     via FE80::2E0:8FFF:FE0D:5501, Serial0/0/0
     via FE80::206:2AFF:FE24:4E02, Serial0/0/1
C   2001:DB8:1::/64 [0/0]
     via ::, Serial0/0/0
L   2001:DB8:1::1/128 [0/0]
     via ::, Serial0/0/0
C   2001:DB8:2::/64 [0/0]
     via ::, Serial0/0/1
L   2001:DB8:2::/128 [0/0]
     via ::, Serial0/0/1
C   2001:DB8:3::/64 [0/0]
     via ::, Serial0/1/0
L   2001:DB8:3::/128 [0/0]
     via ::, Serial0/1/0
C   2222:2:2:2::/64 [0/0]
     via ::, FastEthernet0/0
L   2222:2:2:2::2/128 [0/0]
     via ::, FastEthernet0/0
O   3333:3:3:3::/64 [110/65]
     via FE80::206:2AFF:FE24:4E02, Serial0/0/1
O   4444:4:4:4::/64 [110/65]
     via FE80::210:11FF:FE80:3001, Serial0/1/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Obrázek 19 – Směrovací tabulka u OSPFv3

```
Router#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
1.1.1.1           0   FULL/  -        00:00:34    3               Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:34    6               Serial0/0/1
4.4.4.4           0   FULL/  -        00:00:31    5               Serial0/1/0
```

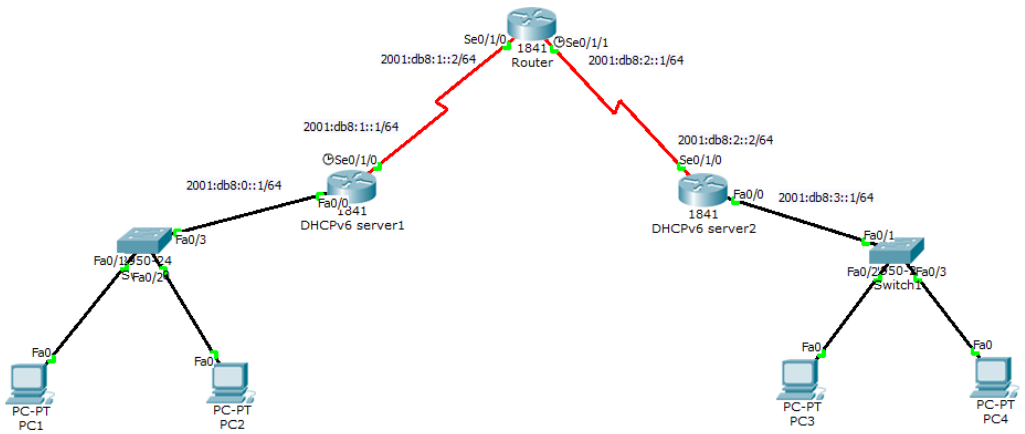
Obrázek 20 – OSPFv3 tabulka sousedů

```
Router#show ipv6 ospf database
            OSPF Router with ID (2.2.2.2) (Process ID 1)

                Router Link States (Area 0)

ADV Router      Age         Seq#       Fragment ID  Link count Bits
2.2.2.2         621         0x80000004 0            3
3.3.3.3         622         0x80000003 0            2
4.4.4.4         622         0x80000002 0            1
1.1.1.1         621         0x80000003 0            2

                Link (Type-8) Link States (Area 0)
ADV Router      Age         Seq#       Link ID     Interface
2.2.2.2         631         0x80000001 1           Fa0/0
2.2.2.2         625         0x80000003 5           Se0/1/0
2.2.2.2         622         0x80000006 4           Se0/0/1
3.3.3.3         622         0x80000004 6           Se0/1/1
4.4.4.4         622         0x80000003 5           Se0/1/0
2.2.2.2         621         0x80000007 3           Se0/0/0
1.1.1.1         625         0x80000004 3           Se0/0/0

                Intra Area Prefix Link States (Area 0)
ADV Router      Age         Seq#       Link ID     Ref-lstype  Ref-LSID
2.2.2.2         622         0x80000004 2           0x2001      0
1.1.1.1         631         0x80000003 2           0x2001      0
3.3.3.3         623         0x80000003 2           0x2001      0
4.4.4.4         625         0x80000002 2           0x2001      0
```

Obrázek 21 – OSPFv3 databáze

5.6 DHCPv6

Jako další úloha na konfiguraci IPv6 byla zvolena stavová konfigurace pomocí DHCPv6. V topologii jsou dva směrovače představující DHCP server a třetí, který je spojuje. Pro ulehčení je zde nastaveno statické směrování.



Obrázek 22 – Topologie sítě v úloze na DHCPv6

Při žádosti o IPv6 adresu musí stanice kontaktovat DHCP server, který vlastní databázi s rozsahem adres, které lze stanici přidělit. Konfigurace tedy probíhá v následujícím sledu.

Příkazem

```
ipv6 dhcp pool název
```

se nastaví název a přejde se do konfiguračního režimu DHCPv6 „poolu“. Zde se určí příkazem

```
prefix-delegation pool název_prefixu
```

alias prefixu, který bude delegován klientům. Dále je nutné tento alias blíže specifikovat a zadat tedy adresu a prefix, který bude hostům delegován (bude se hostům z „poolu“ přiřazovat).

```
ipv6 local pool název_prefixu adresa/prefix délka_přiřazeného_prefixu
```

Nakonec stačí dodat vlastnost pro odchozí rozhraní, pro které chceme, aby čerpal adresy z databáze DHCPv6. V konfiguračním režimu rozhraní to tedy zařídí příkaz

```
ipv6 dhcp server název_poolu.
```

Tím jsme s konfigurací hotovi a už jen stačí u klientských PC nastavit formu získání adresy na DHCP. Příkazem

```
ipv6config
```

si pak můžeme v příkazovém řádku počítače ověřit, zda se adresa přiřadila a jak vypadá.

Pro řešení potíží a výpisy informací o DHCPv6 slouží následující příkazy:

- `show ipv6 dhcp binding,`
- `show ipv6 dhcp pool,`
- `show ipv6 dhcp interface.`

Ve zkráceném výpisu ze směrovače na následujícím obrázku lze vidět celou konfiguraci DHCPv6.

```
hostname DHCPv6_Server2
!
!
!
!
!
ipv6 unicast-routing
!
!
ipv6 dhcp pool test
 prefix-delegation pool test-pool
!
ipv6 local pool test-pool 2001:DB8:3::1/64 64
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:3::1/64
 ipv6 enable
 ipv6 dhcp server test
!
```

Obrázek 23 – Zkrácený výpis ze směrovače konfigurovaného jako DHCPv6 server

Závěr

V práci byl obsáhle uveden základní popis protokolu – specifický zápis adresy, porovnání IPv4 a IPv6 hlaviček, popis směrovací hlavičky, typy adres a dále popis konfigurace IPv6 a ověření konfigurace s využitím protokolu ICMPv6. Druhá kapitola se snaží poukázat na jeden nedostatek, a to přechod mezi IPv6 a jeho předchůdcem, a přiblížit čtenáři metody přechodu z IPv4 na nový protokol. Třetí kapitola se zaměřuje především na statické směrování v IPv6, přičemž je zde pro lepší pochopení směrování a porovnání uveden vyhledávací proces i u IPv4. Čtvrtá kapitola je již obsáhlejší a představuje principy dynamicky směrovaných sítí v IPv6, které jsou potom předvedeny názorně prakticky.

V praktické části práce byly představeny v simulačním nástroji Cisco Packet Tracer vybrané směrovací protokoly, konkrétně OSPFv3, RIPng a EIGRPv6 a dále bylo předvedeno nastavení protokolu pomocí stavové i bezstavové konfigurace.

Práce odráží požadavky mého vedoucího práce a je tedy podle mého názoru patrné, že splnila svůj cíl v celé míře a splňuje tak očekávání od uživatele, který tuto práci čte. Také ji lze, dle mého mínění, využít jako výukový materiál pro předmět Počítačové sítě.

Výsledek mojí činnosti mi dal určitý přehled a hlubší povědomí o IPv6. Rozšířil jsem si také své vědomosti o dalších protokolech a službách počítačových sítí. V praktické části bakalářské práce jsem si osvojil práci s IPv6 na směrovačích firmy Cisco.

Literatura

ABLEY, J., P. SAVOLA a G. NEVILLE-NEIL, 2007. *RFC 5095: Deprecation of Type 0 Routing Headers in IPv6* [online]. December 2007 [cit. 2014-02-02]. Dostupné z: http://www.ietf.org/rfc/rfc5095.txt

BAGNULO, M., P. MATTHEWS a I. VAN BEIJNUM, 2011. *RFC 6146: Stateful NAT64: Network Address and Protocol from IPv6 Clients to IPv4 Servers* [online]. April 2011 [cit. 2014-03-06]. Dostupné z: https://tools.ietf.org/html/rfc6146

CARPENTER, B. a C. JUNG, 1999. *RFC 2529: Transmission of IPv6 over IPv4 Domains without Explicit Tunnels* [online]. March 1999 [cit. 2014-03-06]. Dostupné z: https://www.ietf.org/rfc/rfc2529.txt

CARPENTER, B., 2001. *RFC 3056: Connection of IPv6 Domains via IPv4 Clouds* [online]. February 2001 [cit. 2014-03-06]. Dostupné z: http://www.ietf.org/rfc/rfc3056.txt

COLTUN, R. et al., 2008. *RFC 5340: OSPF for IPv6* [online]. July 2008 [cit. 2014-02-24]. Dostupné z: http://tools.ietf.org/html/rfc5340

CONTA, A., S. DEERING a M. GUPTA, ED., 2006. *RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification* [online]. March 2006 [cit. 2014-02-11]. Dostupné z: http://tools.ietf.org/html/rfc4443

DAVIES, Joseph, 2012. *Understanding IPv6*. 3rd ed. Redmond, Wash: Microsoft. ISBN 978-073-5659-148.

GEORGE, W. et al., 2012. *RFC 6540: IPv6 Support Required for All IP-Capable Nodes* [online]. April 2012 [cit. 2013-11-15]. Dostupné z: http://tools.ietf.org/html/rfc6540

HINDEN, R. a S. DEERING, 1995. *RFC 1883: Internet Protocol, Version 6 (IPv6) Specification* [online]. December 1995 [cit. 2013-11-15]. Dostupné z: https://tools.ietf.org/html/rfc1883

HINDEN, R. a S. DEERING, 1998. *RFC 2460: Internet Protocol, Version 6 (IPv6) Specification* [online]. December 1998 [cit. 2013-11-15]. Dostupné z: https://tools.ietf.org/html/rfc2460

HINDEN, R., S. DEERING a E. NORDMARK, 2003. *RFC 3587: IPv6 Global Unicast Address Format* [online]. August 2003 [cit. 2013-12-02]. Dostupné z: https://tools.ietf.org/rfc/rfc3587.txt

HINDEN, R. a S. DEERING, 2006. *RFC 4291: IP Version 6 Addressing Architecture* [online]. February 2006 [cit. 2013-12-02]. Dostupné z: https://tools.ietf.org/html/rfc4291

HUITEMA, C. a B. CARPENTER, 2004. *RFC 3879: Deprecating Site Local Addresses* [online]. September 2004 [cit. 2013-12-07]. Dostupné z: https://tools.ietf.org/html/rfc3879

HUITEMA, C., 2006. *RFC 4380: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)* [online]. February 2006 [cit. 2014-03-06]. Dostupné z: http://www.ietf.org/rfc/rfc4380.txt

HUSTON, G., A. LORD a P. SMITH, 2004. *RFC 3849: IPv6 Address Prefix Reserved for Documentation* [online]. July 2004 [cit. 2013-12-07]. Dostupné z: http://tools.ietf.org/html/rfc3849

KAWAMURA, S. a M. KAWASHIMA, 2010. *RFC 5952: A Recommendation for IPv6 Address Text Representation* [online]. August 2010 [cit. 2013-12-02]. Dostupné z: https://tools.ietf.org/html/rfc5952

LAMMLE, Todd, 2010. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Vyd. 1. Brno: Computer Press, 928 s. ISBN 978-802-5123-591.

LOSHIN, Pete, 2004. *IPv6 theory, protocol, and practice*. 2nd ed. San Francisco: Morgan Kaufmann, 536 s. ISBN 15-586-0810-9.

MALKIN, G. a R. MINNEAR, 1997. *RFC 2080: RIPng for IPv6* [online]. January 1997 [cit. 2014-02-24]. Dostupné z: http://tools.ietf.org/rfc/rfc2080.txt

MOY, J, 1998. *RFC 2328: OSPF Version 2* [online]. April 1998 [cit. 2014-02-25]. Dostupné z: https://www.ietf.org/rfc/rfc2328.txt

R. DROMS, ED. et al., 2003. *RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* [online]. July 2003 [cit. 2014-02-02]. Dostupné z: http://www.ietf.org/rfc/rfc3315.txt

SATRAPA, Pavel, 2012. Co je IPv6. *IPv6.cz* [online]. 23. 8. 2012 [cit. 2013-11-17]. Dostupné z: https://www.ipv6.cz/Co_je_IPv6

SATRAPA, Pavel, 2011. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, 407 s. CZ.NIC. ISBN 978-80-904248-4-5. Dostupné z: http://knihy.nic.cz/files/nic/edice/pavel_satrapa_ipv6_2012.pdf

SATRAPA, Pavel, 2008a. Adresy. *IPv6.cz* [online]. 23. 8. 2012 [cit. 2013-12-02]. Dostupné z: https://www.ipv6.cz/Adresy

SATRAPA, Pavel, 2008b. Formát datagramu. *IPv6.cz* [online]. 2. 7. 2012 [cit. 2013-11-15]. Dostupné z: https://www.ipv6.cz/Formát_datagramu

TEMPLIN, F., T. GLEESON a D. THALER, 2008. *RFC 5214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)* [online]. March 2008 [cit. 2014-03-06]. Dostupné z: http://tools.ietf.org/html/rfc5214

THOMSON, S. a T. NARTEN, 1998. *RFC 2462: IPv6 Stateless Address Autoconfiguration* [online]. December 1998 [cit. 2014-02-02]. Dostupné z: http://tools.ietf.org/html/rfc2462

VENAAS, S. et al., 2012. *RFC 6676: Multicast Addresses for Documentation* [online]. August 2012 [cit. 2013-12-07]. Dostupné z: http://tools.ietf.org/html/rfc6676

Online kurikulum CCNA Exploration − CCNA R&S: Routing and Switching Essentials, 2013. *Cisco networking academy* [online]. [cit. 2013-03-30]. Dostupné z: www.netacad.com

Protocol Numbers, 1994. *Iana.org* [online]. 16. 1. 2014 [cit. 2013-11-23]. Dostupné z: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Směrovací tabulka IPv6, 2011. *Microsoft Technet* [online]. [cit. 2014-03-27]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc757026%28v=ws.10%29.aspx

Zdroje obrázků

HUSTON, Geoff. IPv4 Address Report. *Potaroo.net* [online]. [cit. 2013-11-07]. Dostupné z: http://www.potaroo.net/tools/ipv4/fig06.png

PODERMAŃSKI, Tomáš a Matěj GRÉGR, 2011. IPv6 Mýty a skutečnost, díl V. - Zjednodušené hlavičky. *Lupa.cz* [online]. 10. 3. 2011 [cit. 2013-11-15]. ISSN: 1213-0702. Dostupné z: http://i.iinfo.cz/images/358/porovnani-zakladni-ipv4-a-ipv6-hlavicky-1.png

SATRAPA, Pavel, 2011. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, 407 s. CZ.NIC. ISBN 978-80-904248-4-5. Dostupné z: http://knihy.nic.cz/files/nic/edice/pavel_satrapa_ipv6_2012.pdf

ICMP for IPv6 Redirect, 2012. *Cisco.com* [online]. 01. 08. 2012 [cit. 2014-02-11]. Dostupné z: http://www.cisco.com/c/dam/en/us/td/i/000001-100000/50001-55000/52501-53000/52728.ps/_jcr_content/renditions/52728.jpg

IPv6. *Us.ntt.net* [online]. [cit. 2014-03-06]. Dostupné z: https://www.us.ntt.net/assets/gr_ipv6_tunneling.jpg