UNIVERZITA PARDUBICE

Fakulta elektrotechniky a informatiky

Analýza chování IGP protokolů při směrování s využitím IPv4 a IPv6

Jan Šmíd

Bakalářská práce

2014

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Šmíd**
Osobní číslo:	**I11202**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza chování IGP protokolů při směrování s využitím IPv4 a IPv6**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem je provést analýzu chování interior gateway protokolů využívajících pro směrování protokol IPv4 a IPv6. Autor představí principy směrování pomocí protokolu IP verze 4 a IP verze 6. Provede analýzu jejich podpory na nejvýznamnějších otevřených a proprietárních protokolech pro LAN sítě. Konkrétně se zaměří na protokoly RIP, EIGRP a OSFP. Autor navrhne možnosti analýzy chování vybraných směrovacích protokolů a provede jejich analýzu na vytvořených testovacích topologiích, které budou realizovány v laboratoři počítačových sítí.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.
GRAZIANI, Rick. IPv6 fundamentals: a straightforward approach to understanding IPv6. Vyd. 1. Brno: Computer Press, 2010, xix, 419 pages 23 cm. ISBN 15-871-4313-5.

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 6. 5. 2014

Poděkování

Rád bych poděkoval panu Mgr. Josefu Horálkovi, Ph.D. za odborné vedení této práce a za jeho rady při řešení problémů, které během vypracovávání této práce nastaly. Dále bych chtěl poděkovat paní Ing. Soně Neradové za pomoc s řešením problémů týkajících se podpory IPv6 ve školních laboratořích.

Anotace

Cílem je provést analýzu chování interior gateway protokolů využívajících pro směrování protokol IPv4 a IPv6. Autor představí principy směrování pomocí protokolu IP verze 4 a IP verze 6. Provede analýzu jejich podpory na nejvýznamnějších otevřených a proprietárních protokolech pro LAN sítě. Konkrétně se zaměří na protokoly RIP, EIGRP a OSPF. Autor navrhne možnosti analýzy chování vybraných směrovacích protokolů a provede jejich analýzu na vytvořených testovacích topologiích, které budou realizovány v laboratoři počítačových sítí.

Klíčová slova

routování, protokol, srovnání, analýza

Title

Analysis of the behavior of IGP routing protocols while using IPv4 and IPv6

Annotation

The aim is to analyze the behavior of interior gateway protocols using for routing protocol IPv4 and IPv6. Author introduces the principles of routing with protocol IP version 4 and IP version 6. He analyzes their support in the most known open and proprietary protocols for LAN networks. Specifically he focuses on protocols RIP, EIGRP and OSPF. The author suggests the way of analysis of the behavior of selected routing protocols and analyze them in the created test topologies which are implemented in the laboratory of computer networks.

Keywords

routing, protocol, comparison, analysis

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

IPv4 - Internet Protokol version 4. Síťový protokol verze 4 používající 32bitové adresy.
IPv6 - Internet Protokol version 6. Síťový protokol verze 6 používající 128bitové adresy.
RIP - Routing Information Protocol
OSPF - Open Shortest Path First
EIGRP - Enhanced Interior Gateway Routing Protocol

Terminologie

byte: Jednotka množství dat, česky bajt.
router: Síťové zařízení pracující převážně na třetí vrstvě, česky směrovač.
point-to-point spojení: Přímé propojení dvou rozhraní jedním fyzickým propojením.

Úvod

Cílem této práce je analyzovat chování nových generací IGP routovacích protokolů v součinnosti s dlouho připravovaným protokolem třetí vrstvy IPv6 a porovnat je s chováním jejich předešlých verzí pracujících nad v současnosti nejrozšířenějším síťovým protokolem IPv4.

Ačkoli je přechod na IPv6 považován již od počátku jeho vývoje za prakticky nevyhnutelný, ozývají se i dnes hlasy brojící proti tomuto protokolu a volající po jiném řešení nedostatečného adresního prostoru protokolu IPv4 a i jiných jeho nedostatků. Těmto hlasům bylo před lety krátkodobě dáno za pravdu zavedením techniky VLSM, která na určitou dobu výrazně snížila tempo úbytku dostupných IPv4 adres.

V posledních letech je za hlavní zbraň proti IPv6 považována technologie překladu síťových adres neboli NAT, která se při práci s omezeným adresním prostorem velmi dobře osvědčila. Nicméně s tempem, jakým v dnešní době přibývají zařízení komunikující přes internet, je i tento přístup k počítačovým sítím nevhodný. Navíc, sama původní myšlenka internetu říká, že každé

IPv6, na rozdíl od myšlenky nekonečného překládání adres, opět přiřazuje samostatnou světově unikátní adresou pro každé k internetu připojené zařízení. V současnosti není počítáno s žádnou alternativou k IPv6, a budoucí rozšíření tohoto protokolu je tedy skutečně nevyhnutelné.

Toto tvrzení bude postupně přibývat na váze tak, jak se budou regionálním registrům tenčit poslední zásoby volných IPv4 adres. IPv6 je nyní podporováno všemi majoritními operačními systémy, v čele s výrobci síťových zařízení jako je Cisco. Širokému nasazení IPv6 již tedy stojí v cestě pouze odpor či nezájem ze strany společností a administrátorů, kteří se změnám ve svých sítích brání z finančních či jiných důvodů.

V této práci je nejdříve zkoumán nový přístup k tvorbě adresního plánu, který již více nevychází z velikosti sítě, ale z jejího „tvaru". Je zde zmíněno několik způsobů jak toto nové paradigma adresování použít k vytvoření co nejefektivnějšího adresního plánu, ať už z hlediska efektivity routování, zabezpečení nebo územního rozdělení sítě.

Dále tato práce zkoumá dopad nového protokolu na návrh jednotlivých routovacích protokolů. Práce nepopisuje implementační detaily, které jsou tajemstvím výrobců síťových zařízení, ale zkoumá návrhy routovacích protokolů a jejich změny a rozdíly mezi verzemi pro IPv4 a IPv6.

Posléze je zkoumán vliv na rychlost konvergence sítě. Za tímto účelem byl navrhnut pár testovacích topologiích, na nichž byl opakovaně prováděn simulovaný výpadek. Pro opravdu seriózní vědeckou studii by byl počet opakování těchto pokusů pravděpodobně nedostatečný, tato práce si ale klade za cíl získat základní představu o vlivu protokolu IPv6 na routovací procesy a případně poukázat, jakým směrem by se měla vydat další zkoumání. Nakonec se tato práce zabývá i množstvím dodatečného síťového provozu, které IPv6 přináší na rozhraní jednotlivých síťových prvků.

1 Adresování v IPv6

Jednou z velkých změn, které protokol IPv6 přinesl, jsou nejenom prodloužené a přepracované síťové adresy, ale i nové paradigma adresování, jež je nutné si předem osvojit. Ještě než přistoupí k tvorbě IPV6 adresního plánu, musí si každý administrátor uvědomit, že sítě nové generace nejsou definovány svou velikostí neboli počtem adres.

Až na výjimky obsahuje koncová IPv6 síť 2^{64}adres. To znamená, že i ta nejmenší síť dokáže pojmout téměř 18,5 milionu bilionů stanic. Toto číslo mnohonásobně převyšuje 4 294 967 296, které představuje všechny IP adresy protokolu IPv4. Šetření a efektivní rozdělování adres lze tedy z procesu přípravy adresního plánu zcela vyloučit.

V podstatě nevyčerpatelná kapacita IPv6 adres umožňuje administrátorům soustředit se na optimalizaci adresování a směrovaní mezi sítěmi, namísto šetření adres. Efektivní správa sítě je totiž cílem protokolu IPv6 (Hoek, 2013, s. 3), přičemž limitujícím faktorem není počet adres, ale právě počet sítí v rámci autonomního systému.

1.1 Přidělení bloku adres

Přidělování bloků IPv6 adres probíhá obdobně jako u IPv4. Úvodní bloky, většinou o délce 23 bitů (ICANN, 2013), přiděluje IANA jednotlivým RIRům, kteří posléze přidělují 32bitové bloky LIRům spadajícím pod jejich správu (Maigron, 2013). Zákazníci LIRů získávají typicky bloky s délkou 48 bitů. Pro sítě v rámci organizace to znamená 16 bitů pro vlastní podsíťování, což znamená až 65 536 koncových sítí (York, 2013, s. 8).

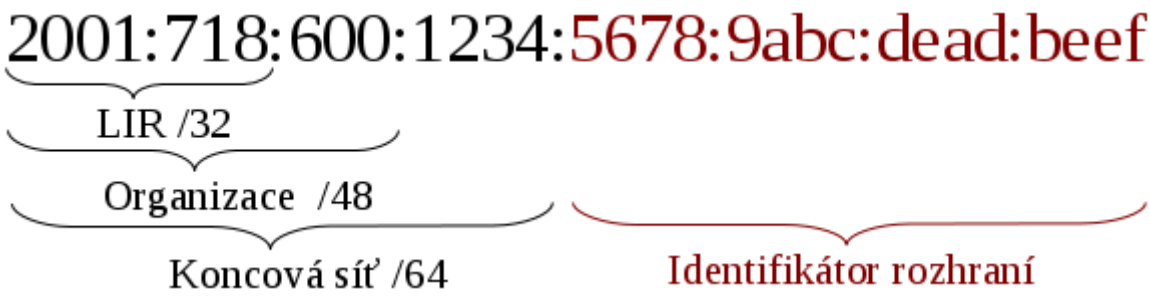
Prefix	Přiřazení	Počet adres
/32	LIR (ISP)	2^{96}
/48	Organizace	2^{80}
/64	koncová síť	2^{64}
/128	koncové zařízení	1

Tabulka 1: Address Block Assignments dle Internet Society

RIPE NCC, registr pro Evropu, Rusko a střední východ, takto 1. 7. 1999 obdrželo prefix 2001:600::/23 (ICANN, 2013). CESNET z tohoto bloku později získal prefix 2001:718::/32. Pardubický POP (přístupový bod do IPv6 sítě) má od CESNETu přidělen blok 2001:718:0600::/42 (Cesnet,2013). Pro Univerzitu Pardubice by mohl být vyhrazen například jeden z 64 možných prefixů od 2001:0718:0600::/48 do 2001:0718:063f::/48. Sítě v rámci Univerzity Pardubice by tak opět měly k dispozici právě 16 bitů.

1.2 Adresace vnitřních sítí

Pro adresaci vnitřních sítí byla vytvořena řada doporučení a nezávazných pravidel (Hoek, 2013, s. 10). Tato pravidla pohlíží na síť z různých úhlů a ulehčují její správu s důrazem na odlišné aspekty, přičemž se jejich kombinace mohou vzájemně doplňovat.



Obrázek 1: IPv6 prefix v rámci pardubického POPu

Nadále pomiňme domácnosti a malé společnosti, které mohou vystačit i s náhodným přidělením několika IP adres. Větší organizace jsou zpravidla tvořeny určitou hierarchií územních celků a pracovních oddělení. Čím větší organizace, tím větší a složitější hierarchie.

Tato organizační struktura se musí nutně promítnout i do počítačové sítě, která musí vyhovovat požadavkům jednotlivých oddělení. A právě tyto požadavky určují, jaký postup zvolit při budování příslušné sítě. Je nezbytné rozhodnout, který aspekt hierarchie bude použit jako klíčový faktor při tvorbě adresního plánu. Může jím být například územní nebo organizační příslušnost.

1.2.1 Dělení primárně dle územních celků (Location based subneting)

Po určení potřebného počtu podsítí pro všechny pobočky a infrastrukturu mezi nimi jsou nejvýznamnější bity přiřazovány nejdříve územním celkům (Hoek, 2013, s. 11). Každá budova takto dostane vlastní blok adres, jejichž další rozdělování bude nezávislé na ostatních budovách. Všechny sítě v rámci jedné budovy budou agregovány do jednoho záznamu v routovací tabulce, která díky tomu bude nabývat menších rozměrů a bude výkonnější.

2001:718:600:LLLL|BBBB|BBBB|BBBB::/64

Univerzita Pardubice má 7 fakult a dalších 5 organizačních celků. Těmi jsou Rektorát, Jazykové centrum, Centrum transferu technologií, Katedra tělovýchovy a Univerzitní knihovna. To znamená alespoň 4 bity pro směrování mezi územními celky ($2^4 = 16$). Ostatní volné bity (B) mohou být přiděleny dle potřeby kancelářím, katedrám a učebnám v dané budově či areálu.

1.2.2 Dělení primárně dle oddělení / aplikace (use-type based subneting)

Pokud je kladen větší důraz na zabezpečení, může se struktura adresního plánu řídit politikami firewallů, které jsou ve většině případů založeny na „typu použití" (Hoek, 2013, s. 10). Vyšší úroveň zabezpečení by mohlo vyžadovat například právnické, účetní nebo vývojové oddělení.

2001:718:600:TTTT|BBBB|BBBB|BBBB::/64

Organizační struktura Fakulty elektrotechniky a informatiky zahrnuje 5 kateder, Oddělení pro operační programy a rozvoj, Oddělení pro vědu a výzkum, Studijní oddělení a Sekretariát děkana. Ke směrování mezi devíti odděleními budou opět potřeba minimálně 4 bity.

1.2.3 Kombinace location a use-type subnetů

Organizační struktura Fakulty elektrotechniky a informatiky nicméně nemusí vyhovovat všem útvarům a fakultám Univerzity Pardubice. Mnohem vhodnějším přístupem může být kombinace předešlých dvou metod. Nejvýznamnější bity se nejdříve přidělí budovám a areálům a až poté v v nich existujícím oddělením (Hoek, 2013, s. 13).

2001:718:600:LLLL|TTTT|BBBB|BBBB::/64

1.2.4 Subnety v hranicích „nibblů"

Nibble jsou 4 po sobě jdoucí bity tvořící jedno hexadecimální číslo. Při vytváření subnetů není nutné se hranic nibblů držet, nicméně jejich použití významně ulehčuje identifikaci podsítí a čtení adres celkově. Použití nibblů odstraňuje nutnost převádět prefixy mezi hexadecimální a binární soustavou, čímž ulehčuje konfiguraci i řešení problémů síťových zařízení (York, 2013, s. 15).

2001:718:600:1300::/64

Takto by například mohla vypadat adresa jedné ze sítí **třetího** oddělení nacházejícího se v **první** budově Univerzity Pardubice. Použití nibblů je spojeno s prefixy /48, /52, /56, /60 a /64 (York, 2013, s. 13). Použití nibblů ovlivňuje i počet dostupných subnetů (viz Tab. 2).

	počet subnetů dané délky			
Prefix	/52	/56	/60	/64
/48	16	256	4096	65536
/52		16	256	4096
/56			16	256
/60				16
/64				1

Tabulka 2: Common subnet prefixes

1.2.5 Odrážení VLAN

Pro identifikaci podsítí je možné použít i virtuální sítě VLAN. Jejich označení, které může zachycovat i location a use-type hierarchii, lze do IPv6 adresy promítnout v dekadické, ale i hexadecimální notaci. Případně je možné použít reverzní zápis. Adresy nad rozsah značení VLAN mohou mít libovolné jiné využití (Hoeck, 2013, s. 15 - 17).

Notace	VLAN	Location	Use-type	
10	529	5	29	
16	211	2	11	
	přímý zápis			reverzní zápis
10	2001:db8:1234:529::/ 64			2001:db8:1234:2905::/ 64
16	2001:db8:1234:211::/ 64			2001:db8:1234:0112::/ 64

Tabulka 3: Promítnutí VLAN do IPv6 adresy

1.2.6 Odrážení IPv4

Pokud již existující IPv4 síť obsahuje podsítě s délkou masky 24 bitů, je možné použít „shodné" subnety i v budované IPv6 síti. Tento přístup lzese nicméně doporučuje pouze pro menší sítě (Hagen, 2006, s. 45). Dodržování hranice 255 podsítí na oktet IPv4 adresy je pro IPv6 doslova nevhodné.

192.0.**2**.0/24	2001:db8:1234:**2**::/64
203.0.**113**.0/24	2001:db8:1234:**113**::/64

Tabulka 4: Shodné IPv4 a IPv6 subnety

Protokol ISATAP a tunelovací mechanismus TEREDO používají adresy obsahující v posledních 32 bitech kompletní IPv4 adresu v její standardní notaci. Ve výsledné adrese IPv6 je ale kvůli převodu do hexadecimální soustavy těžko postřehnutelná (Hagen, 2006, s. 46 - 47).

IPv4	192.168.0.1
ISATAP adresa s původní notací	2001: DB8:510:200:0:5EFE:**192.168.0.1**
ISATAP adresa v IPv6 notaci	2001:DB8:510: 200:0:5EFE:**C0A8:1**

Tabulka 5: ISATAP adresa

1.3 Inter-router (Point-to-Point) adresování

Původním úmyslem bylo přiřazovat i point-to-point spojením prefixy s délkou 64 bitů. S tímto přístupem jsou ale mimo jiné spojeny dva závažné problémy (Kohno, 2011, s. 2). Těmi jsou tzv. „ping pong efekt" a „vyčerpání paměti sousedů".

Ping pong efekt je problémem v sítích, kde není povoleno objevování sousedů (například SONET). Pokud se v takové síti objeví do ní spadající paket, nicméně určený pro neexistující uzel, bude tento paket předáván cyklicky mezi existujícími uzly a zbytečně je zatěžovat. Řešením tohoto problémů je nepřeposílat dále pakety, jejichž odchozím rozhraním je rozhraní příchozí (Kohno, 2011, s. 4).

Vyčerpání paměti sousedů nastává naopak v sítích, v nichž k objevování sousedů dochází. Routeru mohou být například útočníkem podvrhovány pakety od neexistujících uzlů, jež bude router evidovat v paměti sousedů. Služba objevování sousedů se posléze

bude snažit s těmito neexistujícími sousedy komunikovat, čímž bude daný router opět zbytečně zatěžovat. Toto chování může značně omezit zpracovávání užitečného provozu routerem a dovést ho tak prakticky až k DoS (Kohno, 2011, s. 4). Tento problém lze kompletně odstranit pouze přiřazováním prefixů /127.

Prefix /127 lze přirovnat k /31 z IPv4. Nechává nám všehovšudy 2 volné adresy. V IPv4 by to byla adresa sítě a broadcastu. V IPv6 je jedna z těchto adres validní, druhá je tzv. subnet-router anycast, na němž by měly naslouchat všechny routery v dané síti.

Tento problém se určitou dobu řešil použitím prefixů /126, /120 a /112 (Hoeck, 2013, s. 18), nicméně většina výrobců síťových zařízení subnet-router anycast neimplementovala, v důsledku čehož se stalo použití prefixu /127 možným. Tento přístup byl později přijat za standard (Kohno, 2011, s. 5).

2 Routovací protokoly pro IPv6

2.1 Router Information Protocol - RIP, RIP 2, RIPng

Příchod IPv6 sice znamená tak zásadní změny v adresování, že o zpětné kompatibilitě s předešlými verzemi RIPu nemůže být řeč, ale díky prozíravosti, s jakou byl původní návrh vytvořen, mohla být zachována nejen základní funkčnost protokolu, ale i formát „zpráv", kterými mezi sebou jednotlivé routery komunikují.

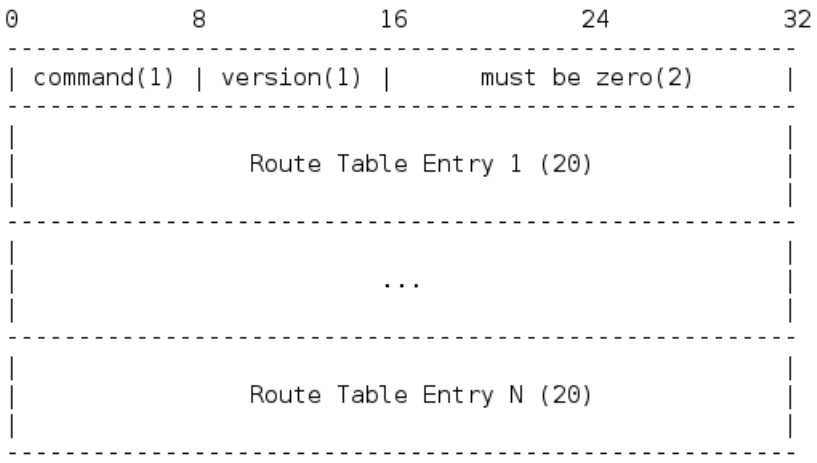
2.1.1 RIP messages

RIP messages (dále jen „zprávy") jsou PDU aplikační vrstvy, pomocí nichž si routery v dané routovací doméně vyměňují informace o cestách v síti. Jejich formát se tedy ani kvůli IPv6 nijak zásadně nezměnil, co se změnilo, je formát Route Table Entries (dále jen „RTE") obsažených v každé zprávě, jejich počet a číslo portu, který protokol pro většinu své komunikace používá (Malkin, 1997, s. 5).

Zatímco původní verze RIPu používají „rip port" 520 a zprávičky mohou nabývat velikosti až 504 bytů (mohou tedy nést až 25 RTE záznamů) (Malkin, 1998, s. 21), u RIPng je používán port 521 a počet RTE záznamů je určen pomocí vzorce zohledňujícího celkovou velikost MTU a velikost zapouzdřujících IPv6, UDP a RIPng hlaviček (Malkin, 1997, s. 6).

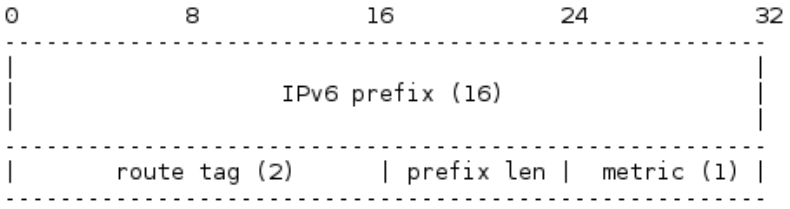
$$RTE\_count = \frac{mtu\_size - ipv6\_hdr\_size - UDP\_hdr\_size - RIPng\_hdr\_size}{RTE\_size}$$

Pojmem RIPng hlavička jsou myšleny první 4 byty zprávy obsahující pole command, version a prozatím nevyužité pole o velikosti 2 bytů. Pole version označuje verzi RIPng protokolu (v současnosti 1) a pole command slouží k odlišení typu zpráv, přičemž jsou definovány typy request a answer.

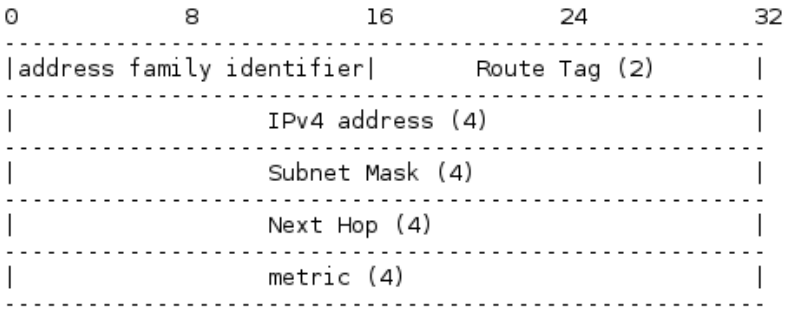


Obrázek 2: RIP message

Formát RTE byl u RIPng oproti RIPu 2 značně zjednodušen. Většinu celé RTE zabírá 128 bitová IPv6 adresa, maska podsítě je v IPv6 nahrazena délkou prefixu (prefix length), pole address family identifier bylo odstraněno a (téměř) nezměněna zůstala pouze pole metriky a route tag pro odlišení interních a externích cest (Malkin, 1997, s. 7). Původní RIP propaguje pouze přímo připojené sítě (directly connected networks), jeho RTE tedy v polích masky podsítě a next hop adresy nese nulové hodnoty (Malkin, 1998, s. 21).



Obrázek 3: RIPng Entry



Obrázek 4: RIP 2 Entry

Pole next hop adresy je v RIPng nahrazeno tzv. „next hop entry" (next hop RTE). Samostatná next hop RTE snižuje velikost celé zprávy, protože její IPv6 prefix je platnou next hop adresou pro všechny po ní následující RTE záznamy, a to až do výskytu další next hop entry. Jednotlivé next hop RTE jsou odlišeny hodnotou 0xFF v poli metriky a povinně vynulovanými poli route tag a prefix length. Přijímající router poté tato pole ignoruje. Pokud je jako next hop adresa uvedena vyhrazená hodnota 0:0:0:0:0:0:0:0 nebo :: (u RIPu 2 je to 0.0.0.0), pak je za next hop považována adresa odesilatele dané zprávy. V jiném případě musí být jako next hop adresa vždy uvedena lokální linková adresa některého routeru v routovací doméně. Naopak, cesty k link local adresám (lokální linková adresa by tedy nebyla uvedena jako next hop, ale jako cílová) nesmí být nikdy propagovány. V RTE nesmí být obsaženy lokální linkové adresy jako koncové sítě (Malkin, 1997, s. 7).

2.1.2 Zpracování RIP messages

Stejně jako předešlé verze, používá i RIPng více verzí RIP zpráv. Pole „command" sice rozlišuje zprávy typu request (požadavek) a response (odpověd), každá z nich se nicméně dále dělí.

- **General request** - Požadavek na celou routovací tabulku. Router je po svém startu používá pro úvodní zaplnění routovací tabulky. Identifikován je jedinou přiloženou RTE a prefixem 0:0:0:0:0:0:0:0 (::). Odesílán je z portu 521 s lokální linkovou adresou rozhraní na „all rip routers" multicast ff02::9 opět na port 521. Během vytváření těchto požadavků je zohledňován proces „split horizon" (Malkin, 1997, s. 10).
- **Specific request** - Dotaz na 1 nebo více adres. Odesílány jsou z libovolného UDP portu (jiného než 521) z globální nebo lokální unicastové adresy na globální nebo lokální unicastovou adresu příjemce na port 521. Split horizon není zohledňováno (Malkin, 1997, s. 10).
- **Unsolicited response** - Tyto v překladu nevyžádané odpovědi se používají při pravidelných nebo triggerovaných aktualizacích. Odesílánu jsou z portu 521 s lokální linkovou adresou rozhraní na multicast ff02::9 na port 521. Zohledňují „split horizon" (Malkin, 1997, s. 15).
- **Solicited response** - Používají se jako odpovědi na požadavky a odesílány jsou vždy z portu 521 na adresu a port uvedené v požadavku. Zdrojová adresa se ale liší dle typu požadavku (Malkin, 1997, s. 15).
    - **response to general request** - Zdrojová adresa odpovědi bude lokální linková adresa rozhraní.
    - **response to general request** - Zdrojová adresa odpovědi bude globální nebo lokální unicastová adresa rozhraní.

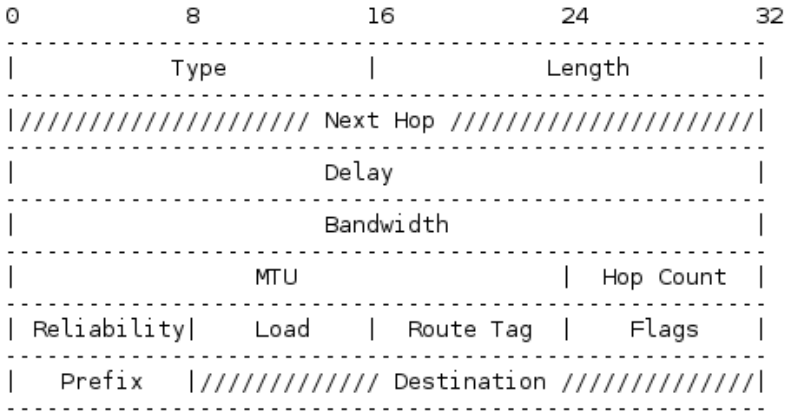
	zdrojová adresa	zdrojový port	cílová adresa	cílový port
Requests				
General	link-local	521	ff02::9	521
Specific	global/local unicast	libovolný kromě 521	global/local unicast	521
Answers				
Unsolicited	link-local	521	ff02::9	521
Solicited to general	link-local	521	request source	request source
Solicited to specific	global/local unicast	521	request source	request source

Tabulka 6: Adresace RIP zpráv

2.2 EIGRP

Enhanced Interior Gateway Routing Protocol, původně proprietární protokol společnosti Cisco Systems Inc., zaznamenal s příchodem IPv6 pouze minimální změny. EIGRP, který byl v roce 2013 uvolněn v podobě informačního RFC i pro jiné výrobce, je již od základu navržen jako modulární protokol nezávislý na použitém protokolu třetí vrstvy. Formát hlavičky EIGRP paketu je tedy univerzální a trvale neměnný (CISCO SYSTEMS, Inc., 1992-2014a).

Protocol Dependent Module pro IPv6, obdobně jako OSPFv3, užívá lokální linkové adresy jako zdrojové adresy Hello paketů (odesílány jsou na multicastovou adresu FF02::A) a implementuje modifikovaná Type-Length-Value pole (Savage, 2014, s. 16). Formát TLV zůstává také prakticky nezměněn, změnila se pouze velikost některých polí tak, aby byla schopná pojmout 128 bitovou IPv6 adresu (CISCO SYSTEMS, Inc., 1992-2014a).



Obrázek 5: EIGRP Internal Route TLV

Například v paketu IP Internal Route TLV se změna týká polí Next hop a Destination. Zatímco je velikost pole Next hop fixní, u Destination je proměnlivá. Vždy však závisí na použitém protokolu třetí vrstvy, respektive délce adres v daném protokolu. V IPv4 bude tedy Next hop dlouhé 32 bitů, v IPv6 128 bitů. Obdobně pro limit délky pole Destination.

Mezi další změny související s IPv6 patří absence split-horizon v EIGRP for IPv6, jak se tato verze protokolu oficiálně nazývá. To proto, že je možné použít více IPv6 prefixů na jednom rozhraní. S přihlédnutím k povaze IPv6 zmizela i možnost automatické sumarizace podsítí „třídních" adres, známých z IPv4 (CISCO SYSTEMS, Inc., 1992-2014a).

2.3 OSPFv3

OSPF, na rozdíl od RIP, nepoužívá k zapouzdření ani TCP, ani UDP protokol. OSPF je stejně jako EIGRP plnokrevný protokol třetí vrstvy nesoucí číslo protokolu 89, jehož zprávy jsou přímo kódovány do IP paketů.

I přesto zůstává formát jednotlivých hlaviček velmi podobný. Klíčová funkcionalita protokolu zůstala nezměněna (CISCO SYSTEMS, Inc., 1992-2014a).

2.3.1 Novinky OSPFv3

1. Protokol pracuje v rámci linku.

   Protože IPv6 užívá k označení média či „prostředníka přenášejícího data" termín „link", pracuje i OSPF nově v rámci linku. Zatímco OSPFv2 připojuje rozhraní k určité síti/subnetu, OSPFv3 jej připojuje k linku. Dvě rozhraní mohou v rámci linku komunikovat, aniž by se nacházely ve společném subnetu. Z toho přímo vyplývá, že více subnetů může sdílet jeden link.

2. Z paketů byly odstraněny adresy.

   Z paketů a klíčových LSA byly jako nesený obsah odstraněny IP adresy. To jinak řečeno znamená, že jádro OSPFv3 je obdobně jako EIGRP nezávislé. To umožnilo zavést do OSPFv3 podporu pro různé „rodiny adres" (Lindem, 2010, s. 4), potažmo i pro jiné protokoly třetí vrstvy, než je IPv6. IP adresy jsou obsaženy pouze v LSU paketech (Link State Update). Router ID, které stejně jako Area ID a Link State ID zůstalo 32bitovou hodnotou, je nově jediným identifikátorem použitelným pro objevování sousedů.

3. Aktualizované rozsahy zaplavování.

   Rozsahy zaplavování (flooding scopes) byly rozděleny podle typu.

   (a) Link-local: LSA je šířeno jen v rámci sdíleného média - linku.

   (b) Area: Zaplavena je pouze oblast, v níž LSA vznikl. Zbytek autonomního systému je vynechán.

   (c) AS: Zaplavení všech oblastí v rámci autonomního systému.

4. Podpora více instancí protokolu na jednom linku.

   Více instancí OSPF může sdílet jeden link. To je umožněno pomocí InstanceID a AreaID obsaženým v OSPF paketech. Link může být součástí jak více autonomních systémů, tak i více oblastí v rámci jednoho AS.

5. Použití lokálních linkových adres.

   Lokální linkové adresy musejí být přiřazeny všem fyzickým rozhraním. Používány jsou k objevování sousedů a automatické konfiguraci. Routery je nepředávají dále, slouží pouze ke komunikaci v rámci jednoho linku (kromě těch virtuálních, kde je potřeba použít globálně unikátní adresu) a k určení next-hop adresy. Linkové adresy jsou obsaženy v Link-local LSA.

6. Změny v autentizaci.

   OSPFv3 nedisponuje žádnou možností autentizace nebo kontroly paketů proti jejich porušení. V autentizaci se OSPF spoléhá na samotný IPv6 protokol, respektive na jeho autentizační hlavičku. Kontrola délky se vypočítává z celého IPv6 paketu na vyšší vrstvě.

7. Změna formátu OSPF paketů.

   Vzhledem k výše popsaným změnám došlo ke změně formátu OSPF paketů a Link State Advertisements. Tyto změny jsou podrobně popsány v následujících sekcích. U LSA nedošlou pouze ke změně formátu, ale také jejich názvů.

8. Zpracovávání neznámých typů LSA.

   Zaplavování se může účastnit i LSA neznámého typu. Zatímco v OSPFv2 by bylo ihned smazáno, v OSPFv3 zprávách přibyl do pole LS type tzv. handling bit (U-bit), který zacházení s neznámým LSA řídí.

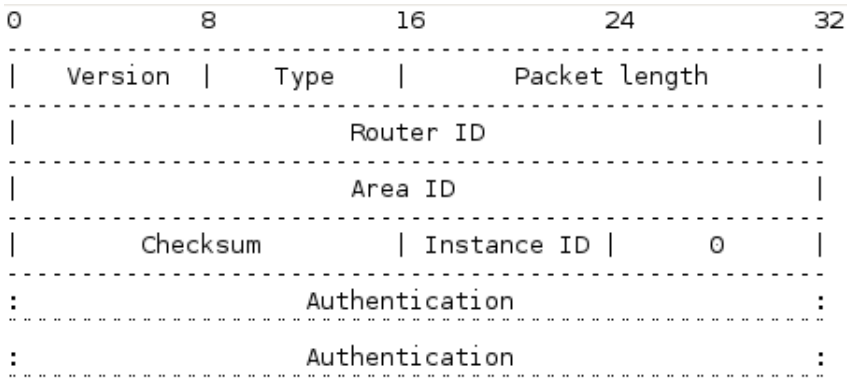
9. Identifikace routerů pomocí RouterID.

   Objevování sousedů identifikuje vždy na základě RouterID, a nezávisle na typu sítě. OSPFv2 používá RouterID pouze u point-to-point spojení, v ostatních typech sítí slouží k identifikaci sousedů IP adresa rozhraní.

(Bhagat, 2010)

2.3.2 OSPF header

Hlavičky základních paketů nijak výraznou změnou neprošly, odstraněna byla dvě pole autentizace a pole určující druh autentizace bylo rozděleno na InstanceID pole a jedno pole pro budoucí využití (Coltun, 2008, s. 60).

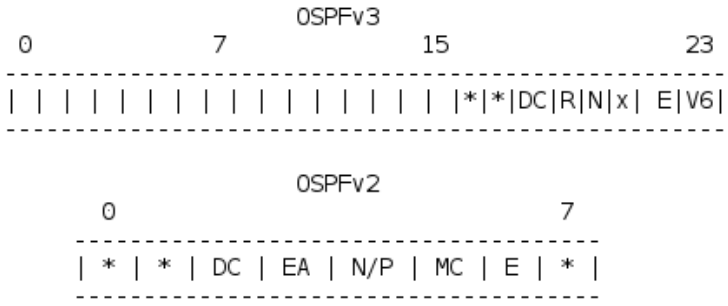


Obrázek 6: OSPF packet header

OSPFv3 nadále používá stejné typy zpráv jako OSPFv2, tedy Hello pakety, Database Description a zprávy informující o stavu linku (LSU, LSR, LSA). Ty prošly dílčí úpravou formátu, zejména co se týče přechodu na identifikaci routerů pomocí jejich ID. Tato práce nezahrnuje podrobnosti o jejich změnách, ty jsou ale dostupné v příslušných RFC dokumentech.

2.3.3 Pole Options

Pole „options", které ovlivňuje navazování sousedností a předávání LSA paketů mezi routery lišícími se úrovní svých schopností například v důsledku rozdílné implementace protokolu, bylo v OSPFv3 značně prodlouženo. V OSPFv2 toto pole nabývá délky osm bitů, z nichž je pouze pět definováno přímo protokolem. Ostatní bity jsou vyhrazeny rozšířením OSPFv2 (Moy, 1998, s. 187).

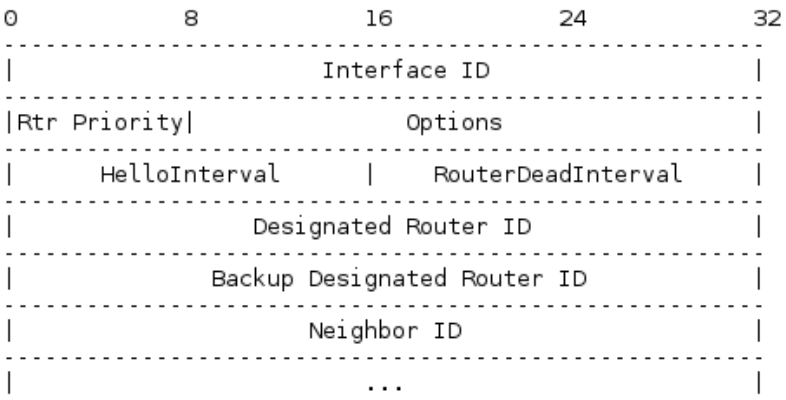


Obrázek 7: Pole options

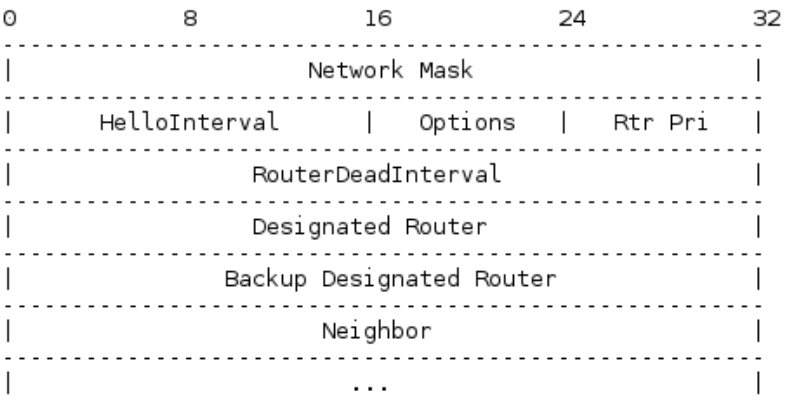
Ve třetí verzi OSPF bylo protokolem definováno šest bitů a další dva byly vyhrazeny pro rozšíření. Celkově bylo ale poli "options" vyhrazeno celých 24 bitů. Většina z nich je tedy momentálně nevyužita a routery by je měly ignorovat. Novinkou je především bit označený jako V6. Ten určuje, zda bude paket použit pro účely routovacího protokolu. Bit X, který odpovídá bitu MC z OSPFv2, je protokolem ignorován. MC bit v OSPFv2 ovlivňuje přeposílání multicastových datagramů, v OSPFv3 je označen jako zastaralý (Coltun, 2008, s. 59).

2.3.4 OSPF Hello paket:

Prakticky všechny typy OSPF zpráv prošly řadou změn, v této práci ale nemá smysl se jimi všemi zabývat. Jako příklad jsou zde uvedeny hello pakety obou zmiňovaných verzí OSPF protokolu, z nichž je jasně vidět odklon od síťových adres k RouterID ale i nové prodloužené pole options (Coltun, 2008, s. 60).



Obrázek 8: OSPFv3 Hello



Obrázek 9: OSPFv2 Hello

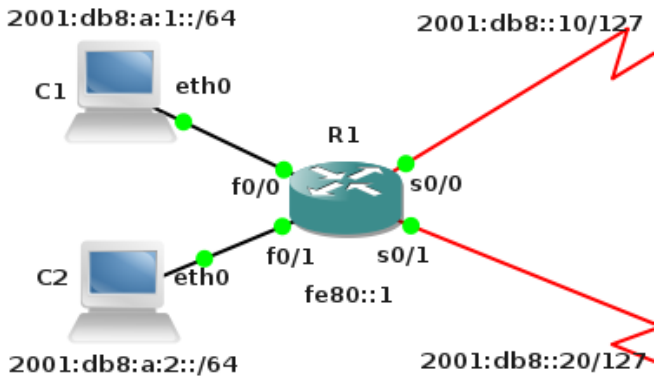
2.3.5 Link State Advertisements

LSA doznali v OSPFv3 řady menších i větších změn. Například výše zmíněné pole options bylo z hlavičky LSA paketů přesunuto přímo do jejich těla, z Router a Network LSA byly odstraněny adresy, několik typů LSA bylo přejmenováno a dva nové byly představeny.

Mezi nově představené patří Link LSA, jehož zaplavovací oblastí je pouze přímo připojený link. Nese informace o linku, rozhraní a na něm nastavených prefixech. Druhým novým LSA typem je Intra-Area-Prefix LSA. Ten nese informace a prefixy, které byly v OSPFv3 odstraněny z Router a Network LSA. Na Inter-Area-Prefix a Inter-Area-Router byly přejmenovány Summary a ASBR-Summary LSA (Stretch, 2010).

3 Konfigurace zařízení Cisco

Nejvýraznější konfigurační změnou, kterou Cisco IOS s podporovou IPv6 přináší, je absence dobře známého příkazu „network". Nastavení routování s IPv6 neprobíhá v rámci sítě, ale v rámci linky neboli rozhraní. Pro zahrnutí více rozhraní do routovacího procesu je tedy zapotřebí povolit libovolný routovací protokol na každém rozhraní zvlášť. Hromadné povolení více rozhraní jedním příkazem již není možné. Další důležitou novinkou je nutnost explicitně povolit samotné routování IPv6 paketů jako takové (CISCO SYSTEMS, Inc., 1992-2014a).



Obrázek 10: Ciso router v GNS3

Následující sekce popisuje základní nastavení Cisco routeru s dvěma lokálními sítěmi a dvěma point-to-point spojeními (viz Obrázek 10) pro různé routovací protokoly s IPv6.

```
R1(config)#ipv6 unicast-routing
```

Explicitní povolení předávání IPv6 paketů. Tento příkaz je nutné zadat ještě před nastavením jakéhokoli routovacího protokolu. Pokus o spuštění routovacího procesu jinak skončí s hlášením „% IPv6 routing not enabled".

```
R1(config)#int s0/0
R1(config-if)#ipv6 add fe80::1 link-local
```

Lokální linková adresa je generována automaticky příkazem „ipv6 enable" nebo při nastavení unikátní adresy. Protože jsou ale linkové adresy užívány v rámci routovacího procesu i jako next-hop adresy, je vhodné používat vlastní čitelné adresy. Vzhledem k jejich platnosti omezené pouze na daný link (spojení), neměl by to být problém.

```
R1(config-if)#ipv6 add 2001:db8::31/127
R1(config-if)#no sh
R1(config-if)#int s0/1
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#ipv6 add 2001:db8::21/127
R1(config-if)#no sh
```

```
R1(config-if)#int f0/0
R1(config-if)#ipv6 add 2001:db8:a:1::1/64
R1(config-if)#no sh
R1(config-if)#int f0/1
R1(config-if)#ipv6 add 2001:db8:a:2::1/64
R1(config-if)#no sh
```

3.0.6 Konfigurace RIPng

```
R1(config)#ipv6 route 2001:db8:a::/48 null0
```

Statická routa pro neexistující podsítě z daného rozsahu. Výhodou všech routovacích protokolů pro IPv6 je, že již ve výchozím nastavené obsahují všechny tzv. „null-interface". Ten slouží jako odchozí interface pro jinak nedostupné sítě, čímž zabraňuje cyklickému předávání paketů v síti se „summary" nebo „default route".

```
R1(config)#ipv6 router rip cisco
R1(config-rtr)#redistribute connected
```

Slovo „cisco" v prvním příkazu znamená název routovacího procesu. Na rozdíl od RIPv2, s RIPng je možné nastavit více instancí routovacího procesu na jednom routeru. Druhý příkaz je možnou náhradou za pasivní rozhraní, které není v RIPng podporováno. V tuto chvíli router ví, že má propagovat prefixy všech rozhraní. Neví ale, která rozhraní se budou na routování účastnit.

```
R1(config-rtr)#int s0/0
R1(config-if)#ipv6 rip cisco enable
R1(config-if)#ipv6 rip cisco summary-address 2001:db8:a::/48
R1(config-if)#int s0/1
R1(config-if)#ipv6 rip cisco enable
R1(config-if)#ipv6 rip cisco summary-address 2001:db8:a::/48
```

Povolení routovacího procesu na sériových rozhraní nastavení sumarizační routy pro lokální sítě. Sumarizaci sítí lze nastavit i bez „redistribute connected", nicméně nebudou mít žádný efekt a lokální sítě nebudou vůbec propagovány.

3.0.7 Konfigurace EIGRP for IPv6

Protože je vnitřní funkcionalita EIGRP univerzální, nezměnil se ani způsob určení router ID, které je stále 32 bitovou hodnotou. ID je nutné definovat v konfiguračním režimu EIGRP. Samotnout instanci EIGRP je v nově potřeba aktivovat příkazem „no sh".

```
R1(config)#ipv6 route 2001:db8:a::/48 null0
R1(config)#ipv6 router eigrp 100
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#no sh
```

```
R1(config-rtr)#passive-interface f0/0
R1(config-rtr)#passive-interface f0/1
R1(config-if)#int f0/0
R1(config-if)#ipv6 eigrp 100
R1(config-if)#int f0/1
R1(config-if)#ipv6 eigrp 100
```

EIGRP stále disponuje možností nastavit rozhraní jako pasivní, tato rozhraní lze tedy klasicky zahrnout do routovacího procesu bez toho, aby z nich byly odesílány Hello nebo jiné pakety související s routovacím procesem.

```
R1(config-if)#int s0/0
R1(config-if)#ipv6 eigrp 100
R1(config-if)#ipv6 summary-address eigrp 100 2001:db8:a::/48
R1(config-if)#int s0/1
R1(config-if)#ipv6 eigrp 100
R1(config-if)#ipv6 summary-address eigrp 100 2001:db8:a::/48
```

3.0.8 Konfigurace OSPFv3

```
R1(config)#ipv6 router ospf 100
R1(config-rtr)#router-id 3.3.3.3
R1(config-rtr)#passive-interface f0/0
R1(config-rtr)#passive-interface f0/1
```

Co se určení router ID a pasivních rozhraní týče, platí pro OSPF stejná pravidla jako pro EIGRP. Pokud se OSPF nepodaří úspěšně určit své router ID, končí s hláškou „OSPFv3 process 100 could not pick a router-id, please configure manually".

```
R1(config-rtr)#int f0/0
R1(config-if)#ipv6 ospf 100 area 0
R1(config-if)#int f0/1
R1(config-if)#ipv6 ospf 100 area 0
R1(config-if)#int s0/0
R1(config-if)#ipv6 ospf 100 area 0
R1(config-if)#int s0/1
R1(config-if)#ipv6 ospf 100 area 0
```

Protože OSPF implementuje sumarizaci pouze na hranicích oblastí a autonomních systémů, nemá význam se jimi v této síti zabývat. Můžeme nicméně zmínit, že v syntaxi jejich nastavení nedošlo oproti předchozí verzi OSPF k žádné změně.

4 Praktické úlohy

Praktické testovací úlohy mají za úkol popsat chování jednotlivých routovacích protokolů a porovnat rozdíly v tomto chování vzhledem k použitému protokolu síťové vrstvy. Tyto úlohy jsou vypracovány na dvou zkušebních topologiích charakterizujících rozdílné typy sítí, přičemž jsou obě topologie vybudovány tak, aby bylo možné pokusy provést jak na dostupných Cisco routerech, tak ve speciálním simulátoru počítačových sítí GNS3.

4.1 Síťová laboratoř

Vzhledem k nízkému počtu routerů s více než dvěma sériovými porty jsou obě testovací topologie navrženy tak, aby je bylo možné sestavit jen s použitím routerů disponujících právě dvěma sériovými a dvěma ethernetovými rozhraními. Další skutečnosti, které ovlivnily průběh pokusů s reálnými zařízeními, jsou počet routerů a stav podpory síťového protokolu IPv6 a routovacích protokolů RIPng, OPSFv3 a EIGRP for IPv6.

Protože jsou navržené topologie pro účel zkoumání zbytečně rozsáhlé, byly z výše popsaných důvodů testovány pouze vybrané části z obou topologií, které jsou popsány v následujících kapitolách. K praktickým úlohám byly použity dále popsané routery.

- Cisco IOS Software, 2801 Software (C2801-ADVIPSERVICESK9-M), Version 12.4 (16b), RELEASE SOFTWARE (fc3)

    - Cisco 2801 (revision 7.0) with 116736K/14336K bytes of memory. Processor board ID FCZ131811YW 2 FastEthernet interfaces 2 Low-speed serial(sync/async) interfaces 1 Virtual Private Network (VPN) Module DRAM configuration is 64 bits wide with parity disabled. 191K bytes of NVRAM. 62720K bytes of ATA CompactFlash (Read/Write).

- Cisco IOS Software, 2800 Software (C2800NM-IPVOICE_IVS-M), Version 15.0(1) M9, RELEASE SOFTWARE (fc1)

    - Cisco 2811 (revision 53.50) with 245760K/16384K bytes of memory. Processor board ID FCZ131820LY 2 FastEthernet interfaces 2 Serial (sync/async) interfaces 1 terminal line 1 cisco Integrated Service Engine(s) Cisco WLAN Controller 5.2.178.0 in slot 1 DRAM configuration is 64 bits wide with parity enabled. 239K bytes of non-volatile configuration memory. 62720K bytes of ATA CompactFlash (Read/Write).

4.2 Graphical Network Simulator 3

Graphical Network Simulator 3, zkráceně GNS3, je multiplatformní svobodný nástroj vycházející pod licencí GNU GPL určený pro simulaci síťových a koncových zařízení. GNS3 funguje jako uživatelské prostředí propojující jinak nezávislé komponenty do komplexního simulátoru (Documentation, 2007-2014). Součástmi GNS3 jsou či mohou být

- Cisco IOS emulátor Dynamips,
- emulátor platforem x86 a amd64/Intel64 Oracle VirtualBox,
- pokročilý emulátor Qemu.

4.2.1 Dynamips

Dynamips je klíčovou součástí GNS3. Na rozdíl od Cisco Packet Traceru, který implementuje pouze část funkcionality Cisco routerů, je GNS3 téměř úplnou substitucí reálné sítě, za což vděčí právě Dynamipsu. Dynamips je emulátor vybraných modelových řad Cisco routerů a jsou v něm spouštěny originální Cisco IOS image. GNS3 tedy spouští virtuální verzi reálných zařízení Cisco.

Dynamips vytvořil v létě roku 2005 Christophe Fillot na University of Tennessee jako emulátor modelové řady routerů 7200, nicméně jeho vývoj byl zastaven v roce 2007 po vydání verze 0.2.8-RC2. Později byl znovuobnoven v rámci projektu GNS3. V současnosti jsou podporovány řady 1700, 2600, 3600, 3700, a 7200.

4.2.2 Oracle VirtualBox

Známý virtualizační nástroj proslulý snadnou uživatelskou obsluhou. Původně dílo společnosti Sun Microsystems, po jejímž odkoupení připadl korporaci Oracle. VirtualBox, který taktéž vychází pod licencí GNU GPL, má v rámci GNS3 na starosti virtualizaci desktopových a serverových stanic a síťových zařízení Juniper s operačním systémem JunOS.

4.2.3 Qemu

Emulátor schopný virtualizovat mnoho instrukčních sad včetně PowerPC, SPARC a ARM. Často se objevuje jako součást pokročilých virtualizačních řešení, jako jsou XEN a KVM. Umožněje virtualizovat hardware jak pro celé operační systémy, tak zamostatné uživatelské programy. V GNS3 v něm mohou běžet firewally Cisco ASA, PIX a IPS

4.3 Metodika a scénář pokusů

4.3.1 Metodika

Při praktickém měření byla zkoumána rychlost konvergence jednotlivých routerů a vytížení jejich rozhraní v souvislosti s tímto procesem. Zkoumání rychlosti, s jakou se router

přizpůsobí probíhajícím změnám v síti, vycházejí z informací generovaných ladícím režimem routovacího procesu. Ten poskytuje standardizované informace o změnách prováděných v routovací tabulce nezávisle na použitém routovacím protokolu.

Množství síťového provozu neboli režie spojená s použitými protokoly byla zkoumána studiem rámců zachycených analyzátorem síťového provozu Wireshark (dříve známý jako Ethereal) na rozhraních vybraných routerů z obou topologií. Dále byly zkoumány také samotné informace, kterými routovací protokoly plnily routovací tabulky všech routerů. K tomuto účelu posloužily široce známé příkazy operačního systému Cisco IOS.

4.3.2 Scénář

Provedené pokusy vycházejí ze situace, která může snadno nastat v libovolné reálné síti. Pro zkoumání doby reakce na změnu v síti je simulována krátkodobá nefunkčnost jednoho z routerů. Doba, po kterou je router nedostupný, se pohybuje v řádech jednotek až desítek sekund. Výpadek je simulován vypnutím daného routeru popřípadě vypnutím všech jeho rozhraní.

Zkoumány jsou výpisy debugovacího režimu v konzoli systému IOS a pakety zachycené na rozhraních, přičemž nás zajímají především délky intervalů mezi první a poslední změnou v routovacích tabulkách a množství a délka paketů zachycených během konvergování sítě.

Následující sekce popisují testované topologie, jejich charakteristiky a chování v závislosti na použitém síťovém a routovacím protokolu. Jsou zde umístěny naměřené hodnoty pro každou topologii a jejich porovnání vzhledem k daným protokolům.

4.4 Hierarchická topologie

První z testovacích topologií představuje čtyřvrstvou hierarchii s celkem devíti routery. Router na vrcholu této hierarchie by mohl představovat například bránu do internetu, v důsledku čehož by v reálném nasazení s největší pravděpodobností disponoval největším výpočetním výkonem a nejlepší konektivitou. Protože je předmětem zkoumání vliv použitého síťového protokolu, nejsou tyto aspekty v simulacích zohledněny.

První tři vrstvy, které lze považovat za kombinaci jádra a distribuční vrstvy sítě, jsou propojeny primárními sériovými linkami. Přístupová vrstva tvořená čtyřmi routery na nejnižší úrovni hierarchie je připojena pouze za pomoci ethernetu. Každý router této vrstvy, společně s dvěma hraničními routery distribuční vrstvy, představují bránu do zbytku sítě pro vlastní lokální sítě.

4.4.1 Adresní plán

IPv4

K adresování této topologie jsou použity privátní rozsahy 10.0.0.0/8 a 172.16.0.0/12. Podsítě prvního rozsahu jsou přiděleny lokálním koncovým sítím, přičemž každý router disponuje vlastním rozsahem s prefixem /16 s 65536 možnými adresami. To, ve spojení s rozhraním „null", umožňuje routerům propagovat ručně sumarizované routy. Automatická sumarizace je na všech routerech deaktivována.

Podsítě druhého rozsahu jsou použity pro adresování point-to-point spojení. Celkem pět podsítí s prefixem /30 z rozsahu 172.16.0.0/24 je použito pro adresování sériových linek. Pro adresování ethernetových linek mezi routery je použito šest podsítí sítí s prefixem /30 z rozsahu 172.16.1.0/24.

Celkem podsítí	*První podsíť*	*Poslední podsíť*	*Použití*
5	172.16.0.0/30	172.16.0.16/30	sériové linky
6	172.16.1.0/30	172.16.1.20/30	ethernetové linky
2	10.1.1.0/24	10.1.2.0/24	lokální sítě R4
2	10.2.1.0/24	10.2.2.0/24	lokální sítě R5
2	10.3.1.0/24	10.3.2.0/24	lokální sítě R6
2	10.4.1.0/24	10.4.2.0/24	lokální sítě R7
2	10.5.1.0/24	10.5.2.0/24	lokální sítě R8
2	10.6.1.0/24	10.6.2.0/24	lokální sítě R9

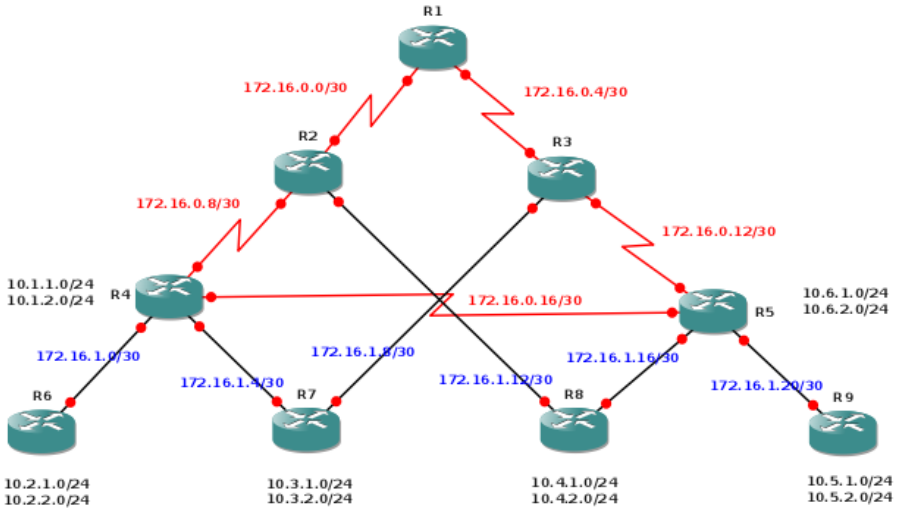
Tabulka 7: IPv4 v hierarchicke topologii

IPv6

Adresace IPv6 se nese v podobném duchu jako u IPv4, přičemž je jako základ použit dokumentační prefix 2001:db8::/32. Pro adresování point-to-point spojení jsou v souladu s RFC 6164 použity prefixy s délkou 127 bitů. Použité rozsahy adres jsou i zde navrženy tak, aby bylo možné intuitivním způsobem využít ruční sumarizace rout.

Celkem podsítí	*První podsíť*	*Poslední podsíť*	*Použití*
5	2001:db8::10/127	2001:db8::50/127	sériové linky
6	2001:db8::60/127	2001:db8::b0/127	ethernetové linky
2	2001:db8:1:1::/64	2001:db8:1:2::/64	lokální sítě R4
2	2001:db8:2:1::/64	2001:db8:2:2::/64	lokální sítě R5
2	2001:db8:3:1::/64	2001:db8:3:2::/64	lokální sítě R6
2	2001:db8:4:1::/64	2001:db8:4:2::/64	lokální sítě R7
2	2001:db8:5:1::/64	2001:db8:5:2::/64	lokální sítě R8
2	2001:db8:6:1::/64	2001:db8:6:2::/64	lokální sítě R9

Tabulka 8: IPv6 v hierarchické topologii



Obrázek 11: Hierarchická topologie

4.4.2 Popis pokusu

V této topologii je simulován výpadek routeru R5. Pro určité části sítě to znamená přesměrování přes router R4, výpadek alternativní routy, ale i naprostou nedostupnost. Zkoumány jsou zde routovací protokoly z rodiny protokolů s vektorem vzdálenosti RIP a EIGRP. OSPF nebyl v této topologii zahrnut z toho důvodu, že umožňuje sumarizaci rout pouze na tzv. Area Border Routerech, tedy na hraních „oblastí", s nimiž tato topologie nepočítá.

4.4.3 Výsledky pokusů

Dále uvedené hodnoty popisují rychlost konvergence jednotlivých routerů v testovaných topologiích během malého vzorku vybraných pokusů. Z celkem dvou až třínásobku pokusů, které byly v simulátoru GNS3 skutečně vypracovány, je zde zmíněno 5. V těchto pěti vybraných pokusech jsou nicméně obsaženy nejtypičtější hodnoty, které se napříč všemi pokusy objevovaly.

Lze namítat, že takto omezený výběr zkresluje vypovídající hodnotu pokusů, to nicméně platí pouze pro pokusy provedené v simulátoru. Při testování na reálných zařízeních bylo totiž zjištěno, že naměřené hodnoty dosahují i při malém množství pokusů velmi stálých hodnot. Stabilních výsledků bylo v laboratoři dosaženo i při namátkovém zvýšení počtů pokusů.

RIP - konvergence

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	4.	6.	7.	10.	**průměr**
R1	4.592	10.308	5.384	11.72	9.564	**8,314**
R2	23.72	25.176	27.432	26.096	26.496	**25,784**
R3	35.496	28.32	32.056	30.456	35.24	**32,314**
R4	36.0	45.924	36.224	38.584	36.364	**38,619**
R6	3.268	8.3	7.292	8.416	4.524	**6,36**
R7	7.336	8.32	7.272	8.428	4.5	**7,171**
R8	44.72	43.592	39.736	43.776	38.864	**42,138**
R9	44.7	43.604	39.7	43.764	38.868	**42,127**

Tabulka 9: konvergence RIPv2

	Pokusy (uvedené časy v jednotkách sekund)					
						průměr
R1	22.052	18.436	20.808	22.088	19.876	**20,652**
R2	18.772	18.628	15.864	17.78	15.052	**17,219**
R3	25.864	29.384	29.332	26.6	29.34	**28,104**
R4	16.156	11.228	16.804	14.428	17.536	**15,23**
R6	14.98	13.14	8.98	8.704	12.504	**11,662**
R7	27.068	27.276	28.744	26.296	27.992	**27,475**
R8	19.468	17.144	15.016	15.056	20.04	**17,345**
R9	27.02	27.224	28.6	27.68	27.892	**27,683**

Tabulka 10: konvergence RIPng

K výběru „typicky" vyhlížejících hodnot bylo přistoupeno z toho důvodu, že dosáhnout stabilních hodnot je s použitím simulátoru téměř nemožné. Routery se musí dělit o společný výpočetní výkon nejenom mezi sebou, ale i s operačním systémem, na němž simulátor běží.

V simulátoru je každému routeru dostupný pouze zlomek výkonu, kterým disponuje router skutečný. Svou roli hraje i operační systém a jeho plánovač procesů. Hodnoty naměřené v simulátoru je tedy nutno brát z rezervou a slouží pouze pro srovnání s hodnotami naměřenými v laboratoři.

Svou hodnotu nicméně tato data mají. Poměrně překvapivá informace totiž vyplývá již z předešlých dvou tabulek. Ačkoli to může být poměrně překvapující, většina routerů zkonvergovala rychleji s použitím IPv6 a RIPng.

EIGRP - konvergence

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	2.	3.	4.	5.	průměr
R1	13.804	13.592	13.58	13.732	13.7	**13,682**
R2	13.588	13.544	13.536	13.544	13.64	**13,57**
R3	13.496	13.44	13.472	13.436	13.396	**13,448**
R4	13.452	13.46	13.54	13.532	13.424	**13,482**
R6	13.964	13.436	13.424	13.404	13.276	**13,501**
R7	13.888	13.44	13.448	13.416	13.284	**13,495**
R8	13.472	13.516	13.516	13.368	13.328	**13,44**
R9	13.324	13.34	13.36	13.284	13.228	**13,307**

Tabulka 11: konvergence EIGRP pro IPv4

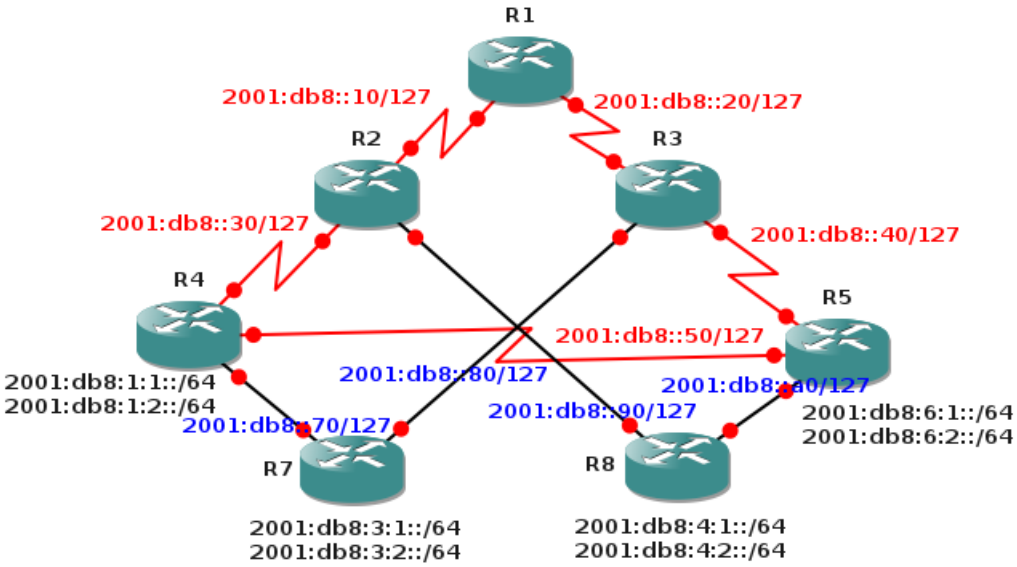
Náskok EIGRP pro IPv6 není nijak výrazný, přesto lze tvrdit, že i zde většina routerů konvergovala o zhruba sekundu rychleji než s IPv4.

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	3.	6.	9.	10.	průměr
R1	10.692	14.112	13.592	14.968	10.164	**12,706**
R2	14.972	14.74	14.268	14.928	14.604	**14,702**
R3	14.912	14.684	14.192	14.904	14.516	**14,642**
R4	13.992	14.72	14.26	15.764	11.632	**14,074**
R6	12.152	12.956	11.412	10.368	11.048	**11,587**
R7	5.424	12.972	12.344	10.392	11.012	**10,429**
R8	12.24	12.976	12.416	10.432	11.164	**11,846**
R9	11.984	13.484	11.092	12.076	13.384	**12,404**

Tabulka 12: konvergence EIGRP pro IPv6

4.4.4 Výsledky pokusů v laboratoři

Hodnoty získané v laboratoři potvrzují trend nastolený u předešlých měření. V podstatě všechny routery konvergovaly v laboratoři podstatně rychleji při použití protokolu IPv6, než při použití IPv4 a příslušných verzí zkoumaných routovacích protokolů.



Obrázek 12: Hierarchická topologie v laboratoři

RIP - konvergence

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	2.	3.	4.	5.	průměr
R1	3.96	0.588	0.068	1.036	3.832	**7,3**
R2	5.988	3.432	2.988	2.988	2.276	**7,352**
R3	29.304	29.996	32.108	29.932	28.632	**7,641**
R8	29.372	31.156	32.128	30.696	28.652	**7,501**
R9	6.952	0.968	0.976	0.976	2.092	**7,507**
R10	29.34	31.56	32.088	30.648	28.608	**7,66**

Tabulka 13: konvergence RIPv2

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	2.	3.	4.	5.	průměr
R1	4.996	4.996	4.996	4.996	4.996	**1,648**
R2	5.0	5.0	5.0	5.0	5.0	**1,626**
R3	7.02	7.02	7.016	7.02	7.016	**4,341**
R8	3.084	3.084	3.084	3.084	3.08	**4,407**
R9	10.0	10.0	10.004	10.0	10.0	**1,622**
R10	5.004	5.0	5.0	5.0	5.0	**5,001**

Tabulka 14: konvergence RIPng

Částečně lze doslova propastný rozdíl mezi pokusy s IPv4 a IPv6 zdůvodnit routery použitými v laboratořích. Zatímco většina měření probíhala s výkonnými routery ze série Security s nejnovějším operačním systémem Cisco IOS 15, měření protokolu RIPv2 probíhalo se staršími zařízeními ve vedlejší laboratoři.

Důvodem byla chyba v ladícím režimu RIPu v IOS 15, v němž jsou namísto změn routovací tabulky vypisovány veškeré události protokolu RIP, včetně všech přijatých a odesílaných zpráv. Touto chybou, která způsobuje nekonečnou záplavu informací, která činí monitorování routovací tabulky nemožným, nejsou starší verze IOSu postiženy.

EIGRP - konvergence

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	**2.**	**3.**	**4.**	**5.**	**průměr**
R1	6,416	9,912	6,744	7,292	6,136	**7,3**
R2	6,472	9,936	6,86	7,32	6,172	**7,352**
R3	8,14	9,884	6,804	7,26	6,116	**7,641**
R8	7,632	9,88	6,628	7,256	6,108	**7,501**
R9	7,636	9,84	6,772	7,22	6,068	**7,507**
R10	7,588	10,072	6,896	7,444	6,3	**7,66**

Tabulka 15: konvergence EIGRP pro IPv4

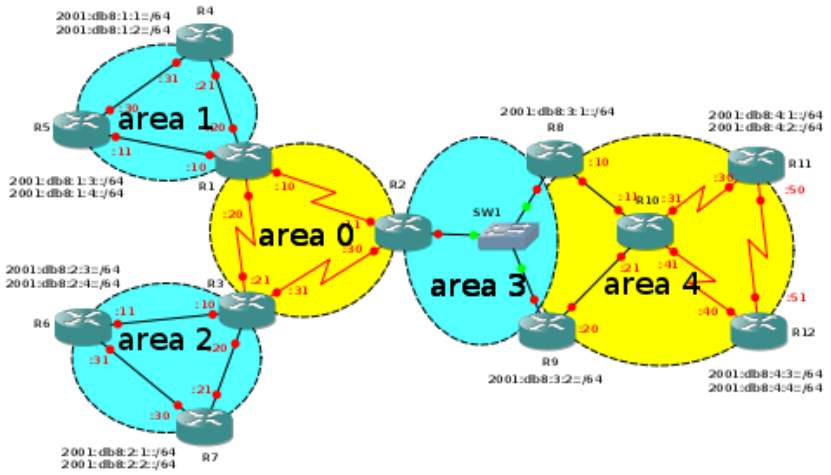
	Pokusy (uvedené časy v jednotkách sekund)					
	1.	**2.**	**3.**	**4.**	**5.**	**průměr**
R1	1,376	1,364	2,148	1,368	1,984	**1,648**
R2	1,332	1,328	2,16	1,336	1,976	**1,626**
R3	4,392	4,388	4,4	4,392	4,132	**4,341**
R8	4,436	4,432	4,436	4,432	4,3	**4,407**
R9	1,356	1,356	2,14	1,364	1,896	**1,622**
R10	5,004	5	5	5	5	**5,001**

Tabulka 16: konvergence EIGRP pro IPv6

4.5 Topologie s oblastmi

Pro druhý experiment byla použita topologie rozdělující autonomní systém do několika oblastí. Ta byla navržena speciálně pro routovací protokol OSPF, který byl z předešlého experimentu vyloučen právě pro svůj koncept síťových oblastí. Topologie se skládá z celkem čtyř koncových oblastí a z oblasti páté tvořící páteř sítě (backbone).

Úkolem páteřní oblasti je spojit oblasti koncové a směrovat výhradně mezi nimi, v tomto případě se skrz ni tedy šíří pouze sumarizované routy. Dle standardu je jí v OSPF vyhrazen identifikátor 0 a každá koncová síť v ní musí mít minimálně jedno rozhraní. Z pohledu na obrázek autonomního systému ale jasně vyplývá, že tento požadavek není splněn pro oblast 4. Ta je ale k páteři připojena dvěma virtuálními linky, které oba ústí v routeru R2.



Obrázek 13: Topologie s oblastmi

Pro srovnání s OSPF byl v této topologii dále testován i protokol EIGRP. V něm bylo taktéž využito konceptu oblastí, ale protože pro ně EIGRP neimplementuje žádnou podporu, bylo ho dosaženo manuální sumarizací na rozhraních „hraničních" routerů. Sumarizované routy jsou v EIGRP identické jako v OSPF.

4.5.1 Popis pokusu

V této topologii byl simulován výpadek routeru R2, který síť fyzicky rozděluje na dvě poloviny. S EIGRP jsou během výpadku vzájemně dostupné všechny „oblasti", které jsou přímo či nepřímo fyzicky propojeny. S OSPF spolu mohou komunikovat pouze oblasti 1 a 2. Zbylé dvě oblasti, ačkoli jsou propojeny hned dvěma routery, nemohou komunikovat ani mezi sebou, ani s žádnou jinou oblastí.

To proto, že v OSPF probíhá komunikace mezi oblastmi výhradně skrze oblast páteřní, v níž oblasti 3 a 4 nemají během výpadku R2 žádné rozhraní. Na rozdíl od EIGRP, které má během konvergence za úkol pouze rozšíření sumarizovaných rout do znovu dostupných sítí, OSPF kromě toho musí provést i znovuustavení virtuálních linků.

4.5.2 Adresní plán pro IPv4 a IPv6

Každé oblasti je v této topologii přidělen samostatný 16bitový prefix z privátního rozsahu 10.0.0.0/8. V každé oblasti jsou až 4 koncové sítě s prefixem /24, prefix s nulami v posledním oktetu je ve všech oblastech použit pro adresování point-to-point spojení. Ručně sumarizované routy mají délku právě 16 bitů.

oblast	*summary*	obslužné sítě		koncové sítě	
area 0	10.0.0.0/16	10.0.0.0/30	10.0.0.8/30		
		10.0.0.4/30			
area 1	10.1.0.0/16	10.1.0.0/30	10.1.0.8/30	10.1.1.0/24	10.1.3.0/24
		10.1.0.4/30		10.1.2.0/24	10.1.4.0/24
area 2	10.2.0.0/16	10.2.0.0/30	10.2.0.8/30	10.2.1.0/24	10.2.3.0/24
		10.2.0.4/30		10.2.2.0/24	10.2.4.0/24
area 3	10.3.0.0/16	10.3.0.0/29		10.3.1.0/24	10.3.2.0/24
area 4	10.4.0.0/16	10.4.0.0/30	10.4.0.12/30	10.4.1.0/24	10.4.3.0/24
		10.4.0.4/30	10.4.0.16/30	10.4.2.0/24	10.4.4.0/24
		10.4.0.8/30			

Tabulka 17: IPv4 v topologii s oblastmi

Pro IPv6 je opět použit dokumentační prefix 2001:db8::/32. Každá oblast má přiřazen vlastní prefix o délce 48 bitů, který je jako sumarizační routa propagován celým autonomním systémem. Pro adresování point-to-point spojů jsou opět použity prefixy /127.

oblast	*summary*	obslužné sítě	koncové sítě
area 0	2001:db8::/48	2001:db8::10/127	
		2001:db8::20/127	
		2001:db8::30/127	
area 1	2001:db8:1::/48	2001:db8:1::10/127	2001:db8:1:1::/64
		2001:db8:1::20/127	2001:db8:1:2::/64
		2001:db8:1::30/127	2001:db8:1:3::/64
			2001:db8:1:4::/64
area 2	2001:db8:2::/48	2001:db8:2::10/127	2001:db8:2:1::/64
		2001:db8:2::20/127	2001:db8:2:2::/64
		2001:db8:2::30/127	2001:db8:2:3::/64
			2001:db8:2:4::/64
area 3	2001:db8:3::/48	2001:db8:3::/64	2001:db8:3:1::/64
			2001:db8:3:2::/64
area 4	2001:db8:4::/48	2001:db8:4::10/127	2001:db8:4:1::/64
		2001:db8:4::20/127	2001:db8:4:2::/64
		2001:db8:4::30/127	2001:db8:4:3::/64
		2001:db8:4::40/127	2001:db8:4:4::/64
		2001:db8:4::50/127	

Tabulka 18: IPv4 v topologii s oblastmi

4.5.3 Výsledky pokusu

EIGRP - konvergence

	Pokusy (uvedené časy v jednotkách sekund)					
						průměr
R1	3.36	3.364	3.384	1.392	3.596	**3,019**
R3	10.056	10.012	10.052	10.032	10.024	**10,035**
R4	0.0	0.004	1.9	0.156	0.004	**0,413**
R5	10.08	10.06	10.064	10.068	10.052	**10,065**
R6	5.568	4.372	4.596	3.628	3.348	**4,302**
R7	0.008	0.012	1.932	0.112	0.012	**0,415**
R8	16.544	15.336	16.112	16.112	15.532	**15,927**
R9	0.0	0.016	0.012	0.004	0.008	**0,008**
R10	13.44	16.196	10.104	11.64	17.612	**13,798**
R11	16.576	15.404	16.136	16.124	15.58	**15,964**
R12	9.58	9.624	9.572	9.56	9.584	**9,584**

Tabulka 19: konvergence EIGRP pro IPv4

	Pokusy (uvedené časy v jednotkách sekund)					
	3.	**4.**	**5.**	**8.**	**10.**	**průměr**
R1	7.308	6.428	5.092	5.464	4.588	**5,776**
R3	8.856	8.46	8.572	3.924	8.664	**7,695**
R4	2.02	4.892	2.196	1.252	1.56	**2,384**
R5	5.824	6.4	6.76	1.348	8.592	**5,785**
R6	5.988	4.848	3.536	3.92	4.504	**4,559**
R7	4.716	1.008	5.556	0.056	1.596	**2,586**
R8	10.632	16.668	12.904	13.136	13.224	**13,313**
R9	17.436	14.524	13.048	14.088	15.704	**14,96**
R10	15.736	17.516	15.668	18.148	12.616	**15,937**
R11	10.584	14.532	12.964	11.248	13.176	**12,501**
R12	17.468	14.552	13.048	14.136	14.192	**14,679**

Tabulka 20: konvergence EIGRP pro IPv6

OSPF - konvergence

Hodnoty naměřené v simulátoru jsou sice poměrně stabilní, hlavně pokud se budeme zabývat pouze hodnotami jednotlivých routerů s použitím jednoho protokolu. Nicméně pokud začneme srovnávat hodnoty s IPv4 a IPv6, všimneme si velmi podivných rozdílů hlavně u routerů R5,R6 a R7.

	Pokusy (uvedené časy v jednotkách sekund)					
						průměr
R1	10.052	10.016	10.056	10.024	15.552	**11,14**
R3	15.124	15.468	12.092	15.072	15.532	**14,658**
R4	10.028	10.072	10.068	10.04	10.056	**10,053**
R5	9.988	10.068	10.04	10.004	10.072	**10,034**
R6	10.056	10.056	10.036	10.056	10.04	**10,049**
R7	10.044	10.036	10.044	10.032	10.024	**10,036**
R8	0.004	0.0	0.0	0.004	0.0	**0,002**
R9	0.008	0.004	0.004	0.0	0.008	**0,005**
R10	9.576	9.56	9.604	9.532	9.58	**9,57**
R11	9.624	9.552	9.588	9.564	9.596	**9,585**
R12	9.564	9.544	9.6	9.616	9.568	**9,578**

Tabulka 21: konvergence EIGRP pro IPv4

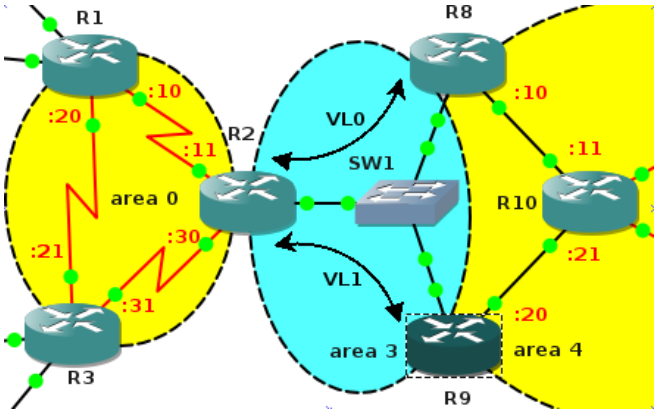
Ostatní routery nicméně disponují poměrně podobnými hodnotami jednou ve prospěch IPv4, podruhé ve prospěch IPv6. Lze tedy říci, že na hodnotách naměřených s použitím simulátoru zde není vhodné vytvářet jakékoli závěry. Za tímto účelem je vhodnější použít hodnoty z měření v laboratoři, které nabývají i při srovnání velmi podobných hodnot.

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	**5.**	**6.**	**7.**	**8.**	**průměr**
R1	25.136	15.076	10.008	15.52	15.124	**16,173**
R3	15.516	10.824	15.472	15.1	15.088	**14,4**
R4	9.988	9.988	9.992	10.004	10.008	**9,996**
R5	0.004	0.004	0.012	0.008	0.0	**0,006**
R6	0.008	0.008	0.004	0.02	0.004	**0,009**
R7	0.004	0.02	0.0	0.004	0.004	**0,006**
R8	20.04	20.988	20.06	20.044	10.02	**18,23**
R9	20.088	10.02	20.088	20.024	20.06	**18,056**
R10	4.556	4.532	14.588	14.564	10.632	**9,774**
R11	4.556	14.64	4.604	14.604	4.564	**8,594**
R12	14.616	4.644	14.592	4.56	14.572	**10,597**

Tabulka 22: konvergence EIGRP pro IPv6

4.5.4 Výsledky pokusů v laboratoři

Při pokusu na reálných zařízeních byly v této topologii z větší části zanedbány oblasti 1, 2 a 4. Tato zmenšená topologie se zaměřuje především na nutnou páteř sítě a oblasti 3 a 4, v nichž participují virtuální linky. V síti jsou nicméně stále propagovány všechny oblasti.



Obrázek 14: Topologie s oblastmi v laboratoři

EIGRP - konvergence

Na reálných zařízeních v laboratoři nabývají naměřené hodnoty opět stabilních hodnot. Jejich vypovídající hodnota je tedy vyšší než při měření v simulátoru GNS3 a mnohem věrněji popisují chování routerů a vliv použitých protokolů.

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	2.	3.	4.	5.	průměr
R1	33.912	33.556	34.808	32.884	32.424	**33,517**
R2	35.5	36.752	34.832	34.372	34.592	**35,21**
R3	33.904	33.54	34.792	32.88	32.42	**33,507**
R8	2.028	2.036	2.032	2.072	2.044	**2,042**
R9	2.016	2.032	2.024	2.016	2.032	**2,024**
R10	0.016	0.004	0.012	0.024	0.016	**0,014**

Tabulka 23: konvergence EIGRP pro IPv4

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	2.	3.	4.	5.	průměr
R1	27.972	28.804	30.492	32.104	32.732	**30,421**
R2	29.912	30.744	30.432	30.048	30.668	**30,361**
R3	27.956	28.792	30.484	32.092	32.716	**30,408**
R8	2.06	2.04	2.016	2.02	2.016	**2,03**
R9	2.036	2.068	2.016	2.016	2.016	**2,03**
R10	1.992	1.996	0.012	0.012	0.012	**0,805**

Tabulka 24: konvergence EIGRP pro IPv6

Jak vyplývá z hodnot v tabulkách, jsou naměřené časy s IPv4 i IPv6 velmi podobné, avšak EIGRP pro IPv6 opět často konvergoval s náskokem až několika sekund.

OSPF - konvergence

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	2.	3.	4.	5.	průměr
R1	68,416	78,172	69,424	68,444	68,6	**70,611**
R2	63,392	73,148	64,396	63,42	63,572	**65,586**
R3	68,4	73,152	69,404	68,432	68,58	**69,594**
R8	25,016	35,016	25,016	25,02	25,012	**27,016**
R9	20,456	35,02	25,02	25,02	25,02	**26,107**
R10	14,548	19,972	14,548	14,552	14,544	**15,633**

Tabulka 25: konvergence OSPFv2

	Pokusy (uvedené časy v jednotkách sekund)					
	1.	2.	3.	4.	5.	průměr
R1	64.02	64.852	68.236	60.86	61.936	**63,981**
R2	60.792	61.636	65.02	58.236	58.28	**60,793**
R3	63.924	64.76	68.148	60.764	61.86	**63,891**
R8	25.012	25.012	25.012	35.012	25.016	**27,013**
R9	25.008	25.008	25.008	20.012	25.008	**24,009**
R10	12.836	12.836	12.344	10.004	13.308	**12,266**

Tabulka 26: konvergence OSPFv3

Stejně jako pro EIGRP, platí i pro OSPF tvrzení, že časy při použití IPv4 i IPv6 jsou téměř identické. Nicméně zas a znovu jsou zde rozdíly v řádech jednotek sekund a opět ve prospěch IPv6.

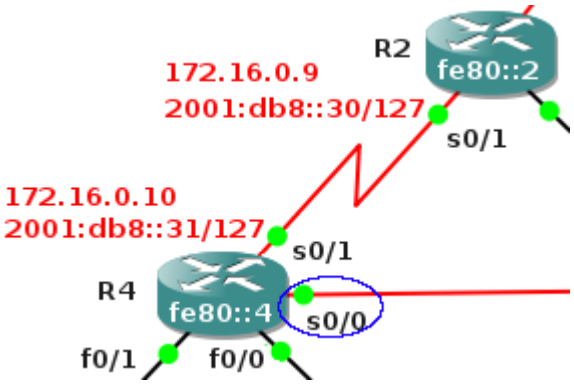
Na základě předešlých pokusů bychom mohli opatrně vyslovit hypotézu, že ačkoli IPv6 přináší vyšší požadavky na výkon, zkracuje dobu konvergence sítě. Tuto hypotézu by nicméně bylo nutné ověřit několikanásobně vyšším počtem pokusů na skutečně funkční síti s reálným provozem během dlouhodobého monitorování této sítě.

Na základě předešlých hodnot bohužel nelze s jistotou prohlásit, že nasazení IPv6 jednoznačně přináší zrychlení procesu konvergence. Nicméně z informací zjištěných v této kapitole jednoznačně vyvstává otázka, zda tomu tak může být. Tuto, řekněme hypotézu, by bylo vhodné ověřit dlouhodobým sledováním reálné sítě zatíženou skutečným provozem.

5 Vytížení rozhraní

Tato kapitola se zabývá rozdíly v objemu dat, které router přijme a odešle během konvergence sítě. Jsou zde zkoumány rozdíly v množství a velikosti paketů, které během procesu konvergence přijímá a odesílá daný routovací protokol. Cílem této kapitoly je určit míru nárůstu síťového provozu spojeného s nasazením IPv6 protokolu.

Informace v této kapitole obsažené vycházejí z komunikace zachycené na rozhraních vybraných routerů měřených topologií. Zkoumaná data byla získána během pokusných měření rychlosti konvergence, viz předchozí kapitola. K jejich zachycení a analýze byl použit síťový analyzátor Wireshark, dříve známý jako Ethereal.



Obrázek 15: Rozhraní s0/0 na R4

Nejdříve se podívejme na router R4 z první (hierarchické) topologie. Ten v době nefunkčnosti R5 představuje hlavní uzel distribuční vrstvy, protože přes něj nutně musí procházet všechny pakety předávané mezi dostupnými koncovými sítěmi. Pro podrobnější zkoumání se zaměříme na jeho rozhraní „serial 0/1".

5.1 EIGRP for IPv4 vs IPv6

Budeme-li se zajímat o všechny EIGRP rámce, které jsou po obnovení funkcionality R5 přijaty či odeslány libovolným rozhraním routeru R4, zjistíme, že jejich počty nabývají s IPv4 i IPv6 prakticky totožných hodnot.

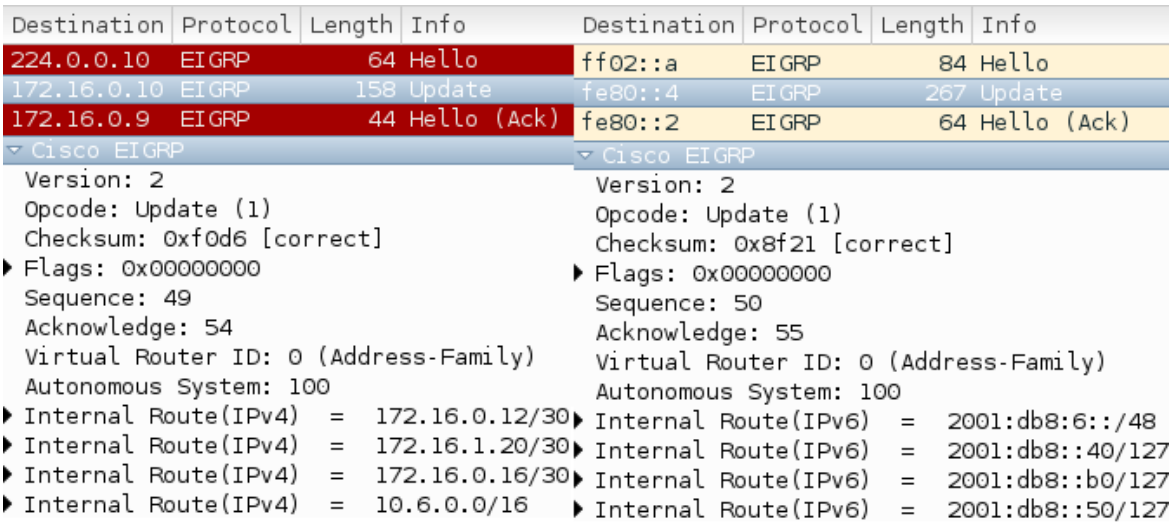
		odeslané			přijaté		
		počet	Bytů	Celkem	počet	Bytů	Celkem
IPv4	f0/0	24	1984	5,7 kB	24	2038	5,26 kB
	f0/1	14	1384		14	884	
	s0/0	7	1100		8	1397	
	s0/1	18	1379		18	1072	
IPv6	f0/0	23	2725	8,66 kB	22	2651	7,61 kB
	f0/1	15	2133		15	1260	
	s0/0	11	2063		10	2422	
	s0/1	16	1950		16	1465	

Tabulka 27: IPv4 a IPv6 EIGRP rámce na R4

Velikost jednotlivých rámců již ale svědčí o důsledku 128bitových IPv6 adres. S IPv6 router R4 odešle o téměř 3 kB více EIGRP rámců a přijme jich o necelých 2,5 kB více. Celkově musí zpracovat o 48.45 % více dat než s IPv4.

Rozhraní serial 0/0 podrobněji

Každý paket narůstá s IPv6 o 20 bytů kvůli větší délce samotné hlavičky, v důsledku čehož zdánlivě narůstají i „hello" pakety. Velikost paketů zde posléze narůstá s každou interní routou zhruba o dalších 20 bytů. Vzhledem k tomu, že EIGRP ve svých paketech používá pro každou routu proměnnou délku polí, má na velikost rámců vliv každá sumarizační routa.



Obrázek 16: EIGRP update ve Wiresharku

		přijato			odesláno		
	pokus	IPv4	IPv6	rozdíl v %	IPv4	IPv6	rozdíl v %
bytů	1	1397	2422	73,37	1164	2147	84,45
	2	1698	1944	14,49	1533	2294	49,64
	3	1288	2590	101,09	1425	2147	50,67
	4	1278	2864	124,1	1327	3172	139,03
	5	1691	2008	18,74	1733	2230	28,67
	6	1618	2544	57,23	1567	2711	73,01
	7	1663	2672	60,67	1316	2828	114,89
	8	1678	1944	15,85	1360	2230	63,97
	9	1495	2294	53,44	1508	2008	33,156
	10	1422	2744	92,97	1391	2361	69,73

Tabulka 28: Statistika pro s0/0 za 10 pokusů

5.2 RIPv2 vs RIPng

Pro posouzení množství síťového provozu u protokolů RIPv2 a jeho rozšíření RIPng byl použitý postup, který je popsaný výše, mírně upraven. Důvodem k tomu byl fakt, že Routing Information Protocol používá vždy pouze dva typy paketů, a to ať už ke změnám v síti dochází nebo ne.

Pakety typu „Request" nejsou protokolem za normálních okolností využívány. Po vlastním spuštění se jimi každý router dotazuje svých sousedů na obsah jejich routovacích tabulek. Souvislost těchto paketů s procesem konvergence je tedy nepopiratelná.

V odpovědi na požadavky odesílají routery pakety typu „Response". Stejný typ paketů ale slouží i k rozesílání pravidelných aktualizací. Mohla by tedy vyvstat otázka, jak ze všech přijatých a odeslaných paketů vybrat pouze ty, které byly vygenerovány v reakci na změnu v síti. Navíc, další změnu routovací tabulky může vyvolat kterákoli „response message", ať už vznikla v reakci na požadavek nebo při vynulování časovače.

Pravidelné aktualizace jsou sice typické svou velikostí, přesto by na tuto otázku přesněji odpověděla například podrobná analýza ladících režimů „debug ip routing" a „debug ip rip" v součinnosti s podrobným studiem obsahu paketů zachycených Wiresharkem. Pro naše potřeby je však takto podrobné zkoumání zbytečné.

		přijato			odesláno		
	pokus	IPv4	IPv6	rozdíl v %	IPv4	IPv6	rozdíl v %
bytů	1	1312	800	-39,02	460	684	48,7
	2	1312	720	-45,12	292	524	79,45
	3	1312	800	-39,02	292	448	53,42
	4	1312	800	-39,02	292	448	53,42
	5	1312	720	-45,12	292	760	160,27
	6	1312	800	-39,02	292	684	134,25
	7	1352	800	-40,83	292	684	134,25
	8	1312	800	-39,02	292	448	53,42
	9	1312	720	-45,12	292	760	160,27
	10	1312	720	-45,12	292	524	79,45

Tabulka 29: Statistika pro f0/0 za 10 pokusů

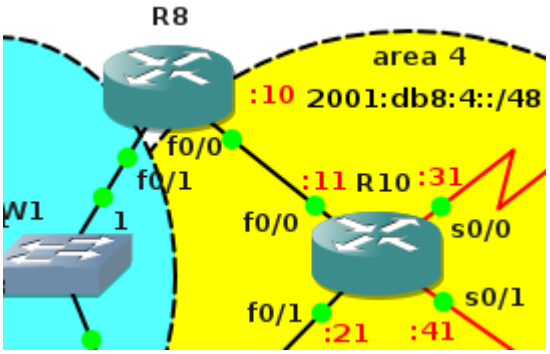
Pro posouzení síťové režie protokolů RIPv2 a RIPng bylo stanoveno časové okno o délce zhruba až 60 vteřin, během nějž probíhal režim konvergence. Hodnoty uvedené v tabulkách zahrnují všechny RIP pakety zachycené během tohoto okna routerem R4. Znát důvod vzniku jednotlivých paketů je pro naše potřeby zbytečné.

		odeslané			přijaté		
		počet	Bytů	Celkem	počet	Bytů	Celkem
IPv4	f0/0	7	1122	3,68 kB	6	1016	4,42 kB
	f0/1	6	1336		3	198	
	s0/0	2	272		7	1352	
	s0/1	9	1044		10	1960	
IPv6	f0/0	7	1262	4,13 kB	0	0	1,6 kB
	f0/1	5	1370		2	212	
	s0/0	3	684		5	800	
	s0/1	5	920		3	628	

Tabulka 30: IPv4 a IPv6 RIP pakety na R4

5.3 OSPFv2 vs OSPFv3

Rozdíly v chování OSPF lze sledovat například na routeru R10 z topologie s oblastmi. Ten se zde nachází uprostřed oblasti 4, která je k páteřní oblasti 0 redundantně připojena dvěma virtuálními linky. Připomeňme si, že v této topologii je simulován výpadek routeru R2, který představuje druhý konec obou virtuálních linků.



Obrázek 17: Router R10

		odeslané			přijaté		
		počet	Bytů	Celkem	počet	Bytů	Celkem
IPv4	f0/0	6	624	2,55 kB	5	686	2.05 kB
	f0/1	6	624		5	686	
	s0/0	7	684		4	436	
	s0/1	7	684		2	296	
IPv6	f0/0	3	838	3,37 kB	5	838	2.49 kB
	f0/1	3	838		5	838	
	s0/0	4	888		2	440	
	s0/1	4	888		2	440	

Tabulka 31: IPv4 a IPv6 OSPF rámce na R10

Úkolem R10 je tedy vyčkat na ustavení virtuálních linků a naučit se sumarizované routy do zbylých oblastí autonomního systému. Tato očekávání, založená především na předešlých zkušenostech, jsou naplněna v případě použití OSPFv2 a IPv4. První pohled do routovací tabulky OSPFv3 ale odhaluje, že s tímto protokolem nejsou skrze IPv6 propagovány pouze sumarizované adresy.

OSPFv3 šíří nejen sumarizované prefixy jednotlivých oblastí, jako to dělá OSPFv2, ale i koncové adresy tří rozhraní (prefix /128). Samy prefixy a hlavně jejich pozice v jednotlivých oblastech nicméně prozrazují, že OSPFv3 takto propaguje i koncové „uzly" virtuálních linků. Vzhledem k tomu, že se jedná o „OSPF inter" routy, jsou oba virtualní linky propagovány do všech oblastí v celém autonomním systému.

Pro všechny routery i mimo oblasti 1 a 2 to znamená, že budou vědět o tom, kde v „poměrně vzdálené" oblasti 4 končí oba virtuální linky. Toto chování pravděpodobně souvisí s požadafkem RFC, které pro adresování virtuálních linků vyžaduje globálně unikátní prefix jednoho z funkčních rozhraní (Coltun, 2008. s. 17).

Algoritmus 1 Výřez routovací tabulky na R10

```
OI 2001:DB8::/48 [110/148]
via FE80::8, FastEthernet0/0
 via FE80::9, FastEthernet0/1
OI 2001:DB8::30/128 [110/20]
 via FE80::9, FastEthernet0/1
via FE80::8, FastEthernet0/0
OI 2001:DB8:1::/48 [110/104]
 via FE80::8, FastEthernet0/0
 via FE80::9, FastEthernet0/1
OI 2001:DB8:2::/48 [110/104]
 via FE80::8, FastEthernet0/0
 via FE80::9, FastEthernet0/1
OI 2001:DB8:3::/48 [110/20]
 via FE80::9, FastEthernet0/1
 via FE80::8, FastEthernet0/0
C 2001:DB8:4::10/127 [0/0]
via ::, FastEthernet0/0
OI 2001:DB8:4::10/128 [110/10]
 via FE80::8, FastEthernet0/0
L 2001:DB8:4::11/128 [0/0]
 via ::, FastEthernet0/0
C 2001:DB8:4::20/127 [0/0]
via ::, FastEthernet0/1
OI 2001:DB8:4::20/128 [110/10]
via FE80::9, FastEthernet0/1
```

Rozdíl v režii mezi OSPFv2 a OSPFv3 již není tak výrazný, jako u EIGRP. Router R10 musel s použitím IPv6 zpracovat o pouze 27.4 % více dat, než s použitím IPv4. Tento rozdíl by byl určitě ještě menší, kdyby OSPFv3 „zbytečně" nepropagoval virtuální linky. Ve vyšších verzích Cisco IOS byla nicméně tato funkcionalita přidána i do OSPF pro IPv4. To platí přinejmenším pro IOS 15.0(1)M9.

		přijato			odesláno		
	pokus	IPv4	IPv6	rozdíl v %	IPv4	IPv6	rozdíl v %
bytů	1	812	932	14,78	874	932	6,64
	2	812	932	14,78	874	932	6,64
	3	812	1120	37,93	812	1026	26,35
	4	812	932	14,78	812	932	14,78
	5	812	1026	26,35	874	1026	17,39
	6	812	1026	26,35	812	932	14,78
	7	718	988	37,6	874	988	13,04
	8	812	1120	37,93	874	1026	17,39
	9	812	1120	37,93	874	1026	17,39
	10	812	1120	37,93	780	1026	31,54

Tabulka 32: Statistika pro f0/0 za 10 pokusů

5.4 Vytížení ostatního hardwaru

Vyšší výpočetní požadavky na paměť, procesor a jiné fyzické vybavení síťových zařízení, jsou neodmyslitelnou součástí IPv6 a vychází už z jeho podstaty. Například 32bitovou IPv4 adresu zpracuje procesor s 32bitovou architekturou během jednoho cyklu, pro IPv6 adresu může potřebovat až 4 cykly.

Obdobně jsou samozřejmostí vyšší nároky na využití paměti. Pokud budeme porovnávat dvě jinak identické routovací tabulky, jednu pro IPv4 a jednu pro IPv6, bude ta s IPv6 adresami zabírat v paměti násobně více místa, než ta pro IPv4. Vyšší hardwarové požadavky jsou tedy neoddiskutovatelnou součástí protokolu IPv6 (CISCO SYSTEMS, Inc., 1992-2014b).

6 Závěr

V této práci byl zkoumán vliv nového síťového protokolu IPv6 na proces návrhu efektivního adresního plánu a implementace tohoto plánu na pokusných topologiích. V těchto topologiích byly posléze implementovány nové generace nejznámějších IGP routovacích protokolů RIP, EIGRP a OSPF. S těmito sítěmi byly posléze vykonávány pokusy sestávající ze simulace krátkodobého výpadku jednoho z routerů, přičemž byl zkoumán čas, po jehož uplynutí dosáhne daná síť původního stavu.

Posléze byly v identických sítích implementovány v současnosti používané verze zkoumaných protokolů se síťovým protokolem IPv4 s cílem zopakovat předešlé pokusy a získat referenční hodnoty pro pozdější analýzu. Výsledky, které z těchto pokusů vzešly, posloužili pro porovnání výkonů stávajících a budoucích technologií. Povaha těchto výsledků se nakonec ukázala být poměrně překvapivá.

Sama hlavička IPv6 paketu nabývá téměř dvojnásobné velikosti, než hlavička paketu protokolu IPv4. V pozdější fázi této práce byl zkoumán i vliv IPv6 protokolu na množství síťového provozu na vybraných rozhraních, výsledkem čehož bylo víceméně očekávané zjištění o nárůstu množství přenesených dat, které se pohybovalo až v řádech desítek procent.

S použitím IPv6 a nových verzí zkoumaných routovacích protokolů bylo tedy očekávaným výsledkem prodloužení doby konvergence. Tyto výsledky se nicméně nedostavily ani při použití simulátoru, ani při opakovaných pokusech v laboratoři. Ke konvergenci obou zkoumaných sítí docházelo s použitím IPv6 vždy značně rychleji, a to v podstatě nezávisle na použitém routovacím protokolu.

Rozsah této práce je bohužel příliš malý, aby mohlo být tvrzení, že má IPv6 pozitivní vliv na rychlost konvergence sítě, přijato jako fakt. Tento poměrně zajímavý výsledek by nicméně mohl být výchozím bodem dalšího zkoumání, které by se mohlo zaměřit například na chování obdobných síťových topologií. Cílem těchto zkoumání by mohlo být ověření správnosti výsledků vzešlých z této práce jak za stejných, tak i různě pozměněných podmínek.

Protože se tato práce zabývala pouze zkoumáním časů konvergence sítí nezatížených „pracovním" provozem, bylo by vhodné ověřit výsledky této práce například v sítích s různými úrovněmi vytížení. Během těchto testování by bylo vhodné ověřit dopadu IPv6 jak během standardního provozu, tak i během tzv. špičky, kdy routery v testované síti běžely prakticky na hranici své kapacity. Dále by mohla být do pokusů zahrnuta například i technologie QoS.

1. BHAGAT, Amit N. Differences in OSPFv3 from OSPFv2. In: *Knowledge Base* [online]. [cit. 2013-12-20]. Dostupné z: https://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/differences-in-ospfv3-from-ospfv2

2. CESNET. 2013. IPv6 Addressing scheme. *CESNET: Czech Education and Science Network* [online]. [cit. 2012-12-03]. Dostupné z: http://www.cesnet.cz/services/ip-connectivity-ip/ipv6/ipv6-addressing-scheme/

3. CISCO SYSTEMS, Inc. 1992-2014a. *Cisco Networking Academy* [online]. [cit. 2014-02-16]. Dostupné z: https://www.netacad.com/

4. CISCO SYSTEMS, Inc. 1992-2014b. *The Cisco Learning Network* [online]. [cit. 2014-01-02]. Dostupné z: https://learningnetwork.cisco.com/

5. COLTUN, R. et al. 2008. OSPF for IPv6. *Request for Comments: 5340* [online]. RFC Series, [cit. 2013-12-18]. ISSN: 2070-1721. Dostupné z: http://tools.ietf.org/html/rfc5340

6. Documentation. 2007-2014. GNS3. *GNS3 Graphical Network Simulator* [online]. [cit. 2014-03-21]. Dostupné z: http://www.gns3.net/documentation/

7. HAGEN, Silvia. 2006. *IPv6 essentials*. 2nd ed. Beijing: O´Reilly, 418 s. ISBN 05-961-0058-2.

8. HOEK, Roel et al. 2013. *PREPARING AN IPV6 ADDRESS PLAN: Manual*. In: SURFNET. [online]. 2. vyd., [cit. 2013-12-10]. Dostupné z: http://www.internetsociety.org/deploy360/resources/surfnet-preparing-an-ipv6-address-plan/

9. ICANN. 2013. IPv6 Global Unicast Address Assignments. *Internet Assigned Numbers Authority* [online]. [cit. 2013-12-03]. Dostupné z: http://www.iana.org/assignments/ipv6-unicast-address-assignments/

10. KOHNO, M. et al. 2011 Using 127-Bit IPv6 Prefixes on Inter-Router Links. *Request for Comments: 6164* [online]. RFC Series, [cit. 2013-12-25]. ISSN: 2070-1721. Dostupné z: http://tools.ietf.org/html/rfc6164

11. LINDEM, A. et al. 2010 Support of Address Families in OSPFv3. *Request for Comments: 5838* [online]. RFC series, [cit. 2013-12-16]. ISSN: 2070-1721. Dostupné z: http://tools.ietf.org/html/rfc5838

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

13. MAIGRON, P., 2013. RIR Delegations. *Regional Internet Registries Statistics: RIR Delegations & RIPE NCC Allocations* [online]. 2013 [cit. 2013-12-03]. Dostupné z: http://www-public.int-evry.fr/~maigron/RIR_Stats/RIR_Delegations/Delegations/IPv6/CZ.html#RIPENCC

14. MALKIN, G. et al. 1997. IPSILON NETWORKS. RIPng for IPv6. *Request for Comments: 2080* [online]. RFC Series, [cit. 2013-11-18]. ISSN: 2070-1721. Dostupné z: https://tools.ietf.org/html/rfc2080

15. MALKIN, G. 1998. BAY NETWORKS. RIP Version 2. *Request for Comments: 2453* [online]. RFC Series, [cit. 2013-11-17]. ISSN: 2070-1721. Dostupné z: https://tools.ietf.org/html/rfc2453

16. MOY, J. 1998. OSPF Version 2. *Request for Comments: 2328* [online]. RFC Series, [cit. 2013-12-17]. ISSN: 2070-1721. Dostupné z: http://www.ietf.org/rfc/rfc2328.txt

17. 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.

18. SAVAGE, D. et al. 2014. Enhanced Interior Gateway Routing Protocol. *Draft-savage-eigrp* [online]. IETF, č. 02 [cit. 2014-04-12]. Dostupné z: https://tools.ietf.org/html/draft-savage-eigrp-02

19. STRETCH, J. 2010. OSPFv2 versus OSPFv3. In: *PacketLife.net* [online]. [cit. 2013-12-16]. Dostupné z: http://packetlife.net/blog/2010/mar/2/ospfv2-versus-ospfv3/

20. YORK, Dan. 2013. IPv6 Address Planning. In: INTERNET SOCIETY. [online]. [cit. 2013-12-12]. Dostupné z: http://www.slideshare.net/Deploy360/ipv6-address-planning