Přechod počítačových sítí z IPv4 na IPv6

Computer networks transition from IPv4 to IPv6

Jan Hrachovský

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan HRACHOVSKÝ**
Osobní číslo:	**A09651**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Přechod počítačových sítí z IPv4 na IPv6**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Porovnejte vlastnosti IPv6 s IPv4.**
3. **Popište rozdíly v konfiguracích síťových rozhraní nejpoužívanějších OS na PC.**
4. **Popište rozdíly v konfiguracích DNS serverů.**
5. **Popište rozdíly v konfiguracích směrovačů.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **VYCHODIL, Vilém. Operační systém Linux: příručka českého uživatele. Brno: Computer Press, 2003, 260 s. ISBN 80-722-6333-1.**
2. **SATRAPA, Pavel. IPv6: internetový protokol IPv6. Praha: CZ.NIC, 2008, 357 s. ISBN 978-809-0424-807.**
3. **DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP a systémem DNS. Praha: Computer Press, 2000, 426 s. ISBN 80-722-6323-4.**
4. **MCFARLAND, Shannon. IPv6: kompletní průvodce nasazením v podnikových sítích. Brno: Computer Press, 2011, 368 s. ISBN 978-802-5136-843.**
5. **IPv6 internet pomocí automatických tunelovacích technologií 6to4 a Teredo [online]. 2012 [cit. 2012-02-02]. Dostupné z: http://www.nic.cz/ipv6/**
6. **MIKROTIK. Routers and Wireless [online]. 2000 – 2006 [cit. 2012-02-02]. Dostupné z: http://www.mikrotik.com/**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **8. června 2012**

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Práce se zabývá problematikou počítačových sítí protokolu IPv4 a jejího následného přechodu na verzi IPv6. První části je zaměřena na seznámení s novým protokolem a možnostmi přechodu. Druhá část se zaměřuje na konkrétní nastavení vybraných metod a popis rozdílů oproti konfiguraci předešlého protokolu IPv4.

Klíčová slova: IPv6, Teredo, OSPFv3, AAAA

ABSTRACT

Diploma work is dealing with computer network problematic of protocol IPv4 and its subsequent transition to protocol IPv6. First part is focused on introduction of new protocol and methods of protocol transition. Second part is focused on specific setting of chosen methods and description of differences in configuration between previous protocol IPv4.

Keywords: IPv6, Teredo, OSPFv3, AAAA

Poděkování

Na tomto místě bych rád poděkoval zejména vedoucímu své práce, tedy Ing. Miroslavu Matýskovi, Ph.D., za udílení cenných rad pro vytvoření práce. Také samozřejmě své rodině, za trpělivost. V neposlední řadě i svému zaměstnavateli p. Jaroslavu Novotnému, za vstřícný přístup ke tvorbě této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Internet, od dob svého počátku, až po dobu v jaké ho známe my nyní, urazil velkou cestu a prošel obrovskými změnami. Když v roce 1969 byla zprovozněna první síť ARPANET, spojovala 4 uzly. Jen s těží si jeho tvůrci představovali, že o několik desítek let později to bude již přes 2 miliardy uživatelů.

Postupem času byla síť modernizována, upravována a rozšiřována o různé služby jako je např. email, WWW, telnet a mnohé jiné. Kromě rozšíření služeb docházelo také k rozšíření rozlohy, kterou síť pokrývala. Původně měl adresaci v této síti na starost protokol NCP – Network Control Program, který byl později nahrazen nám již známým protokolem IPv4. To bylo roku roku 1980, kdy v této síti nebylo ještě ani 27 000 počítačů a protokol byl plně dostačující. Opět postupujeme dále v čase a sledujeme jak uživatelů v síti přibývá.

Již začíná být jasné, že protokol IPv4 brzy nebude tomuto tempu stačit a časem dojde k vyčerpání kapacity jeho adres. K vytvoření nového protokolu komise IETF (Internet Engineering Task Force) ustanovila několik skupin, které měly za úkol vytvořit takzvanou „IP nové generace – IPng“

Postupným vytvářením nových definicí byl navržen nový 128 bitový protokol IPv6. Tento protokol měl díky své velikosti zajistit obrovský počet adres, které nebudou do budoucna vyčerpány. Protokol ale také kromě své velikosti disponuje dalšími vymoženostmi, které starý protokol neobsahuje jako je např. vetší bezpečnost v adresní vrstvě, bezstavová konfigurace adres a mnohé další.

Dalším cílem je nyní tento protokol rozšířit do celé sítě internetu, aby se pomalu začlenil současně se starým protokolem, který by měl pomalu přijít na ústup. Tento proces je ale nesmírně nákladný a také nesmírně pracný a to je i důvod proč jsem si zvolil téma této práce a byl bych rád, kdyby ba i malou měrou, přispěla tato práce k jeho rozšíření a přiblížení ostatním lidem [1].

I. TEORETICKÁ ČÁST

1 Adresa IPv6

1.1 Zápis adresy IPv6

Adresa IPv6 je zapsána o délce 128 bitů, pomocí hexadecimálního zápisu, který nám umožňuje zapsat přibližně 3,40 * 10^{38} unikátních adres. Starý protokol IPv4 je zapsán o délce 32 bitů a umožňoval zápis přes 4,2 miliardy unikátních adres. Je vidět, že kapacita nového protokolu IPv6 jej kapacitou naprosto převyšuje.

Adresa IPv6 je zapisována do „bloků“ o velikosti 4 znaků, které jsou od sebe oddělovány znakem „ **:** “ , počet bloků je 8. Pro přehlednost a efektivnost zapisování adresy jsou stanovena pravidla, která umožňují některé znaky vynechat a provést zkrácený tvar zápisu.

a) v bloku začínajícím 0, např. 0009, můžeme při zapisování nuly vynechat a zapsat jen číslo 9.

b) v zápisu celé adresy mohou některé bloky tvořit jen 0, tyto bloky můžeme opět vynechat a zapsat je jako „ **::** „ Tento druh zkrácení zápisu si v jedné adrese můžeme dovolit použít pouze jedenkrát.

Nyní si uvedeme praktický příklad zkrácení zápisu adresy:

Tab. 1. Úprava zápisu adresy

Běžný tvar zápisu :	**0123:0000:0000:0000:0ab3:d128:1234:0123**
Zkrácený tvar zápisu:	**123::ab3:d128:1234:123**

Nicméně vidíme na zkráceném tvaru, že stále může být dost dlouhý, proto se počítá spíše se zápisem pomocí DNS záznamu.

1.1.1 Prefix

Příslušnost k určité síti nebo podsíti se vyjadřuje prefixem – všechna rozhraní v jedné síti mají stejný prefix (začátek adresy). Jeho délka může být různá. Záleží na tom, s jakou podrobností se na adresy díváme .Můžeme se zajímat jen o prefix poskytovatele internetu (ten bude poměrně krátký) nebo o prefix určité konkrétní podsítě. [2]

Zápis prefixu: IPv6_adresa/délka_prefixu

Např.: 12ab:0:0:cd30::/60

1.1.2 IPv6 hlavička

Definici IPv6 hlavičky najdeme ve specifikaci RFC 1883.Její velikost je neměnná a rovná se 40 B. Hlavička obsahuje tyto údaje:

Verzi – 4 bity – obsahuje údaj o jakou verzi IP se jedná

Třída provozu –*Trafic Class* – 8 bitů

obsahuje prioritu doručování datagramu. Měla by také zaručit provozování služeb s určitou kvalitou, ale zatím v praxi ještě neplatní. Vlastní definice není ještě úplně přesně stanovena

Značka toku – Flow Label– 20 bitů

stejně jako třída provozu není ještě přesně definován. V zásadě by měl být označován jakou proud datagramů se společnými vlastnostmi jako je např. odesílatel, adresát nebo požadavky na spojení. Právě prostřednictvím značky by byl datagram rozpoznám a tím zvýšena jeho rychlost zpracování.[2]

Délka dat - Payload Length – 16 bitů

určuje velikost paketů v oktetech. Velikost dat následujících za hlavičkou

Další hlavička – Next Header – 8 bitů

je v ní obsažena informace jaká bude následující hlavička

Dosah – Hop Limit – 8 bitů

je to takový nástupce za předešlé TTL v IPv4. Při průchodu směrovačem dojde ke snížení hodnoty o 1. Pokud dojde ke snížení až na 0, je datagram zničen a pomocí ICMP je odesílateli zasláno upozornění o vypršení počtu skoků.

Zdrojová adresa – Source Address – 128 bitů

Cílová adresa – Destination Address – 128 bitů

Pro srovnání hlaviček s protokolem IPv4 grafické znázornění rozdílů[4]:

Obr. 1. Porovnání hlaviček IPv4 a IPv6

1.1.3 IPv6 rozšiřující hlavičky

V tomto novém protokolu dochází na rozdíl od jeho předchůdce ke změně ve zřetězení dalších hlaviček. Každá další hlavička je představována jako samostatná část a právě na každou další ukazuje položka „*Next Header – Další hlavička“*. Každá z rozšiřujících hlaviček začíná právě touto položkou.

Seznam rozšiřujících hlaviček najdeme na:

http://www.iana.org/assigments/protocol-numbers

Zde uvedeno jen několik důležitých hlaviček jako příklad[5]:

Tab. 2. Důležité hlavičky

0 - Hop-by-Hop (!musí být hned za IPv6 hlavičkou)	6 – TCP
43 – Routing (typ 2 – nahrazeno místo starého typu 0)	17 - UDP
44 – Fragment	58 – ICMPv6
59 – No next Header	89 - OSPF

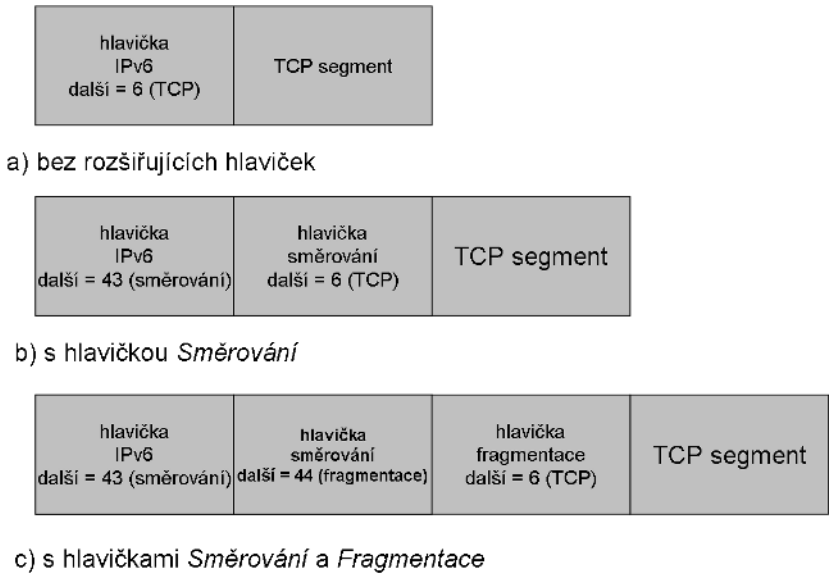
Výhodou takové adresace je, že posíláme jen to co je opravdu potřebné. Nevýhodou by se mohlo stát pouze dlouhé zřetězení více hlaviček. Proto mají hlavičky předepsáno přesné pořadí jak mají být uvedeny.

1.1.4 Doporučné pořadí rozšiřujících hlaviček

- IPv6 Header
- Hop-by-Hop Options header
- Destination Option header (pro první cílovou adresu a dle RH)
- Routing header (RH)
- Fragment header
- Authentication header
- Encapsulating Security Payload header (ESP – šifrování obsahu)
- Destination Options header(pro konečného příjemce)
- mobilita

Rozšiřující hlavičky musí být zpracovány ve stejném pořadí v jakém jsou uvedeny a bývají zpracovány až na straně příjemce. Vyjímku je zpracování hlavičky Hop-by-Hop[2]

Příklad zřetězení hlaviček:



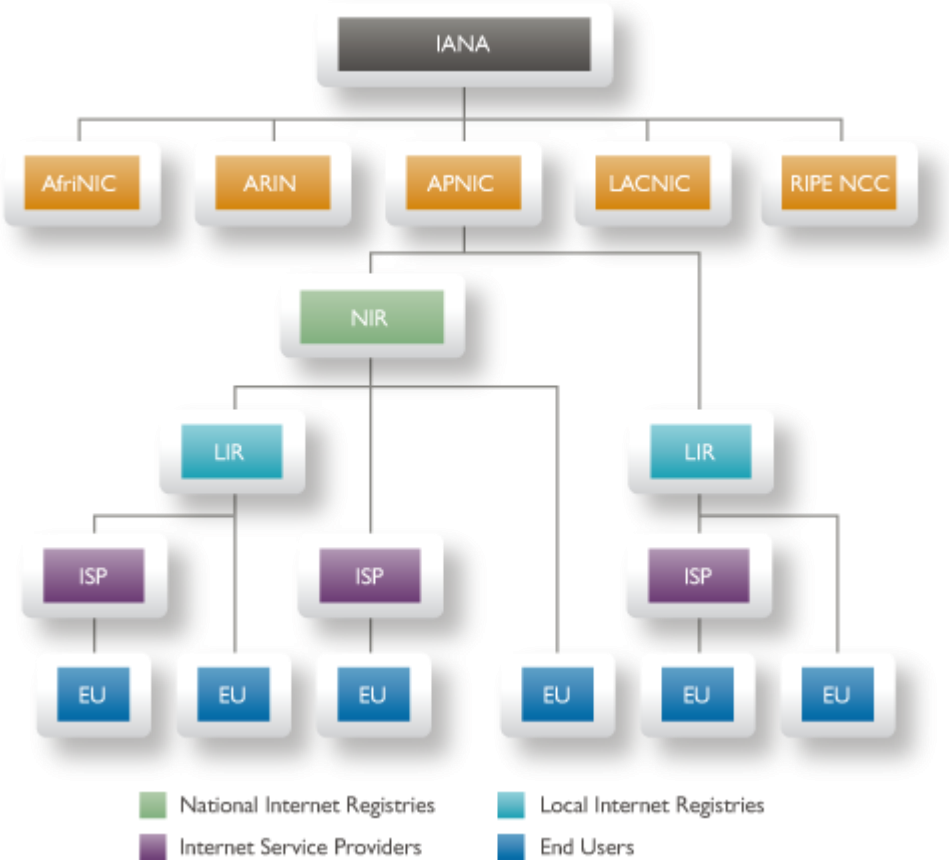
Obr. 2. Zřetězení hlaviček

1.2 Vlastnosti adres IPv6

1.2.1 Přidělování IPv6 adres

Přidělování a hlavní zprávu IPv6 má na starost organizace IANA – Internet Assigned Numbers Authority. Je to celosvětový koordinátor IP adres a Root DNS serverů. Tato organizace pak dále rozděluje adresy národním registračním organizacím. Konkrétně pro Evropu a blízký východ je to organizace RIPE NCC.

Zde je schéma struktury přerozdělování adresných zdrojů:



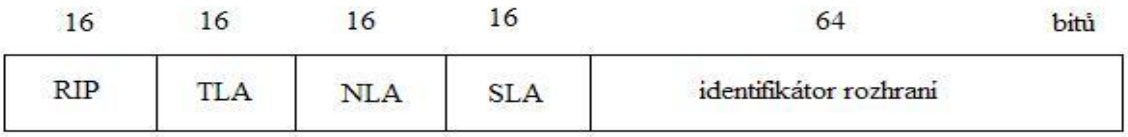
Obr. 3 Distribuce IPv6 adres [6]

1.3 Typy IPv6 adres

Adresní prostor IPv6 je rozdělen do několika specifických skupin, které jsou definovány podle prefixu

::1/128	nedefinované adresy
::1/128	smyčka (loopback)
::ffff /96	IPv4 mapované adresy
fc00::/7	unikátní lokální (unique local)
ff00::/8	skupinové adresy (multicast)
fe80::/10	linková lokální (link-local)
2000::/3	globální individuální (global unicast)

1.3.1 Globální individuální adresy



Obr. 4. Struktura globální individuální adresy

RIP - prefix regionálního registrátora

TLA - Top level aggregation - prefix poskytovatele

NLA - Next level aggregation - prefix zákazníka

SLA - Site level aggregation - prefix podsítě

Je to alternativní řešení k veřejné IP adrese v4 protokolu

Nyní je uvolněn rozsah 2000::/3

2000:0000:0000:0000:0000:0000:0000

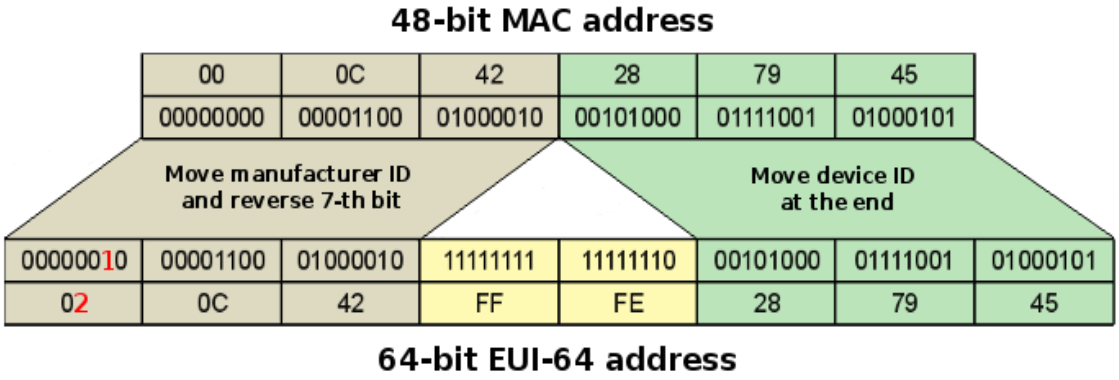
3fff :ffff :ffff :ffff :ffff :ffff :ffff :ffff

1.3.2 EUI 64 - Identifikátor rozhraní

Skládá se z MAC adresy zařízení, kterému je adresa přiřazována.V případě že se jedná o 48 bitovou MAC adresu je doprostřed vkládán 16 bitový kód o hodnotě „FFFE“. Dále ještě v prvním bajtu, v předposledním bytu „000000_0“ hodnota 1 nebo 0 udává zda se jedná o globální nebo lokální adresu.

0 = globální 1 = lokální

Z důvodu bezpečnosti je ale tento způsob ještě upraven na takzvaný *Modifikovaný EUI-64.* Jelikož by bylo možno adresu předvídat a následně zfalšováním zneužít. Proto dochází ještě k náhodnému generování a následné modifikaci. Tato metoda se nazývá *Privacy Extensions* a je definována v RFC 4941. Po této modifikaci dochází k obrácení významu hodnoty globální – lokální adresy v předposledním bitu viz. výše.



Obr. 5. EUI-64 [3]

1.3.3 Linkové lokální adresy

Linkové lokální adresy jsou adresy, které jsou obdobou vnitřních adres u IPv4, které měli původně sloužit pouze pro adresaci sítí, které nebudou připojeny do internetu. U protokolu IPv4 tyto adresy nebyli nijak přesně definovány, u IPv6 je tomu již jinak. Adresy jsou označeny prefixem fe80::/10, následujících 54 bitů obsahuje nuly a zbytek adresy (64 bitů) je sestaven podle výše uvedeného EUI -64.

Jako příklad uvedeme část z Obr. 5:

fe80::20C:42ff:fe28:7945

1.3.4 IPv4 mapované adresy

Některé systémy potřebují k chodu jak adresu IPv4, tak i IPv6, proto vznikly takzvané mapované adresy. U takových to adres je prvních 80 bitů nulových, následně 16 bitů obsahuje jedničky a poté zápis adresy IPv4.

Například : 192.168.1.125 -> ::ffff.192.168.1.125

Tento způsob s sebou nese určitá bezpečnostní rizika, které je možno ošetřit filtrovacími pravidly. Také je možno použitím příkazů funkci vypnout.

1.3.5 Skupinové adresy

Skupinové adresy, nebo-li také multicastové adresy. Zde zůstává funkční princip téměř stejný jako tomu bylo u IPv4 a slouží pro přenos audio-video dat (např. IPTV)

Struktura skupinové adresy je definována v RFC 4291:

Tab. 3 Struktura skupinové adresy

8 bitů	4 bity	4 bity	112 bitů
FF	volby „*TPR*“	*dosah*	*samotná adresa skupiny*

Volby RPT:

- první byt vždy 0

- R…..Rendezvous Point(dále RP); 1 = obsahuje ; 0 = neobsahuje

  umožní do adresy zakódovat adresu RP , použitý protokolem PIM SM pro možnost použití musí byt T i P hodnoty „1“

- P…..Prefix adresa skupiny pochází z unicast prefixu; 1 = obsahuje; 0 = neobsahuje

- T…..Transient určuje zda je adresa přidělena na pevno (trvale) nebo ne, o přidělení se stará IANA. 1 = dočasná; 0 = trvalá

- Dosah…..určuje vzdálenost, jak daleko od sebe mohou členové být. Jedná se 4 bitovou hodnotu a může obsahovat až 16 možností. 0-9 a A-F. Ne všechny jsou zatím stanoveny.

Tab. 4 Dosahy

0 – rezervováno	6,7 - volné
1 – lokální pro rozhraní	8 – pro organizaci
2 – lokální pro linku	9 - volné
3 - rezervováno	A,B,C,D - volné
4 – lokální pro správu	E - globální
5 – lokální pro místo	F - rezervováno

Pokud bychom například, jako poskytovatelé nastavili dosah 8, byli by skupinové pakety doručovány všem našim zákazníkům.

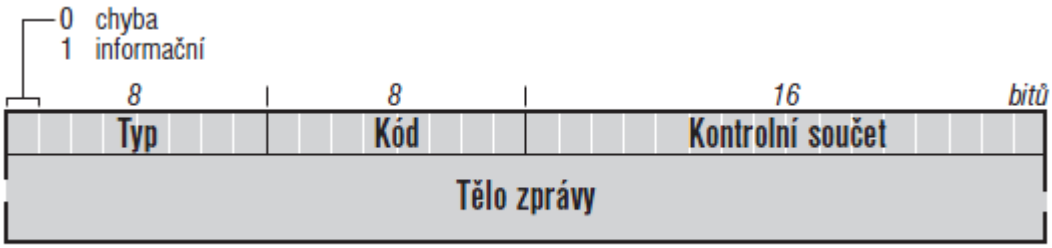
1.3.6 Výběrové adresy

Jedna z významných novinek obsažených v protokolu IPv6. Slouží například k rozložení zatížení „serveru“, který je ve skutečnosti tvořen několika fyzickými PC. Pomocí „Load Balancigu“ dojde k přeposlání požadavku po nejkratší cestě, čímž se také razantně sníží odezva. Také dojde ke zvýšení bezpečnosti, například vyšší odolnost oproti DDoS útokům, které byly v poslední době často používány k útokům na servery skupinou Anonymous nebo také různých Botnetových sítí. Nevýhodou je, že dojde k většímu zatížení směrovacích tabulek routerů.

Adresa má stejný tvar jako globální individuální adresa, jen posledních 64 bitů obsahuje samé nuly.

1.4 ICMP

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.



Obr. 6. Datagram ICMP [2]

Oproti ICMP obsaženém v protokolu IPv4 má ICMPv6 daleko více funkcí. Obecně rozdělujeme přenášené zprávy do 2 skupin:

I. Chybové : Typ 0-127

II. Informační: Typ 128-255

Například zpráva č. 129 – odezva.

Seznam všech ICMPv6 zpráv nalezneme na:
http://www.iana.org/assignments/icmpv6-parameters

1.4.1 Objevování sousedů (Neighbor Discovery)

Je to skupina ICMPv6 zpráv, pomocí kterých můžeme zjistit:

- nalezení routeru
- zjištění prefixu sítě
- MTU, Hop limit
- bezstavová autokonfigurace adres
- **linkovou adresu**
- ….

Objevování sousedů používá tyto zprávy :

133 – výzva směrovači 134 – ohlášení směrovače

135 – výzva sousedovy 136 – ohlášení souseda

137 - přesměrování

Objevování sousedů také nahrazuje ARP, která se používala u IPv4.
Zasláním zprávy 135 - **výzva sousedovy** , se zašle zpráva na povinnou skupinovou adresu hosta tzv. **vyzývavý uzel** - ff02:0:0:0:0:ff00::/104 + 24bitů IP adresa. Odpověď obdržíme pomocí zprávy 136 – **ohlášení souseda.**

1.5 Přechodové mechanismy

Při přechodu sítě na IPv6 je jasné, že se tak nestane z minuty na minutu, ale že to bude nějaký čas trvat. Proto od samého počátku vznikají tzv. *přechodové mechanismy.* Jsou to metody pomocí nichž můžeme používat současně jak IPv4 tak IPv6. Obecně se rozdělují do 3 skupin:

Dvojí zásobník – Dual Stack

Tunelování - Tunneling

Překladače – Translators

1.5.1 Dvojí zásobník

Je to mechanismus, který zahrnuje jak nastavení IPv4 tak IPv6. Do budoucna nijak zajímavý z důvodu zachování IPv4. Použití je například u DNS serverů, kde se záznamy IPv4 označují jako A a záznamy IPv6 sou označeny AAAA (zjednodušeně řečeno). Podle cílové adresy pak server rozhodne, který záznam bude použit.

1.5.2 Tunelování

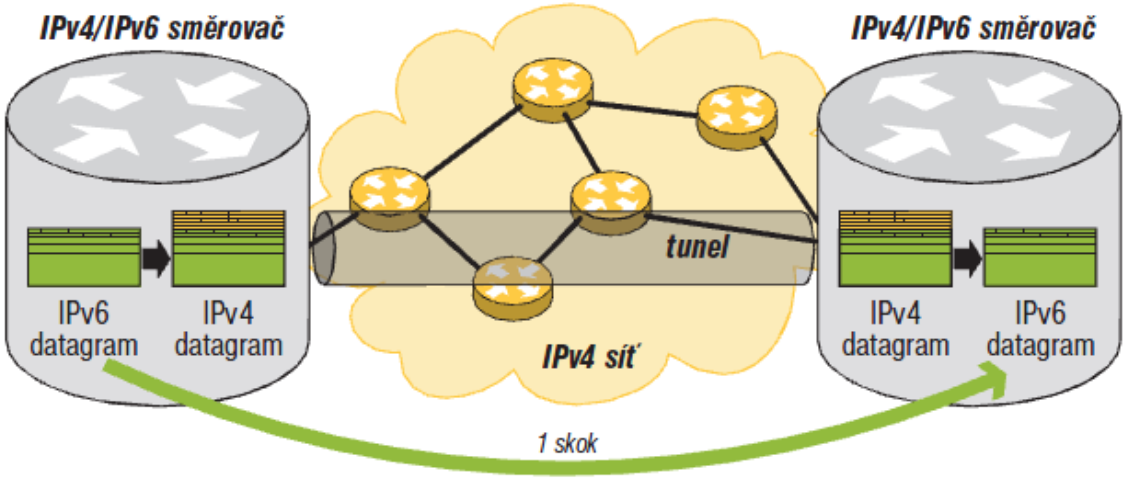
V našem případě se jedná o mechanismus, kdy mezi sebou navážou spojení dva systémy, které jsou odděleny prostorem, jenž nesplňuje požadavky na daný druh komunikace. Proto jsou data IPv6 zabalena do datagramu IPv4 a pomocí něj přenesena.

Je možno zvolit ze dvou způsobů tunelování :

1. automatické

2. manuální

Pro běžné uživatele je lépe zvolit automatické, z důvodu jednoduchosti zprovoznění. Do této kategorie spadají například 6to4, ISATAP nebo Teredo.



Obr. 7. Princip tunelování [2].

Co se týče možnosti použitelnosti, vykazuje dobré výsledky Teredo, které na rozdíl od 6to4 nevyžaduje veřejnou IP adresu.

Nevýhodou je bohužel vyšší odezva při přenosu.

1.5.3 Translátory

Může nastat případ, že jsme připojeni v systému, který obsahuje pouze protokol IPv6 a potřebujeme získat data ze systému, který obsahuje pouze protokol IPv4. K tomuto účelu byly navrženy translátory, které by nám měly data přeložit. Jedním z nich byl i NAT-PT (Network Address Translation – Protocol Translation), který ale nakonec nebyl úspěšný. V tomto směru tedy zůstává stále nedořešený problém.

1.6 Připojení pomocí Tunnel Brokerů

Specializované weby, které nabídnou připojení k IPv6 pomocí specialních clientů, které se pouze nainstalují, vyplní se údaje pro ověření a poté se stačí už jen připojit. Tyto služby jsou většinou bezplatné a nutná je pouze registrace. Tato služba může dobře posloužit pokud uvažujeme o trvalém připojení přes IPv6 a potřebujeme zachovat statické IP adresy a poskytovatel není ochoten nebo schopen IPv6 poskytnout. Při volbě tunnel brokera je vhodné zvolit takového, který je geograficky co nejblíže, tím dochází k zvýšení pravděpodobnost nižší odezvy při přenosech.

Několik zprostředkovatelů brokerů:

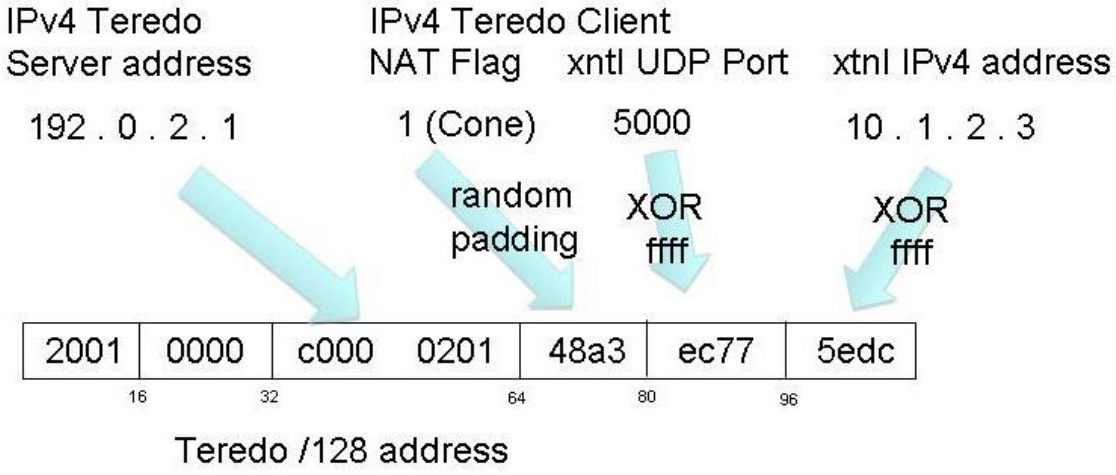
www.gogo6.com (dříve freenet6.net)

www.sixxs.net (vlastní uzel v České republice)

1.7 Připojení pomocí Tereda

Hlavním problém pro tunelovací mechanismy je NAT (Network address translation) z důvodu změny adres a portů. Navíc z bezpečnostních důvodů dochází k propouštění dat do sítě jen z adres, na které v nedávné době dotyčné zařízení nějaké data poslalo. Proto při navázání spojení s Teredo serverem dochází k zahájení komunikace ze strany clienta.

Struktura datagramu Tereda:



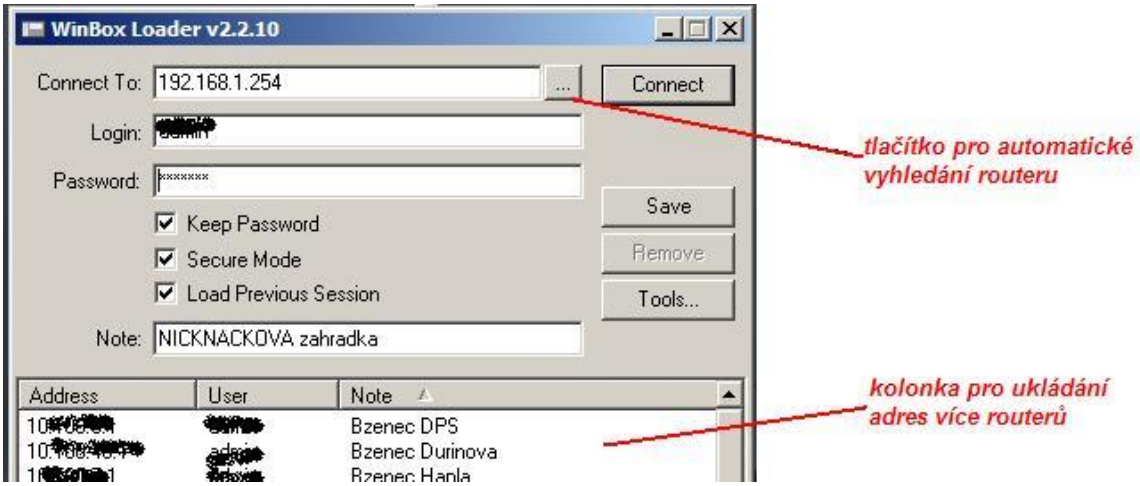
Obr. 8. Datagram Tereda

Datagram Tereda začíná vždy hodnotou 2001::/32, zbylých 32 bitů ukrývá IPv4 adresu Teredo serveru. Dalších 16 bitů ukrývá hodnotu, zda se jedná o trychtýřový NAT (Cone) nebo jiný druh firewallu. Dalších 16 bitů ukrývá UDP port pro vlastní přenos dat, jelikož s pakety UDP umí NAT dobře pracovat. Posledních 32 bitů patří klientské IPv4 adrese.

2 RouterBoard a OS Mikrotik

Firma Mikrotik je Litevská společnost specializující se na software pro správu routerů, který prodává pod značkou Mikrotik, a na výrobu routerů, které jsou pod značkou RouterBoard (dále jen RB). Firma si drží standart na poloprofesionální – profesionální úrovni s cenově dostupnými produkty pro malé-střední firmy i koncového zákazníka. V tomto okruhu zákazníků je to asi nejrozšířenější firma v České a Slovenské republice. Proto byly zvoleny produkty této společnosti pro praktickou část práce.

Hlavní konfigurace těchto zařízení se provádí pomocí speciální utility Winbox, která je pro konfiguraci navržena.



Obr. 9. Winbox Login

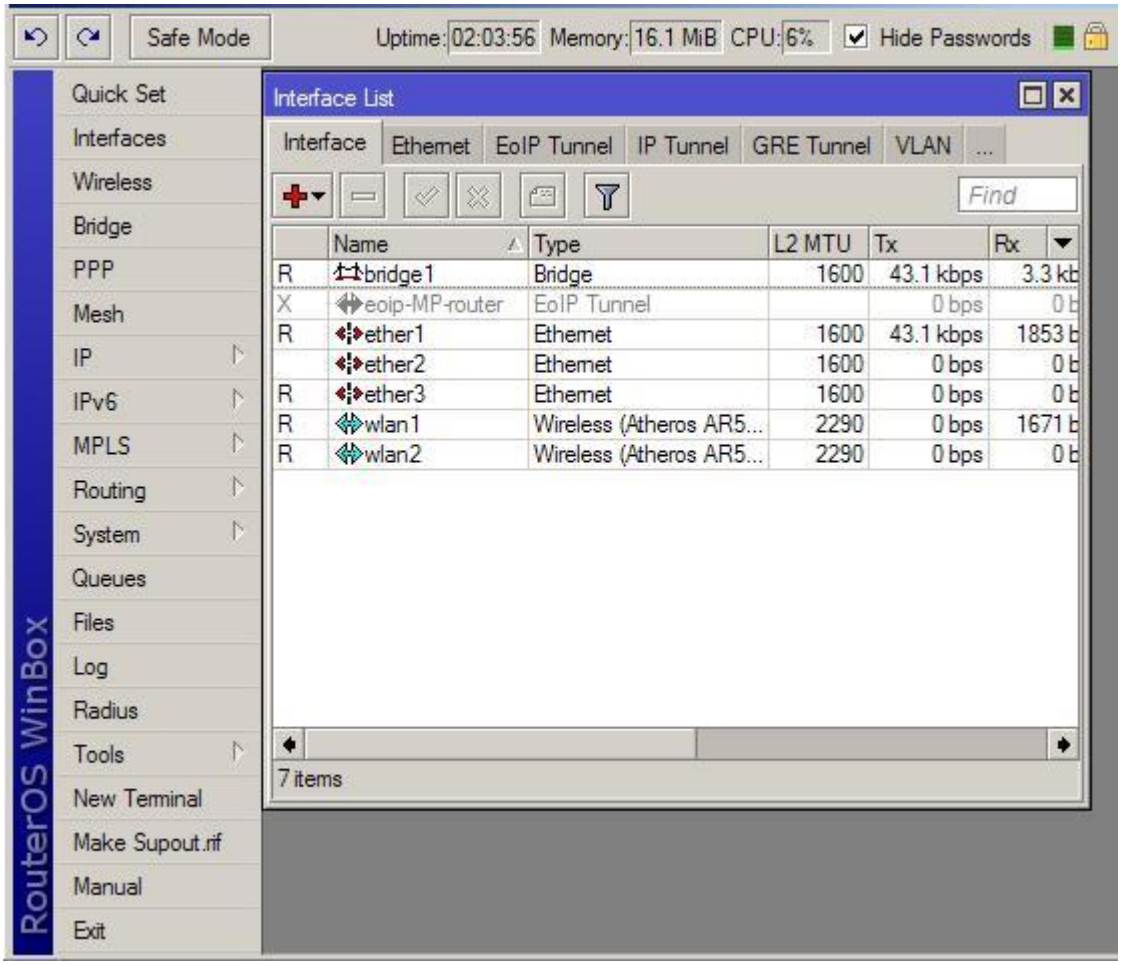
Nyní můžeme router načíst pomocí IP adresy, nebo pokud jsme připojeni napřímo do RB, můžeme použit autodetekci pomocí „tlačítka pro automatické vyhledání“. Po zadání uživatelského jména do kolonky login a hesla do kolonky password zvolíme „Connect“

Nyní se otevře hlavní menu pro konfiguraci, které bude vypadat asi takto:

- horní vodorovná lišta, která zobrazuje systémové zdroje
- levý svislý panel, který obsahuje hlavní položky pro nastavení RB
- zbytek volného prostoru, pracovní plocha, do které se nám budou otevírat námi zvolené položky formou oken, jako je tomu u MS Windows

Položky obsažené v levém panelu je možno do RB dohrávat pomocí balíčkového systému, podle toho, k jakým účelům chceme daný router využít (omezovač, firewall, router, …) Seznam balíčků nalezneme po zvolení položky:

Systém -> Packages



Obr. 10. Winbox menu

Router může být nyní konfigurován 2 způsoby:

I. pomocí příkazů do do příkazové řádky – položka „New Terminal“

II. pomocí tzv. „klikacího nastavení“ kdy volíme položky z hlavní lišty

Stručný přehled funkcí:

Interfaces – obsahuje všechny interface daného routeru (drátové, bezdrátové, virtuální,…)

Wireless – obsahuje pouze bezdrátové interface a jejich statistiky

IP – nastavení IPv4 adres pro interface, Firewall, DHCP server…

IPv6 – stejné jako IP jen pro IPv6

Routing – obsahuje routovací protokoly (RIP, BGP, OSPF,…)

Systém – systémové nastavení routeru (hesla, jména uživatelů, jméno routeru,…)

Queues – obsahuje omezovače rychlostí a jejich nastavení

Files - místo pro vstupní a výstupní soubory (logy, firmware,…)

Tools – programy pro monitorování sítě

New Terminal – terminálová konzole

3 BIND – Berkley Internet Name Domain

Bind je nejrozšířenějším programem pro provozování DNS serverů na světě. Je navržen pro provoz na unixových systémech ale existují verze i pro MS Windows. V současné době je jediná podporovaná verze BIND 9. V roce 2008 byla vydána verze 9.5. Tato verze plně podporuje jak záznamy PTR tak i AAAA.

Po naistalování, pokud chceme využívat IPv6, je nutno editovat soubor *named.conf a* upravit volbu:[2]

listen-on-v6 { any; };

3.1 Zóny

Nejdůležitější části BINDu jsou tzv. zónové soubory. Obsahují data o určité doméně. Soubor *named.conf* by měl obsahovat ke každé doméně zápis v tomto tvaru:

zone *„jméno_domény“* {

type master;

file “jméno_souboru”;

};

Ve skutečnosti ale data nejsou obsažena přímo v souboru *named.conf*, ale jsou do něj inclůdována (vložena) ze souboru *named.conf.local*

Názorný příklad zápisu pro doménu *utb.cz :*

zone *„utb.cz“* {

type master;

file “/etc/bind/db.utb.cz”;

};

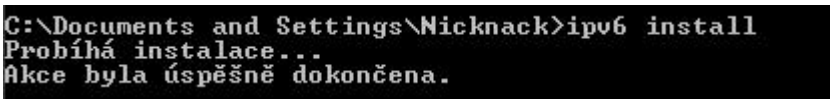
I. PRAKTICKÁ ČÁST

4 Rozdíly v konfiguracích na nejpoužívanějších OS na PC

K vyzkoušení nakonfigurování využijeme operační systém (dále jen OS) Ubuntu 10.04, Windows 7 Home, Windows XP Service Pack 2, Edition .

První dva OS mají již podporu IPv6 obsaženou, tudíž ze začátku není žádný problém a jsou připraveny k použití. U Windows XP je to již o něco horší. Zde je nutno podporu IPv6 nejdříve doinstalovat.

Instalace je jednoduchá a provede se přes příkazovou řádku (Start -> Spustit -> cmd). Dále do příkazové řádky napíšeme : *ipv6 install*



Obr. 11. Instalace IPv6

Nyní již máme systémy připraveny a můžeme pokročit k samotné konfiguraci.

4.1 Připojení pomocí tunelu Teredo

Pokud se hodláme připojit pomocí protokolu IPv6 je zapotřebí získat IPv6 adresu. Ideálním řešením je, že požádáme našeho poskytovatele připojení o její přidělení. Pokud ji ale náš poskytovatel nemá, nebo nám ji z nějaké jiného důvodu nechce přidělit, je možno využít připojení pomocí tunelování. My si zvolíme připojení pomocí systému Teredo, jelikož jak již bylo zmíněno, není nutno mít veřejnou IP adresu (na rozdíl od 6to4). Dále si zvolíme anonymní připojení, kde není potřeba žádné registrace, což opět dostačuje našim potřebám.

4.1.1 Teredo na OS Microsoft Windows

V systémech Windows XP a 7 je client Teredo již naistalován, proto nám stačí jen zadat námi zvolený server pro připojení, nebo také nechat defaultně nastavený.

Nastavení Tereda provedeme přes příkazovou řádku:

netsh int ipv6 set teredo client teredo.nic.cz

nebo pomocí serveru Microsoft

netsh int ipv6 set teredo client teredo.ipv6.microsoft.com

během několika sekund by se nám v příkazové řádce mělo zobrazit hlášení

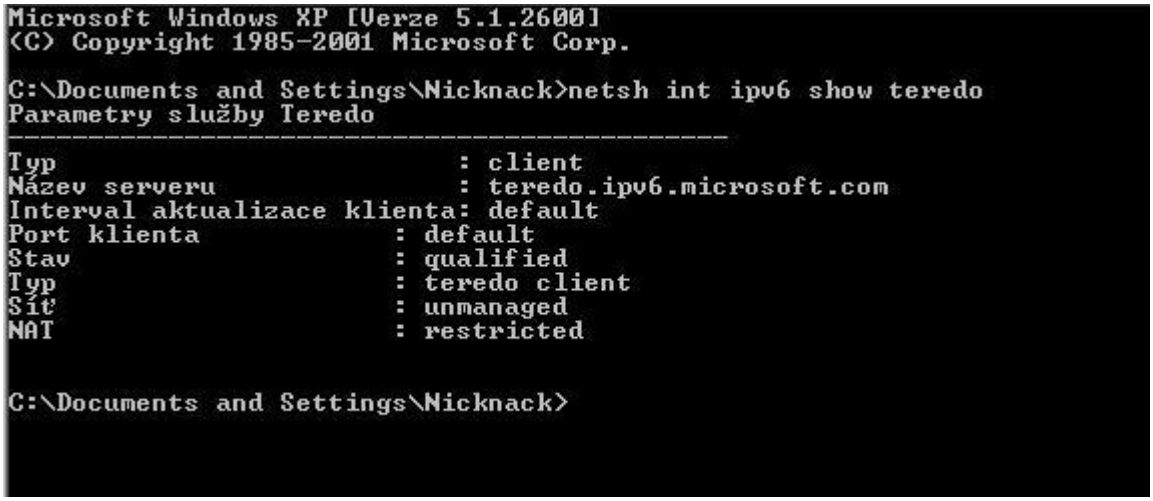
OK

Tato operace může chvíli trvat, dochází ke komunikaci klient/teredo server a zjištění NATu.

Pro kontrolu zda je vše v pořádku použijeme příkaz:

netsh int ipv6 show teredo

Pokud vše proběhlo jak mělo, bude vypadat výpis takto:



Obr. 12. Teredo status

Důležitý je řádek „Název serveru“, kde vidíme na který server se připojujeme.

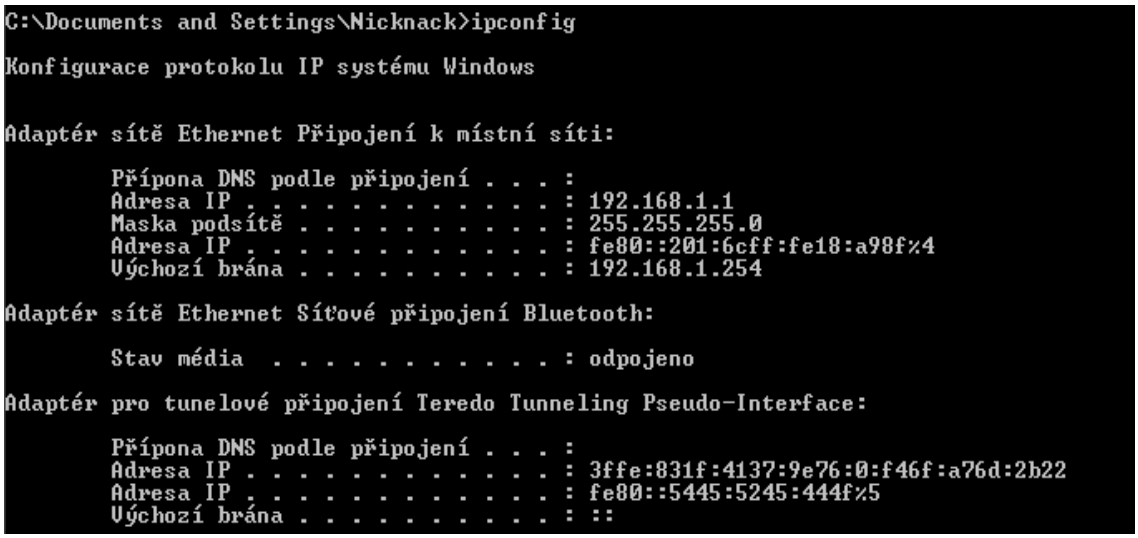
Dále je důležitý řádek „Stav“, kde při úspěšném připojení bude uvedena hodnota „qualifield“.

V řádku „NAT“ už jen dojde k automatické volbě typu NATu buď na hodnotu „restricted“ nebo „cone“

Ještě pomocí příkazu :

ipconfig

můžeme zkontrolovat zda nám byla přidělena IPv6 adresa



Obr. 13. Ipconfig

Pro nastavení ve Windows 7 není potřeba Teredo nijak nastavovat, pokud nechceme změnit Teredo server. Oproti OS Windows XP je při použití příkazu

netsh int ipv6 show teredo

vypsán přechod tunelu přes NAT, jak vidíme ve dvou posledních řádcích. Místní mapování znamená překlad NATu z naší lokální adresy na veřejnou adresu (Externí mapování), kterou dále pokračujeme do internetu.

Zde příklad s NATy ve Windows 7:

```
C:\Users\nicknack>netsh int ipv6 show teredo
Parametry služby Teredo
---------------------------------------------
Typ                            : client
Název serveru                  : teredo.ipv6.microsoft.com.
Interval aktualizace klienta: 30 s
Port klienta                   : unspecified
Stav                           : qualified
Typ klienta                    : Teredo client
Síť                            : unmanaged
NAT                            : restricted
Speciální chování NAT          : UPNP: Ne, Zachování portu: Ano
Místní mapování                : 192.168.1.251:58195
Externí mapování NAT           : 88.146.212.221:58195
```

Obr. 14. Status Tereda(Windows7)

Nyní můžeme prakticky vyzkoušet zda máme přístup do internetu pomocí IPv6. Jako test můžeme použít v Os Windows příkaz:

ping -6 nebo *tracert -6* , parametr „-6“ u obou příkazů vynutí použití protokolu IPv6

```
C:\Users\nicknack>tracert -6 ipv6.google.com

Výpis trasy k ipv6.l.google.com [2a00:1450:4016:800::1011]
s nejvýše 30 směrováními:

  1   743 ms   108 ms   130 ms  6to4.fra1.he.net [2001:470:0:150::2]
  2    33 ms    91 ms    32 ms  gigabitethernet2-6.core1.fra1.he.net [2001:470:0
:150::1]
  3    89 ms    92 ms    86 ms  de-cix20.net.google.com [2001:7f8::3b41:0:2]
  4   118 ms    40 ms    47 ms  2001:4860::1:0:10
  5  2086 ms    46 ms   311 ms  2001:4860::8:0:3015
  6   211 ms   210 ms   222 ms  2001:4860::1:0:336c
  7    44 ms    43 ms    52 ms  2001:4860:0:1::535
  8   123 ms     *      413 ms  muc03s01-in-x11.1e100.net [2a00:1450:4016:800::1
011]

Trasování bylo dokončeno.
```

Obr. 15. Tracert google

```
C:\Users\nicknack>ping -6 ipv6.google.com

Příkaz PING na ipv6.l.google.com [2a00:1450:4016:800::1012] - 32 bajtů dat:
Odpověď od 2a00:1450:4016:800::1012: čas=105ms
Odpověď od 2a00:1450:4016:800::1012: čas=109ms
Odpověď od 2a00:1450:4016:800::1012: čas=89ms
Odpověď od 2a00:1450:4016:800::1012: čas=105ms

Statistika ping pro 2a00:1450:4016:800::1012:
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 89ms, Maximum = 109ms, Průměr = 102ms
```

Obr. 16. Ping google

Podle testů vidíme že vše funguje jak má. Nicméně již na první pohled vidíme poněkud vysokou odezvu. Tyto vysoké hodnoty nejsou způsobeny ani závadou na internetovém připojení ani chybou OS.

Teredo je použito pouze pokud síť vyžaduje připojení pomocí protokolu IPv6, defaultně je upřednostňován protokol IPv4.

Pokud bychom chtěli Teredo vypnout, nebo úplně odstranit použijeme tyto příkazy:

netsh int ipv6 set teredo disable

netst int ipv6 uninstall.

4.1.2 Teredo na OS Ubuntu 10.04

Nyní provedeme test připojení na OS Ubuntu 10.04. Podporu IPv6 v sobě má již Ubuntu implementovanou, je potřeba pouze instalace klienta Teredo. V Ubuntu se tento program jmenuje Miredo a jeho instalace je velmi jednoduchá.

Spustíme Terminál a zadáme příkaz:

sudo apt-get install miredo

Instalace by měla proběhnout naprosto bez jakýchkoliv problému.

Kontrolu můžeme opět provést zapsáním příkazu do Terminálu:

ifconfig

Výpis můžeme zkontrolovat na obrázku viz. níže.

```
nicknack@nicknack-desktop:~$ ifconfig
eth0      Link encap:Ethernet  HWadr 00:11:09:8a:f4:eb
          inet adr:192.168.1.25  Všesměr:192.168.1.255  Maska:255.255.255.0
          inet6-adr: 2001:67c:2194:fff1:211:9ff:fe8a:f4eb/64 Rozsah:Globál
          inet6-adr: fe80::211:9ff:fe8a:f4eb/64 Rozsah:Linka
          AKTIVOVÁNO VŠESMĚROVÉ_VYSÍLÁNÍ BĚŽÍ MULTICAST  MTU:1500  Metrika:1
          RX packets:45830 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46085 errors:0 dropped:0 overruns:0 carrier:0
          kolizí:0 délka odchozí fronty:1000
          Přijato bajtů: 17362977 (17.3 MB) Odesláno bajtů: 37496922 (37.4 MB)
          Přerušení:16 Vstupně/Výstupní port:0xec00

lo        Link encap:Místní smyčka
          inet adr:127.0.0.1  Maska:255.0.0.0
          inet6-adr: ::1/128 Rozsah:Počítač
          AKTIVOVÁNO SMYČKA BĚŽÍ  MTU:16436  Metrika:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          kolizí:0 délka odchozí fronty:0
          Přijato bajtů: 960 (960.0 B) Odesláno bajtů: 960 (960.0 B)

tun0      Link encap:NEZNÁM  HWadr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet6-adr: fe80::ffff:ffff:ffff/64 Rozsah:Linka
          inet6-adr: 2001:0:53aa:64c:20a7:7410:a76d:2b22/32 Rozsah:Globál
          AKTIVOVÁNO POINTOPOINT BĚŽÍ NEARP MULTICAST  MTU:1280  Metrika:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          kolizí:0 délka odchozí fronty:500
          Přijato bajtů: 0 (0.0 B) Odesláno bajtů: 144 (144.0 B)

nicknack@nicknack-desktop:~$
```

Obr. 17. Ifconfig

Zda je připojení plně funkční opět vyzkoušíme pomocí příkazu:

ping6 ipv6.google.com

```
nicknack@nicknack-desktop:~$ ping6 ipv6.google.com
PING ipv6.google.com(muc03s01-in-x11.1e100.net) 56 data bytes
64 bytes from muc03s01-in-x11.1e100.net: icmp_seq=1 ttl=57 time=125 ms
64 bytes from muc03s01-in-x11.1e100.net: icmp_seq=3 ttl=57 time=141 ms
64 bytes from muc03s01-in-x11.1e100.net: icmp_seq=4 ttl=57 time=109 ms
64 bytes from muc03s01-in-x11.1e100.net: icmp_seq=5 ttl=57 time=110 ms
64 bytes from muc03s01-in-x11.1e100.net: icmp_seq=6 ttl=57 time=100 ms
64 bytes from muc03s01-in-x11.1e100.net: icmp_seq=8 ttl=57 time=171 ms
^C
--- ipv6.google.com ping statistics ---
9 packets transmitted, 6 received, 33% packet loss, time 8022ms
rtt min/avg/max/mdev = 100.514/126.663/171.467/24.057 ms
nicknack@nicknack-desktop:~$
```

Obr. 18. Ping6 google

Vše opět v pořádku funguje jen stejně jako u OS Windows opět vyšší hodnota odezvy. Pro kontrolu vyzkoušíme odezvu přes IPv4.

Obr. 19. Ping IPv4 google

Tady vidíme, že linka pro připojení je v pořádku.

5 Popis konfigurace směrovačů

Pro nastavení směrovačů bylo použito RouterBoardů a systému Mikrotik verze 5.16 kvůli jejich cenové dostupnosti a rozšíření u malých a středních firem. Jako routovací protokol byl zvolen OSPFv3, z důvodů plného dokončení pro systém Mikrotik a jeho vhodnost pro středně velké sítě. Variantou by byl protokol BGP4+, který bude ovšem implementován až ve verzi 6 a zatím je uvolněna pouze zkušební verze.

5.1 Konfigurace RB Mikrotik a OSPFv3

Pomocí utility Winbox se připojíme postupně do každého z RB a zkontrolujeme zda jsou spuštěny potřebné balíčky pro realizaci. Provedeme pomocí záložky New Terminal v základním menu a zadáním příkazu :

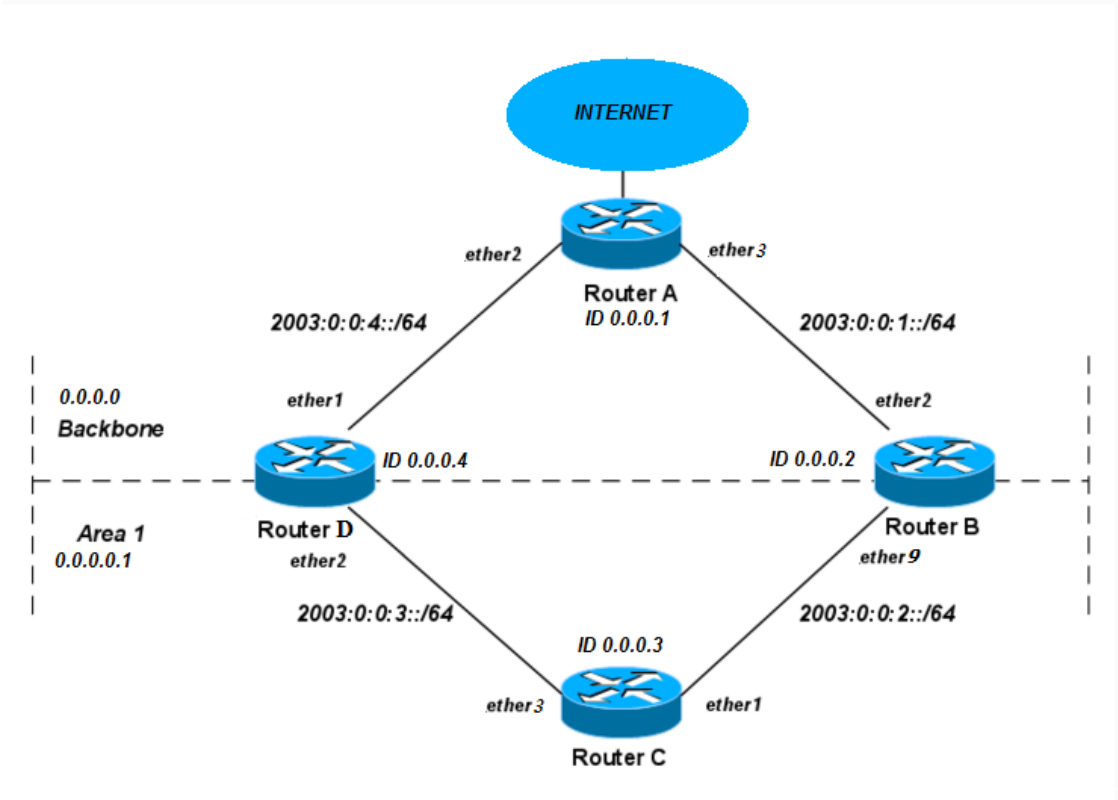
[admin@Nicknackova_zahradka] /system package> print

zobrazí se výpis balíčků a jejich verze:

1. *routeros-mipsle* *5.16*
2. *systém* *5.16*
3. *mpls* *5.16*
4. *ipv6* *5.16*
5. *wireless* *5.16*
6. *routing* *5.16*
7. *dhcp* *5.16*
8. *routerboard* *5.16*
9. *hotspot* *5.16*
10. *advanced-tools* *5.16*
11. *security* *5.16*
12. *ppp* *5.16*

Ne všechny jsou nezbytné pro realizaci, ale pokud máme RB s dostatečným výkonem není nutné je zakazovat. Pro účely realizace routováni OSPFv3 jsou potřebné hlavně balíčky *ipv6* a *routing* (balíčky nutné pro chod routerboardu nezmiňujeme). Tuto kontrolu provedeme na všech použitých RB. Dále je ještě vhodné, abychom měli na všech RB shodnou verzi OS Mikrotik. Můžeme se tak vyhnout pozdějším problémům z nekompatibilitou. V našem případě je použita poslední stabilní verze 5.16

Nastavení routování bude provedeno podle následujícího schématu zapojení:



Obr. 20. Struktura sítě pro OSPFv3

Kompletní specifikace hardwaru je uvedena v příloze této práce PI : Použitý hardware [7].

Nastavení routeru A:

/ipv6 address

add address=2003::1:0:0:0:1/64 advertise=no interface=ether3

add address=2003::4:0:0:0:1/64 advertise=no interface=ether2

add address=2003::1/64 advertise=no interface=WLAN1

/routing ospf-v3

set router-id=0.0.0.1 distribute-default=always-as-type-1

/routing ospf-v3 interface

add interface=ether3 area=backbone

add interface=ether2 area=backbone

Nastavení routeru B:

/ipv6 address

add address=2003::1:0:0:0:2/64 advertise=no interface=ether2

add address=2003::2:0:0:0:2/64 advertise=no interface=ether9

/routing ospf-v3

set router-id=0.0.0.2

/routing ospf-v3 area

add area-id=0.0.0.1 name=area1

/routing ospf-v3 interface

add interface=ether2 area=backbone

add interface=ether9 area=area1

Nastavení routeru C:

/ipv6 address

add address=2003::2:0:0:0:3/64 advertise=no interface=ether1

add address=2003::3:0:0:0:3/64 advertise=no interface=ether3

/routing ospf-v3

set router-id=0.0.0.3

/routing ospf-v3 area

add area-id=0.0.0.1 name=area1

/routing ospf-v3 interface

add interface=ether1 area=area1

add interface=ether3 area=area1

Nastavení routeru D:

/ipv6 address

add address=2003:0:0:3::4/64 advertise=no interface=ether1

add address=2003:0:0:4::4/64 advertise=no interface=ether2

/routing ospf-v3

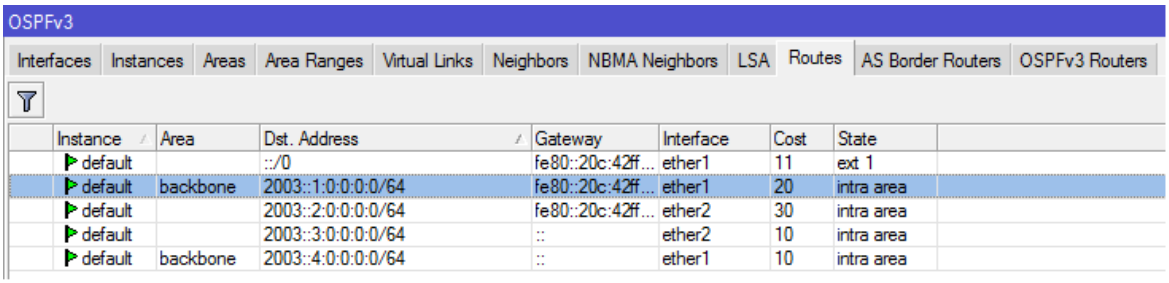
set router-id=0.0.0.4

/routing ospf-v3 interface

add interface=ether1 area= backbone

add interface=ether2 area=area1

Pokud jsme správně nakonfigurovali, musíme v záložce „Routes“ vidět routy z okolních routerů:



Obr. 21. OSPFv3 routers

Ve sloupci „Cost“ je zobrazen výpočet délky trasy na danou routu. Podle této hodnoty určuje OSPFv3 nejkratší cestu pro doručení paketu.

Pokud tedy porovnáme OSPF a OSPFv3, ze stránky konfigurace, nedošlo k žádným výrazným změnám, pouze zápis adresy je ve formátu IPv6 a volbu nastavení v záložce Networks, kde přiřadíme routovaný subnet, např. 10.0.0.0/24 na zvolenou Areu. U IPv4 můžeme zvolit volbu heslovat spojení routerů (MD5 metodou), které u IPv6 není možno zvolit. Veškeré ostatní nastavení zůstává stejné i označení arén, ID routerů.

6 Popis rozdílů konfigurace DNS serveru pro IPv4 a IPv6

6.1 Instalace BIND9

Instalace je velmi jednoduchá. Stačí zadat do terminálu příkaz :

sudo apt-get install bind9

Instalace by měla proběhnout bez jakýchkoliv problémů.

6.2 Konfigurace BIND9

Nyní, aby bylo možno naslouchání na IPv6, je třeba funkci povolit. Před jakoukoliv editací souborů se doporučuje dotyčný soubor zálohovat. Ušetříme si možné potíže.

Naslouchání IPv6 nalezneme v souboru:

named.conf.options

nalezneme a upravíme položku:

listen-on-v6 { any; }; nebo místo „any“ můžeme vypsat konkrétní IP

nyní pokud to bude možno, bude BIND preferovat záznamy IPv6.

Pokud máme hotovo, přistoupíme k samotnému nakonfigurování pro určitou doménu.

Nalezneme soubor:

named.conf.local

a zde můžeme v daném tvaru vložit odkaz na zónový soubor obsahující údaje o hostované doméně. Zápis by měl být v tomto tvaru:

```
zone „jméno_domény“ {
        type master;
        file “jméno_souboru”;
        };
```

pro konkrétní doménu by záznam vypadal takto:

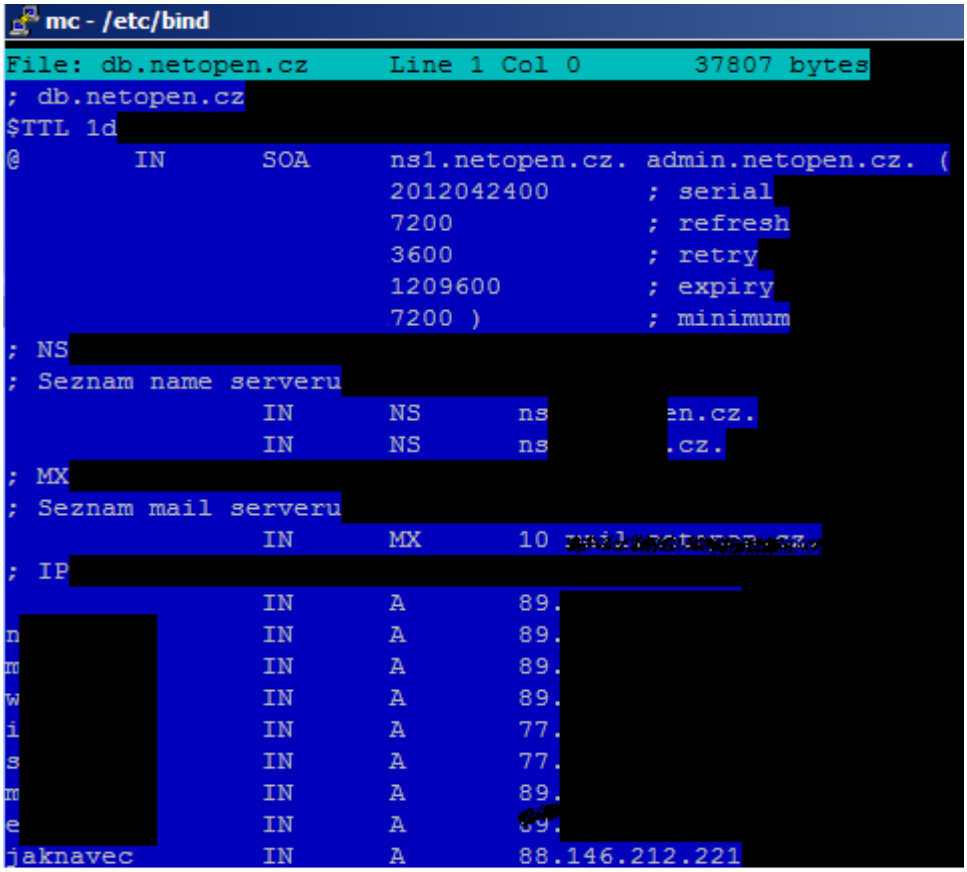
zone *„netopen.cz“* {

type master;

file “/etc/bind/db.netopen.cz”;

};

Nyní podle zadané cesty vytvoříme zónový soubor s názvem db.netopen.cz a vložíme definovanou hlavičku a vyplníme údaje. Soubor vypadá následovně:



Obr. 22. Zónový soubor

Na posledním řádku vidíme záznam „jaknavec“ s označením „A“ a adresou 88.146.212.221.

Tento záznam značí, že se jedná o záznam IPv4. To poznáme podle označení A a hlavně podle tvaru veřejné IP.

Abychom měli tento záznam dostupný i pod IPv6 provedeme na další řádek tento zápis:

jaknavec IN AAAA 2a01:5e0::3:12e

Čímž byl vytvořen odkaz na IPv6.

Nyní je potřeba ještě vytvoření reverzního záznamu (zpětný překlad)

U zpětného překladu na IPv6 již neplatí možnost zkráceného zápisu pomocí „::“, ale je nutno adresu zapsat od zadu do předu a každé číslo oddělit tečkou.

6.2.1 Reverzní záznam IPv6

První tedy reverzní zápis pro tvar IPv6.

Adresa *2a01:5e0::3:12e* je přidělena s prefixem /126

Díky prefixu /126 bude reverzní tvar prefixu domény ve tvaru:

0.0.e.5.1.0.a.2.ip6.arpa

Reverzní záznam pro naši subdoménu „jaknavec“ bude vypadat takto:

0.e.2.1.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR jaknavec.netopen.cz

(čísla jsou barevně odlišena jen pro přehlednost)

6.2.2 Reverzní záznam IPv4

Pro protokol IPv4 bude reverzní záznam uveden jako soubor:

212.146.88.addr-in.arpa

Tento rozsah vlastníme např. v masce /24 a reverzní záznam pro adresu 88.146.212.221 bude uveden jako:

221 IN PTR jaknavec.netopen.cz

Pokud vlastníme jen jednu dotyčnou veřejnou IP bude zápis ve tvaru:

221.212.146.88 IN PTR jaknavec.netopen.cz

Výpis z reverzního souboru IPv4 vidíme na obrázku níže:

```
File: 212.146.~dr.arpa  Line 1 Col 0       8425 bytes
; 212.146.88.addr-in.arpa
$TTL 1d
@       IN      SOA     ns[redacted].cz. [redacted].cz  (
                        2009031900      ; serial
                        7200            ; refresh
                        3600            ; retry
                        1209600         ; expiry
                        7200 )          ; minimum
; Seznam name serveru
        IN      NS      ns1.[redacted].cz.
        IN      NS      ns2.[redacted]n.cz.
        IN      NS      ns3.[redacted].cz.
;
; ---------------------------------------------------------------------------
; Seznam reverzenich zaznamu pro routery
; Po pridani routeru zakomentovat reverzni zaznam IP adresy
; ---------------------------------------------------------------------------

;
; ---------------------------------------------------------------------------
; Seznam reverznich zaznamu
; Subnet 88.146.212.0 / 24
; ---------------------------------------------------------------------------
;
1       IN      PTR     1.212.netopen.cz.
2       IN      PTR     2.212.netopen.cz.

221     IN      PTR     jaknavec.netopen.cz.
```

Obr. 23. Reverzní záznam

Při srovnání DNS záznamů protokolu IPv4 a IPv6 vidíme odlišnost v označení

IPv4 : A IPv6 : AAAA

Další změna je v označení konce reverzního záznamu kdy oproti protokolu IPv4 došlo u IPv6 k označení : **ipv6.arpa**

Problémem také nastává při zapisování 128 bitové délky adresy IPv6, kdy kvůli nepřehlednosti může dojít lehce k omylu.

7 Porovnání vlastností IPv6 s IPv4

Tab. 5 Porovnání IPv6 a IPv4

IPv6	IPv4
velikost adresy 128bitů	velikost adresy 32 bitů
nezapamatovatelný název IP adresy bez reverzního záznamu	zapamatovatelný tvar IP adres
zápis v 16-kové soustavě	oddělení části IP pomocí „ **.** „
oddělení částí pomocí “ **:** „	již nedostačující velikost protokolu
možnost zkracování zápisu IP adresy ::	ARP tabulka
obrovská kapacita kombinací IP adrese	rozsah podsítě udáván maskou
možnost aby každé zařízení v síti mělo svoji unikátní IP	
vyšší bezpečnost (odolnost proti DDoS)	
místo masky sítě prefix	

ZÁVĚR

Cílem této práce bylo popsat rozdíly konfigurace protokolu IPv6 proti starému IPv4. V první části nalezneme popis základních vlastností IPv6, v následující části dostupné možnosti nakonfigurování na nejpoužívanějších OS. Dále je pak popsána možnost konfigurace směrovače za pomocí protokolu OSPFv3. V předposlední kapitole jsou uvedeny rozdíly konfigurace DNS serveru. Jako poslední je uvedeno základní porovnání obou protokolů.

Během vytváření této práce byl vždy největším problém nutnost omezovat se výběrem technologie, která daný protokol IPv6 podporuje, ať již třeba testovaný protokol OSPFv3. Nicméně pokud již podpora IPv6 v dané technologii měla implementovanou podporu, většinou byl její chod již bez problému. Slovem většinou je naráženo na operační systém MS Windows XP, ve kterém i po doinstalováni podpory IPv6, měl systém při používání Tereda nepochopitelné výpadky, které jak bylo v odborných článcích zjištěno, byly naprosto běžné i při zkoumání jinými odborníky v jejich laboratořích.

Při porovnání základních vlastností protokolu IPv4 s IPv6 bylo zjištěno, že nový protokol starý předčí nejen v kapacitě, ale také v bezpečnosti kde je plánována pro každé síťové rozhraní unikátní IP.

Protokol IPv6 bude jistě dobrým nástupcem starého protokolu IPv4 a v mnoha směrech jej předčí. Nicméně hlavní hnací silou, k jeho masivnější propagaci budou muset být velké firmy jako například Google nebo Microsoft, které donutí výrobce IT techniky a menší poskytovatele internetu k jeho běžnějšímu použiti.

CONCLUSION

The main goal of this work was to describe differences in configuration of protocol IPv6 compared to older IPv4. In first part of this work, we can find description of basic properties of IPv6, in next part we can find available options of protocol configuration used with the most common OS. Next is following description of possible configuration of router, using protocol OSPFv3. Last but one chapter describes differences in DNS server configuration. Last chapter is focused on comparison of both protocols.

During writing this work the biggest problem was always the neccessity restrict the choose of a technology which support the protocol IPv6, for example tested protocol OSPFv3. Nevertheless if the support IPv6 in this technology had implemented support, it mostly worked without a problem. With a word mostly I think of operating system MS Windows XP, in which even after installing support IPv6 the system had understandable power cut using Tereda. I found out in specialised articles these are common even in examine by specialists in their labs.

When comparing basic properties of protocol IPv4 and IPv6, it was find out that new protocol is much better not only in its capacity,but also in security, where is planned unique IP for every single network interface.

Protocol IPv6 will be a good successor of the old protocol IPv4 and it will really overtop it in many ways. In my opinion the main virtue to its massive publicity the big companies like Google or Microsoft will be crutial. They will force producers of IT technology and smaller internet provider to more common usage.

SEZNAM POUŽITÉ LITERATURY

[1] Wikipedie: Otevřená encyklopedie. *Internet* [online]. 2012, 9. 5. 2012 [cit. 2012-05-10]. Dostupné z: http://cs.wikipedia.org/wiki/Internet#Historie

[2] SATRAPA, Pavel. *IPv6*: *internetový protokol IPv6*. Praha: CZ.NIC, 2008, CZ.NIC. ISBN 978-80-904248-0-7.

[3] Wiki.mikrotik. *Mikrotik* [online]. 2010 [cit. 2012-05-13]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:IPv6/Address

[4] DiffServ – The Scalable End-to-End QoS Model. *Cisco* [online]. 2005 [cit. 2012-05-13]. Dostupné z: http://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f.html

[5] Protocol Numbers. *IANA — Internet Assigned Numbers Authority* [online]. 2011 [cit. 2012-05-13]. Dostupné z: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml

[6] IPv6 address allocation and assignment policy. *APNIC Pty. Ltd.* [online]. 1999 – 2012 [cit. 2012-05-13]. Dostupné z: http://www.apnic.net/policy/ipv6-address-policy

[7] MIKROTIK. *RouterBoard* [online]. 2002 [cit. 2012-05-27]. Dostupné z: http://routerboard.com

[8] GEOFF HUSTON. *IPv6 Transition Tools and Tui* [online]. 2008 [cit. 2012-05-28]. Dostupné z: http://www.potaroo.net/ispcol/2008-02/tui.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAAA	mapuje jméno DNS záznamu pro IPv6
A	mapuje jméno DNS záznamu pro IPv4
ARP	Address Resolution Protocol
arpa	doména nejvyššího řádu používaná pouze pro vnitřní potřeby
BIND	Berkley Internet Name Domain
Bit	Binární číslo
Byte	Jednotka 8 binárních číslic
DDoS	Denial of Service (Odmítnutí služby)
IANA	Internet Assigned Numbers Authority
ICMP	Internet control message protocol
LAN	Local Area Network
MTU	Maximum transmission unit
NAT	Network address translation
OS	Operační systém
OSPFv3	Open Shortest Path First
IPv4	Internet protokol verze 4
IPv6	Internet protokol verze 6
ping	Packet Internet Groper
RB	Router Board
RIP	Hlavní registrátor domén a IP adres pro Evropu a blízký východ

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: POUŽITÝ HARDWARE

RB493AH – Router B

Produkt	RB493AH
CPU	680Mhz
RAM	128MB
LAN porty	9
MiniPCI porty	3
Napájení	10-28V
Provozní rozsah	-30C až +60
RouterOS Licence	Level 5

RB493 – Router C

Produkt	RB493
CPU	300Mhz
RAM	64MB
LAN porty	9
MiniPCI porty	3
Napájení	10-28V
Provozní rozsah	-30C až +60
RouterOS Licence	Level 4

RB500r5 – Router A

Produkt	RB500r
CPU	400Mhz
RAM	32MB
LAN porty	3
MiniPCI porty	2
Napájení	10-28V
Provozní rozsah	-20C až +70
RouterOS Licence	Level 5

RB600 – Router D

Produkt	RB600
CPU	400Mhz
RAM	128MB
LAN porty	3
MiniPCI porty	4
Napájení	10-48V
Provozní rozsah	-20C až +70
RouterOS Licence	Level 5