Univerzita Pardubice
Fakulta ekonomicko-správní

Nasazení IPv6 v komunikační infrastruktuře firmy

Kateřina Štěpánková

Bakalářská práce
2009

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2008/2009**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Kateřina ŠTĚPÁNKOVÁ**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informatika ve veřejné správě**
Název tématu:	**Nasazení IPv6 v komunikační infrastruktuře firmy.**

Zásady pro vypracování:

Rozbor standardu IPv6
Pořízení informací o síťové infrastruktuře sledovaného subjektu
Vypracování návrhu na přechod na IPv6
Kalkulace nákladů na upgrade zařízení a síťové podpory systémů

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

DOSTÁLEK L., KABELOVÁ A. Velký průvodce protokoly TCP/IP a systémem DNS. 3. vyd. Brno. Computer Press, 2002. 542 s. ISBN 80-7226-675-6

PETERKA J. Archiv článků [online]. Dostupný z WWW: {http://www.earchiv.cz/}.

PUŽMANOVÁ R. TCP/IP v kostce. České Budějovice. Kopp, 2004. 607 s. ISBN 80-7232-236-2

SATRAPA P. IP verze 6. Praha. Neocortex, 2002. 238 s. ISBN 80-86330-10-9

TANENBAUM A.S. Computer Networks, Fourth Edition. Pearson Education, 2003. 891 s. ISBN 0-13-038488-7

Vedoucí bakalářské práce: **Ing. Oldřich Horák**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **6. října 2008**

Termín odevzdání bakalářské práce: **1. května 2009**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 6. října 2008

Prohlašuji:

Tuto práci jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena 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 25. dubna 2009

Kateřina Štěpánková

Na tomto místě bych ráda poděkovala Ing. Oldřichu Horákovi, vedoucímu mé bakalářské práce, za jeho velmi cenné rady, pomoc při tvorbě tohoto textu a čas, po který se mi věnoval v rámci konzultací.

Anotace

Tato práce je zaměřena na nový internetový protokol verze 6. Tento protokol je zde popsán a na modelové firmě je ukázáno, jaká zařízení potřeba vyměnit, nebo upgradovat tak, aby byla síťová infrastruktura schopna pracovat na tomto protokolu. V práci jsou také uvedeny finanční náklady a časová náročnost této změny.

Klíčová slova

ipv6, dhcpv6, dvojí zásobník, 6to4, server, přepínač, směrovač, náklady

Title

The implementation of IPv6 in the Company Communication Infrastructure

Anotation

This work is aimed at new Internet protocol version 6. This protocol is described herein and it is shown which devices have to be replaced or upgraded so that the network infrastructure could work on the protocol. There are financial costs stated in this work as well as the time needed for such modification.

Keywords

ipv6, dhcpv6, dual stack, 6to4, server, switch, router, costs

Obsah

1 Úvod

V současné době se uplatňuje široké využívání internetových služeb. K Internetu se připojuje stále více zařízení a tudíž stoupá i spotřeba veřejných adres, kterých začíná velmi rychle ubývat. Zatím se jako řešení tohoto problému využívá různých opatření, která překládají veřejné adresy na neveřejné. Tyto mechanismy s sebou nesou spoustu nevýhod a komplikací. Jako řešení těchto problémů, a to především nedostatkek veřejných IP adres, byl vytvořen nový internetový protokol verze 6 (odkud je název IPv6). Rozsah adres je zde mnohonásobně větší než u internetového protokolu verze 4.

V České republice je implementace protokolu IPv6 ve firemních sítích ve srovnání např. s Asií nebo USA výrazně nižší. Spousta firem odkládá modernizaci své sítě na pozdější dobu. Tento fakt potvrzuje i to, že v českém jazyce je jen velmi málo publikací, které by se přechodem na protokol IPv6 zabývaly. A právě tímto tématem, tedy zavedením IPv6 do praxe, se zabývá tato bakalářská práce. Měla by zároveň i posloužit ostatním firmám jako návod, co je potřeba v dosavadní infrastruktuře změnit, aby bylo možné protokol IPv6 využívat.

V prvních kapitolách je obecně protokol IPv6 popsán. Jelikož se jedná o velmi rozsáhlé téma, jsou zde popsané jen některé vlastnosti tohoto protokolu. Jsou to především ty, které se liší od jeho předchůdce IPv4, a které jsou potřeba k zavedení tohoho protokolu do provozu. Po této kapitole se čtenář seznámí s mechanismy přechodu, ve které je zároveň popsané, jakých prvků sítě se modernizace bude týkat. Poté následuje kapitola, ve které je na příkladu firmy uvedeno, jaké kroky by právě ona měla podniknout k tomu, aby mohla tento protokol ve své infrastruktuře využívat. Závěrečnou kapitolu tvoří kalkulace nákladů na tento přechod a také samozřejmě závěr, kde je shrnuta problematika přechodu na protokol IPv6.

Cílem této práce je seznámit čtenáře s protokolem IPv6 a na modelové firmě ukázat, jaké kroky je nutné podniknout, aby mohl být tento protokol implementován ve firemní infrastruktuře. Jedním z cílů je i ukázat, jak je tento proces nákladný z hlediska financí a času.

2 Popis protokolu IPv6

V této kapitole je popsán Internet Protokol verze 6 (ve zkratce IPv6), který je v některé literatuře označován i jako IP Next Generation (Ipng), jeho vývoj i některé odlišnosti od stávajícího Internet Protokolu verze 4 (IPv4).

2.1 Vývoj protokolu IPv6

Na začátku 90. let 20. století začalo být zřejmé, že jednoho dne dojde k vyčerpání adresního prostoru, který je dostupný v IPv4. Díky poměrně velkému množství času, které bylo k řešení tohoto problému, se rozhodlo IETF navrhnout nový protokol, který vyřeší nejen problém adresního prostoru, ale dokázal by ho rozšířit i o další nové vlastnosti.
Dle [1] to byly zejména tyto požadavky:

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

V roce 1995 byla vydána sada RFC definujících IPv6. Konkrétně se jedná o *RFC 1883: Internet Protocol, Version 6 (IPv6) Specification* [2].

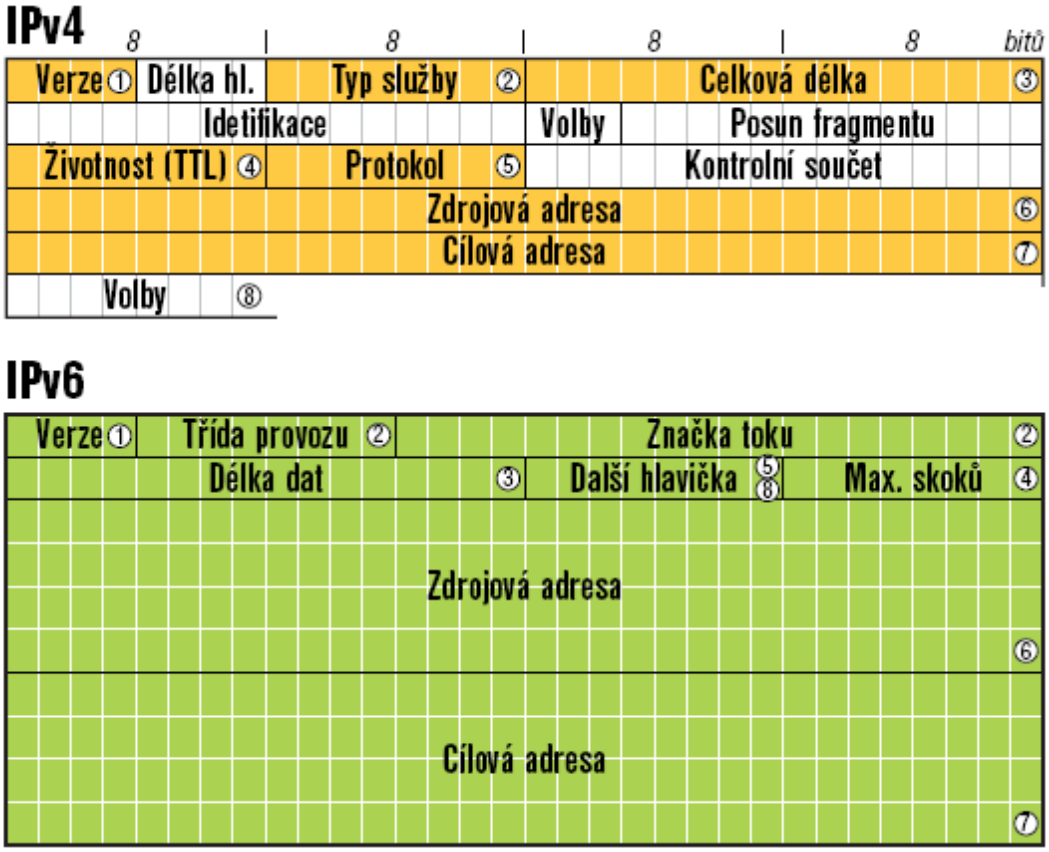
I když bylo nyní možné nový protokol implementovat, nedošlo k tomu tak, jelikož byly zavedeny metody, jak ušetřit adresy IPv4 – zpřísnila se kritéria pro jejich přidělování nebo byly zavedeny mechanismy pro překlad adres – Network Address Translation (NAT), díky kterému si celá vnitřní síť vystačí s jednou veřejnou IP adresou. NAT ovšem přináší i velkou nevýhodu v podobě nemožnosti přímé komunikace dvou počítačů, ležících v odlišných

NATovaných sítích. Pro implementaci IPv6 je tu i fakt, že podle [3] by IPv4 adresy měly být vyčerpány v roce 2011 – 2012.

2.2 Formát datagramu

Formátem datagramu IPv6 se zabývá dokument *RFC 2460: Internet Protocol, Version 6 (IPv6) Specification* [4], který vyšel v roce 1998.

„Datagram má v IPv6 obvyklý základní tvar: začíná hlavičkami, za kterými pak následují nesená data“ [1]. Ovšem oproti hlavičce v IPv4 je standardní hlavička s konstatní velikostí minimalizovaná a obsahuje jen nejnutnější pole, ostatní méně důležité pole byly přesunuty do rozšiřujících hlaviček. To, jak je datagram minimalizován je znázorněno na obrázku 1 kde jsou porovnány hlavičky jak IPv4, tak IPv6. Zakroužkovaná čísla znázorňují, která pole si vzájemně odpovídají.



Obrázek 1: Porovnání hlaviček IPv4 a IPv6 [1]

2.2.1 Popis jednotlivých polí IPv6 hlavičky

Verze – stejně jako u IPv4 identifikuje verzi protokolu, tudíž zde obsahuje hodnotu 6.

Třída provozu – v tomto poli se specifikuje priorita datagramů, což vede k jejich prioritnímu zpracování. Naopak při zahlcení sítě určuje, které datagramy budou zahozeny. Implicitní hodnota je 0.

Značka toku – myšlenka spočívá v tom, že datagramy jednoho toku dat datagramů dostanou svou identifikaci. Pak stačí, aby směrovač vyřešil úlohu do kterého rozhraní datagram předat a do paměti si poznamenal výsledek. Pro další datagram nejprve prohlédne paměť a pokud by tam nenašel poznamenaný tok, tak řeší úlohu směrování. Další datagramy stejného toku pak bude předávat do stejného rozhraní aniž by řešil úlohu směrování – pouze na základě údajů v paměti [5].

Max. skoků – neboli Hop limit – slouží jako ochrana před zacyklením průchodu datagramu. Odesílatel uvede maximální počet skoků, tedy počtu průchodu datagramu jedním směrovačem, a každý směrovač po průchodu datagramu sníží tento počet o jedničku. Jakmile tento počet dosáhne nuly, datagram bude zlikvidován a odesílateli bude odeslána ICMPv6 zpráva o vypršení maximálního počtu skoků.

Délka dat – toto pole nese údaje o počtu bajtů, které jdou za standardní hlavičkou. Tato položka je dvoubajtová, tudíž maximální délka může být 64KB. Pokud by bylo potřeba většího datagramu, je zde možnost použití rozšiřující hlavičky *Jumbo obsah*.

Adresy – jak je z obrázku patrné, tyto dvě položky zabírají 80% celé hlavičky. Adresám se věnuje kapitola 2.6 .

Další hlavička – toto pole je novinkou v IPv6, propojuje jednotlivé jdoucí hlavičky mezi sebou a nese informace o tom, jakého typu je hlavička, která jde za tou stávající.

Typy rozšiřujících hlaviček jsou shrnuty v tabulce 1 a typy nesených dat v tabulce 2.

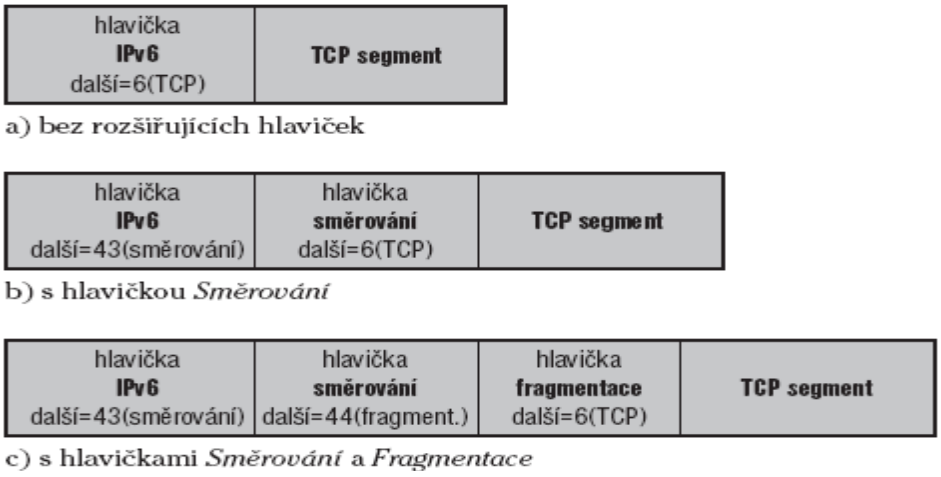
Tabulka 1: Typy dalších hlaviček [1]

0	volby pro všechny (hop-by-hop options)
43	směrování (routing)
44	fregmentace (fragment)
50	šifrování obsahu (ESP)
51	autentizace (AH)
59	poslední hlavička (no next header)
60	volby pro cíl (destination options)
135	mobilita (mobility)

Tabulka 2: Typy přenášených dat [1]

6	TCP
8	EGP
9	IGP
17	UDP
46	RSVP
47	GRE
58	ICMPV6

Na obrázku 2 je vidět, jak vypadá paket, kde nejsou žádné zřetězené hlavičky, kde je jedna zřetězená hlavička *Směrování* a kde jsou 2 zřetězené hlavičky *Směrování* a *Fragmentace*.



Obrázek 2: Zřetězení hlaviček datagramu [1]

Pokud by směrovač musel procházet dlouhým řetězcem hlaviček, mohlo by dojít ke snížení jeho výkonu. Proto bylo stanoveno následující pořadí rozšiřujících hlaviček:

1. základní hlavička IPv6
2. volby pro všechny (hop-by-hop options)
3. volby pro cíl (destination options) – pro průběžného adresáta z hlavičky *Směrování*
4. směrování (routing)
5. fragmentace (fragment)
6. autentizace (authentication)
7. šifrování obsahu (encapsulating security payload)
8. volby pro cíl - pro konečného příjemce datagramu
9. mobilita (mobility)

Kromě rozšiřující hlavičky *Volby pro cíl*, která se může vyskytnout před rozšiřující hlavičkou *Směrování* a před *Mobilitou*, by se všechny hlavičky měly vyskytnout nanejvýše jednou.

2.3 ICMPv6

Stejně jako u IPv4 i zde existuje protokol, jehož hlavní funkcí je ohlašování chyb při přenosu paketů. Je definován v *RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

„The ICMPv6 header is identified by a Next Header value of 58 in the immediately preceding header.“ [8]

Formát ICMPv6 zprávy je uveden na obrázku 3.

Obrázek 3: Formát ICMPv6 zprávy [1]

Zprávy, které tento datagram nese jsou dvojího typu: **chybové zprávy** (položka *Typ* leží v intervalu 0 – 127) a **informační** (položka *Typ* je z intervalu 128 – 255).

Aktuální přehled všech definovaných typů je uveden v [1].

2.4 Objevování sousedů

Nebo-li v originále Neighbor Discovery (ND) je podrobně popsán v *RFC 2461: Neighbor Discovery for IP Version 6 (IPv6)*.

V IPv4 se k hledání lokální síťové (např. ethernetové) adresy zabýval protokol ARP (Address Resolution Protocol). ND slouží mimo jiné k těmto účelům:

Zjišťování linkových adres uzlů ve stejné lokální síti:

tato funkce se od ARP liší jen v názvech a adrese, na kterou tazatel zasílá svůj dotaz.

„Pro potřeby objevování sousedů byl definován hlouček skupinových adres, na něž se rozesílají dotazy. všechny mají společný prefix ff02:0:0:0:0:1:ff00/104. Uzel, který hledá linkovou adresu pro určitou IPv6 adresu, vezme posledních 24 bitů hledané IP adresy a připojí je za výše uvedený prefix. Tím získá skupinovou adresu, na kterou zašle svůj dotaz.“ [1]

Tato adresa se nazývá adresa pro *vyzývaný uzel* a na ni se zašle ICMPv6 zpráva *výzva sousedovi*. Když bude uzel s danou IP adresou aktivní, bude přihlášen do příslušné skupiny a výzvu

tedy obdrží, zareaguje na ni zprávou *ohlášením souseda*, kde jsou informace o jeho linkové adrese.

Detekce dosažitelnosti souseda je proces, kdy uzel neustále aktivně sleduje, zda jsou v dosahu sousedi, se kterými komunikuje. K ověření využívá potvrzení z vyšší vrstvy (např. TCP), že komunikace probíhá. V druhém případě, kdy toto potvrzení neobdrží, si dostupnost ověří vlastními silami tak, že zašle výzvu sousedovi a čeká zda obdrží odpověď nebo ne.

2.5 Automatická konfigurace

Tato vlastnost je jedna z mnoha výhod, které IPv6 přináší. Rozděluje se na stavovou a bezstavovou.

2.5.1 Bezstavová konfigurace

Představuje novinku v IPv6, která je založená na principu objevování sousedů. Funguje tak, že každý směrovač v různých intervalech rozesílá do sítí, ke kterým je připojený, tzv. *ohlášení směrovače*, kde jsou obsaženy podstatné parametry sítě, například tyto informace:

- zda se v síti používá i stavová konfigurace pro nastavení adresy
- zda klient může používat stavovou konfiguraci pro další parametry sítě, kromě adresy
- jaké je MTU zdejší sítě
- prefixy sítě

„Z ohlášení směrovačů (o které může při startu aktivně požádat pomocí výzvy směrovači) se počítač dozví, jaké adresy používá zdejší síť. K nim si doplní identifikátor rozhraní (typicky 64 bitů), který si jednoznačně vygeneruje ze své ethernetové adresy. Tak získá platné IPv6 adresy pro své rozhraní. Jejich jednoznačnost ověří pomocí detekce duplicit - pomocí výzvy sousedovi se dotáže, zda vytvořenou adresu již někdo nepoužívá. Dostane-li kladnou odpověď, nesmí adresu svému rozhraní nastavit a automatická konfigurace skončí neúspěšně.“ [21]

Podrobné vysvětlení této možnosti konfigurace je možné nalézt v *RFC 4862: Stateless Address Autoconfiguration*.

2.5.2 Stavová konfigurace (DHCPv6)

Stavová konfigurace vychází z již známého DHCP, který se využívá v IPv4. Zde nese podobné označení, tedy DHCPv6. Jelikož je to velmi obsáhlé téma, je zde popsané, jak tento mechanismus pracuje. Více informací lze dohledat v *RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6).*

Na DHCPv6 se podílí 3 zařízení: *klient* – což je stanice, která chce získat nějaké informace od *serveru* a *zprostředkovatel* – ten je tu proto, protože klient komunikuje se serverem pomocí lokální linkové vrstvy, tzn. že by na každé lince musel být server. Zprostředkovatel tedy může předávat DHCPv6 zprávy mezi klientem a serverem, pokud se nenacházejí ve stejné podsíti. Všechny typy DHCPv6 zpráv jsou v [1].

Pro servery a zprostředkovatele se používá také jednotný název *agent* – tedy někdo, kdo poskytne DHCPv6 odpověď a nachází se na lokální lince.

Pro komunikaci byly určeny následující skupinové adresy:
ff02::1:2 - adresa s dosahem v rámci linky, používaná klienty ke komunikaci se servery a agenty, kteří jsou členy této skupiny adresy.
ff05::1:3 – adresa s dosahem v rámci sítě, používaná agenty ke komunikaci se servry, které jsou členy této skupiny adresy.

Důležitou součástí DHCPv6 je i **identifikace klientů a serverů**. U IPv4 se k tomuto účelu používala ethernetová adresa, ale zde se zavedl pojem *DHCPv6 Unique Identifer (DUID)*. Jedná se o unikátní identifikátor každého účastníka (tedy každého klienta a serveru), který by měl být trvalý v čase a neměl by záviset na klientově technickém vybavení.
Další identifikací je tzv. *identifikační asociace* (*identity association, IA*), používaná pro rozhraní, které jsou opatřeny jednoznačným identifikátorem („IAID“).

Průběh komunikace tedy probíhá následovně: klient vytvoří IA pro svá rozhraní a opatří je jednoznačnými identifikátory (IAID), vyšle výzvu na adresu ff02::1:2, pokud ho přijme server, tak obratem odpoví pomocí zprávy *ohlášení*, kde jsou uvedeny konfigurační parametry, které by klientovi přiřadil v případě, že by o ně klient žádal. Obsahuje i preference s jakou je server ochoten tyto parametry poskytnout. Pokud dotaz přijme zprostředkovatel, tak

předá dotaz všem DHCPv6 serverům, které má nakonfigurovány v seznamu (podle [1] to může být i obecná skupinová adresa všech DHCPv6 serverů daného místa, tedy ff05::1:3). Klient si z příchozích ohlášeních vytvoří seznam DHCPv6 serverů, které má k dispozici a podle nejvyšší preference si vybere server, kterému odešle zprávu *žádost*, která bude obsahovat DUID právě toho serveru, který si vybral. Protože v této fázi stále nemá potřebné informace o síti, pošle tuto zprávu opět na adresu všech DHCPv6 agentů, kde si ji cílový server vyhodnotí a pošle zpět zprávu *odpověď* s konfiguračními parametry.

Adresy jsou přidělovány pouze na určitý čas a pokud tento čas vyprší, klient musí žádat u serveru, který mu adresu poskytl, o prodloužení její platnosti zprávou *obnovení*. Může se stát, že neobdrží žádnou odpověď. V tomto případě zašle na všechny dostupné servery zprávu *převázání*, která nese dotaz, zda mu danou adresu neprodlouží některý jiný server.
Pokud končí klient svou existenci v síti, měl by o tom server také informovat zprávou *uvolnění.*

DHCPv6 řeší i situaci, kdy se klient vrátí do sítě (např. po fyzickém odpojení nebo po restartu). V této situaci si klient ověří zprávou *potvrzení*, ve které zašle aktuální parametry svých IA, zda jsou správné. Příslušný server opět raguje zprávou *odpověď*, ve které platnost přiřazení potvrdí nebo odmítne.

2.6 Adresy v IPv6

Jak již bylo zmíněno v první kapitole, blížící se vyčerpání IPv4 adres bylo jednou z priorit vzniku IPv6. Existuje tedy i dokument, který tyto adresy definuje a popisuje je. Jedná se o *RFC 4291: IP Version 6 Addressing Architecture* [6].

2.6.1 Druhy adres IPv6

Adresa v IPv6 je čtyřnásobně delší než adresa v IPv4, její délka je 128 bitů, což představuje $3{,}4 \cdot 10^{38}$ adres. Jsou tedy v podstatě nevyčerpatelné.
V tomto novém protokolu byly definovány 3 typy adres:

Individuální (unicast): Identifikuje právě jedno síťové rozhraní. Vyslaná data budou doručena právě tomuto rozhraní, které je identifikováno touto adresou.

Skupinové (multicast): Identifikují skupinu síťových rozhraní. Vyslaná data budou doručena všem členům této skupiny.

Výběrové (anycast): Představují novinku v IPv6 a jsou podobné skupinovým adresám, ale s tím rozdílem, že vyslaná data budou doručena pouze jedinému, nejbližšímu členovi.

2.6.2 Zápis adres

IPv6 adresu je možné zapsat třemi způsoby:

1. Preferovaná forma je x:x:x:x:x:x:x:x, kde „x“, které se vyskytuje osmkrát, vždy představuje čtyřmístné hexadecimální číslo. Pokud by na začátku každé části byla nula, není potřeba ji psát. Hodnota „0000“ lze zapsat jako „0“.

Například adresa 085B:2C5C:0000:0000:CD82:57FC:536C:D4C8:1DDD může být zapsána jako:

85B:2C5C:0:0:CD82:57FC:536C:D4C8:1DDD

2. Druhá forma zápisu je vhodná pro adresy, které obsahují řetězec nulových hodnot, ty se dají nahradit zdvojenou dvojtečkou „::“. Tento symbol se v zápisu adresy může objevit pouze jednou. Pokud by byl použit vícekrát, nedala by se zjistit původní adresa. Obsahuje-li počáteční hodnota řetězce 0, lze ji také vynechat.

Příklady možností zkracování jsou uvedeny v tabulce 6.

Tabulka 3: Možnosti zkracování adres [6]

Původní adresa	**Zkrácený tvar**
1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
FF01:0:0:0:0:0:0:101	FF01::101
0:0:0:0:0:0:0:1	::1
0:0:0:0:0:0:0:0	::
0123:1234:0:0:4567:fecd:ba47:4321	123:1234:0:0:4567:fecd:ba47:4321

3. Pro vyjádření IPv4 adres v některých přechodových mechanismech slouží tzv. IPv4-mapované adresy. Je to speciální případ IPv6 adresy, která obsahuje vloženou IPv4 adresu. Ta se vloží na místo posledních 4 bytů. Např. IPv4 adresa 147.230.49.73 může být buď ve formátu, kdy se převede do šestnáctkové soustavy:

::ffff:93e6:3149

nebo nemusí být převáděna a zápis by vypadal následovně:

::ffff:147.230.49.73

Podle [1] byl celý adresní prostor rozdělen podle typů adres do několika skupin, které sdružují IP adresy se společnou charakteristikou. Příslušnost k jednotlivým typům určuje prefix adresy. Rozdělení adres udává tabulka 4.

Tabulka 4: Rozdělení adres IPv6 [7]

Prefix	**Význam**
::/128	nedefinovaná adresa (uzel, který nemá přidělenou IPv6 adresu
::1/128	lokální smyčka (loopback)
FF00::/8 (1111 1111)	skupinová adresa
FE80::10 (1111 1110 10)	individuální lokální adresa segmentu
FEC0::/10 (1111 1110 11)	individuální lokální adresa místní
ostatní (001)	individuální globální

2.7 Domain Name Server (DNS)

DNS zde zastává obdobnou funkci jako u protokolu IPv4, ale zde je jeho role významější z toho důvodu, že IPv6 adresa se díky své délce těžko pamatuje i zapisuje. Specifikace záznamů pro DNS prošla bouřlivým vývojem. Nejprve bylo navrženo *RFC 1886: DNS Extensions to support IP version 6*, ve kterém byl pro IPv6 určen typ dopředného záznamu AAAA. Poté bylo vytvořeno *RFC 2874: DNS Extensions to Support IPv6 Address Aggregation and Renumbering*, kde bylo předchozí RFC označeno jako zastaralé a byly navrženy nové typy záznamů A6. To ovšem vyvolalo negativní ohlasy a až v roce 2003 vyšlo *RFC 3596: DNS Extensions to Support IP Version 6*, který se vrací k původnímu AAAA dopřednému záznamu. Tento RFC dokument také specifikuje doménu pro zpětné dotazy: ip6.arpa.

3 Přechod na IPv6

Tato kapitola se zabývá mechanismy přechodu na protokol IPv6 a také všemi prvky sítě, které se na tomto přechodu podílejí. Jsou zde popsané i nejčastěji používané operační systémy pro pracovní stanice.

3.1 Poskytovatelé připojení přes IPv6

Přestože se konec IPv4 blíží, není u nás v současné době mnoho internetových poskytovatů, kteří by nabízeli nativní připojení přes IPv6. Jelikož je téma této bakalářské práce zaměřeno na firmy, dostupnost připojení přes protokol IPv6 bylo zjišťováno u významných komerčních poskytovatelů Internetu v České republice. Bohužel ve většině případech se informace nedaly dohledat na jejich webových stránkách, takže výsledky byly zjištěny především mailovou komunikací a jsou uvedeny v následující tabulce:

Tabulka 5: Poskytovatelé IPv6 v České republice [Vlastní]

Název	**Poskytuje**	**Název**	**Poskytuje**
Tiscali	NE	Volný	ANO
GTS - Novera	NE	Telefonica 02	NE
Casablanca	ANO	Dial Telecom	ANO

3.2 Mechanismy přechodu

V této kapitole jsou popsány možnosti přechodu ze stávající IPv4 sítě na IPv6.

3.2.1 Nativní připojení

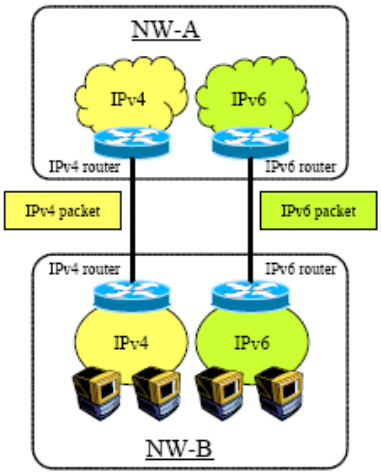
Pokud poskytovatel připojení přes protokol IPv6 umožňuje a samozřejmě i zařízení, které je třeba k němu připojit také, je možné se připojit nativně. Podle [1] nativní připojení znamená, že se datagramy IPv6 dají přenášet přímo a dají se použít individuální globální adresy z rozsahu, kterým poskytovatel disponuje.

Jak je vidět z obrázku 4, v tomto případě protokol IPv6 využívá celou infrastrukturu sítě a protokol IPv4 zde není podporován vůbec. Proto může být toto řešení v některých případech

finančně a časově nejnákladnější, zejména v těch případech, kdy koncová zařízení nepodporují IPv6 a je třeba je nahradit novými.

„When Native is used, it is possible to introduce IPv6 without affecting the IPv4 environment at all, however, the deployment cost is the largest. This method is suitable for critical cases where the IPv4 environment is stable.“ [17]

Na následujícím obrázku je tento typ připojení zobrazen.



Obrázek 4: Nativní připojení [17]

V případě, že poskytovatel neposkytuje nativní připojení přes IPv6, lze využít prostředků, které umožní současný provoz jak protokolu IPv4, tak i protokolu IPv6 a umožní tak plynulý přechod od jednoho k druhému.

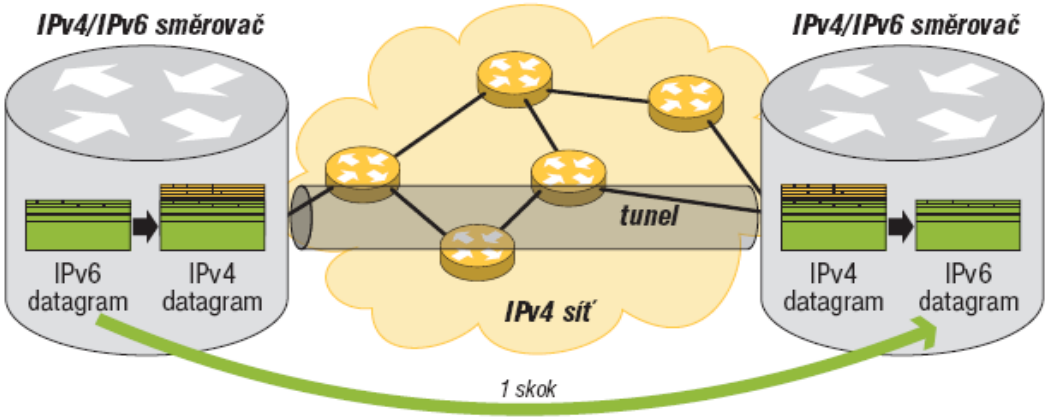
3.2.2 Tunelování paketů

Obecný mechanismus je podrobně popsán v dokumentu *RFC 2473: Generic Packet Tunneling IPv6 Specification.*

„V počátečních fázích přechodu na IPv6 mohou existovat IPv4-only ostrovy a zařízení v těchto ostrovech mohou komunikovat přes IPv4 oceán. Technikou pro tento typ komunikace je zapouzdření IPv6 do IPv4 paketů. To dovolí zařízením s IPv6 využívat stávající IPv4 infrastrukturu bez změny IPv4 komponent. Dual-stack router jednoduše vloží IPv6 hlavičku přímo za IPv4 hlavičku a pošle tento paket jako nativní IPv4 paket dále. Na druhé straně tunelu je další dual-stack router, který rozbalí tento paket (odstraní IPv4 hlavičku) a pošle ho dál

dle informací v IPv6 paketu.“ [9]

Tento mechanismus je ilustrován na obrázku 5.



Obrázek 5: Mechanismus tunelování [1]

Při použití tunelování se dá použít jeden z dvou typů:

- konfigurované tunelování
- automatické tunelování

Konfigurované tunely jsou potřeba explicitně nakonfigurovat. V podstatě se jedná o nové síťové rozhraní, kde na koncích – tzv. tunnel pointech byly provedeny příkazy, kterými tunel vznikl. Podle *RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers* se tato metoda nejčastěji používá při propojení dvou směrovačů.

„Pro uživatele či administrátory menších sítí se nabízejí tunel servery. Jedná se o veřejně nabízené koncové body tunelů. Uživatel vyplní WWW formulář, na základě zadaných údajů se na tunel serveru vytvoří protější strana tunelu a uživatel dostane poštou skript s konfiguračními příkazy pro svůj systém. Když jej spustí, vznikne jeho konec tunelu a připojí tak svůj počítač k IPv6 síti. Je to snadné a může to vyzkoušet prakticky každý - například na Freenet6.“ [10]

Těmto tunelům se také říká *poloautomatické tunely.*

Automatické tunely jsou podrobně popsány v *RFC 2893: Transition Mechanism for IPv6 Hosts and Routers*. Tyto tunely se ustavují oproti veřejnému přepínači nebo směrovači, který je připojen do nativní IPv6 sítě. Přepínač nebo směrovač poskytuje IPv6 konektivitu bez

jakékoliv registrace uživatele. Automatické tunely pracují s IPv4-kompatibilními IPv6 adresami. Tato adresa může být vytvořena tak, že se před 32– bitovou adresu doplní nuly tak, aby celková délka byla 128 bitů. [9]

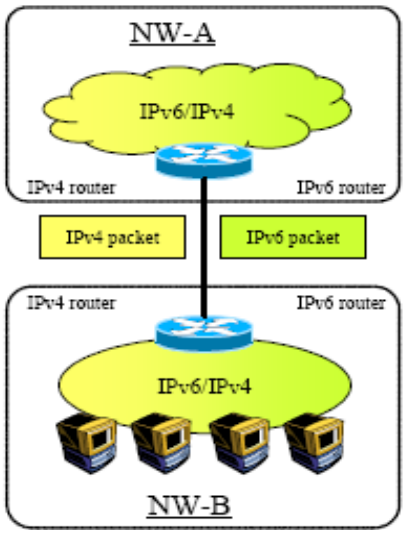
Dnes nejrozšířenějším mechanismem automatického tunelování je mechanismus ***6to4***. Podrobně je popsán v *RFC 3056: Connection of IPv6 Domains via IPv5 Clouds*. Vychází z předpokladu, že mezi dvěmi IPv6 sítěmi leží IPv4 Internet a na hranicích mezi sítěmi a Internetem je směrovač, který podporuje 6to4. Koncovými sítěmi tedy data probíhají v nativním IPv6 a k tunelování dochází mezi oběma hraničními směrovači. Je k tomu potřeba alespoň jedné IPv4 adresy, ze které se vytvoří 6to4 prefix pro adresu koncové sítě. „Konstruuje se tak, že za počátečních 16 bitů s hodnotou 2002 (šestnáctkově) se připojí 32 bitů IPv4 adresy hraničního směrovače. Tím vznikne obvyklý 48 bitů dlouhý prefix, kterým lze adresovat podsítě a počítače v koncové síti. Jediná IPv4 adresa tak pro ni umožňuje zavést plnohodnotné IPv6 adresy.“ [10]

Mezi další mechanismy automatického tunelování patří např. *6over4,* podrobně popsaný v *RFC 2529: Transmission of IPv6 over IPv4 Domains without Explicit Tunels* nebo *ISATAP*, kterým se zabývá *RFC 5214: Intra-Site Automatic Tunnel Addresing Protocol*.

3.2.3 Dvojí zásobník – tzv. Dual stack

Český pojem „dvojí zásobník“ neznamená, že zařízení má dva zásobníky protokolů: jeden pro IPv4 a druhý pro IPv6, ale ve skutečnosti se jedná o termín, který značí, že dané zařízení podporuje oba protokoly a tudíž má i obě adresy. Tyto zařízení jsou označovány jako IPv4/IPv6 uzly.

Tento mechanismus je vhodný pro dnešní dobu, kdy je stále potřeba zároveň i protokolu IPv4. Až bude možnost využívat pouze protokol IPv6, stačí na zařízeních vypnout používání protokolu IPv4. Tyto zařízení jsou označovány jako IPv6-only uzly.



Obrázek 6: Dual stack [17]

3.2.4 Translátory

Poslední variantou jsou tzv. translátory, neboli překladače. Využívají se v případě, kdy jeden uzel podporuje IPv6, ale potřebuje se připojit k serveru, který podporuje jen IPv4. Tento problém tunelování nevyřeší, je potřeba překladu vyslaných paketů do IPv4 a odpovědí od serveru do IPv6. Mezi nejrozšířenější translátory patří **SIIT** (*Stateless IP/ICMP Translation*), definovaný v RFC 2765, **NAT-PT** (*Network Address Translation – Protocol Translation*), který je založený na NATu a vyložený v RFC 2766 a **TRT** (*Transport Relay Translator*), který je podobný NAT-PTu, ale pracuje na transportní vrstvě (NAT-PT na síťové vrstvě) modelu ISO/OSI. Více o translátoru TRT je v RFC 3142.

3.3 Aktivní síťové prvky a IPv6

Pod pojem "aktivní síťové prvky" se v dnešní době zařazují všechna zařízení, která slouží potřebám vzájemného propojování v počítačových sítích, a přitom nejsou jen pasivními mechanickými záležitostmi (jakými jsou například kabely, konektory apod.) [15].

Jedná se o velký počet zařízení, ale pro téma této bakalářské práce jsou potřeba zejména ty, které pracují s IP adresou, tedy na třetí (síťové) vrstvě modelu ISO/OSI. Na této vrstvě se nachází především prvky nazývané jako směrovače, ale také tzv. L3 přepínače (na rozdíl od tzv. L2 přepínačů umějí pracovat i s informacemi z třetí vrstvy modelu ISO/OSI).

Přibližně před 6 lety vznikl certifikační program IPv6 Ready, který testuje produkty, kte-

ré jsou potřebné k provozu IPv6, zda splňují specifikace dané RFC. Tento projekt je zatím rozdělen do 2 fází:

1. fáze: testuje zda zařízení podporují povinné prvky protokolů (v RFC jsou označovány jako „must“). Podle [16] se jedná konkrétně o: IPv6 adresy, ICMPv6, objevování sousedů a bezstavovou automatickou konfiguraci. Prvky, které projdou tímto testem, jsou označeny stříbrným logem IPv6 Ready.

2. fáze: oproti první fázi testuje kromě povinných (tzv. „must“) prvků i důrazně doporučené (v RFC tzv. „should“) prvky. Tato fáze zahrnuje i: bezpečnost (IPsec), mobilní IPv6, DHCPv6 aj. Vyhovující prvky zde získávají zlaté logo IPv6 Ready[1].

Na trhu je mnoho výrobců síťových zařízení, ale mezi ty nejčastější patří především Cisco Systems, kteří mají podporu IPv6 implementovánu od verze IOSu 12.4[2]. Tato společnost patří k jedněm z nejrychleji se rozvíjejících v této oblasti.
Pokud jsou směrovače aktualizovány na potřebnou verzi IOS je nutné ještě povolit IPv6 příkazem:

```
ipv6 unicast – routing
```

3.4 Podpora serverů a služeb na nich běžících

Servery jsou nedílnou součástí každé firemní sítě. Jejich podpora nového protokolu IPv6 je tedy nezbytná. V této podpkapitole jsou popsány nejběžnější typy operačních systémů, Microsoft Windows a servery založené na linuxovém řešení.

3.4.1 Microsoft Windows Servery

Podle webových stránek Microsoftu přímá podpora ve **Windows Serveru 2000** není a také ji neplánují. Ovšem Microsoft nabízí ke stažení software, kterým lze IPv6 doinstalovat. Sami ale upozorňují na to, že se jedná pouze o tzv. „Technology preview“ a kvalita podpory IPv6 není vhodná pro běžný provoz, ale pouze pro testování.
Lepší podpora IPv6 se objevila u **Windows Serveru 2003**, kde je nutno tento protokol explicitně zapnout příkazem:

1 Kompletní přehled všech zařízení, které jsou označené zlatým logem IPv6 Ready je na adrese http://www.ipv6ready.org/phase-2_approved_list

2 Konkrétně od verze IOSu 12.4(9)T.

```
netsh interface ipv6 instal
```

V následujících tabulkách je přehled vybraných vlastností[3] (Tabulka 6) a aplikací (Tabulka 7), které jsou, popř. nejsou podporovány Windows Serverem 2003 na IPv6:

Tabulka 6: Vybrané vlastnosti pro Windows Server 2003 [19]

Vlastnost	**Podpora**
Dual IPv6/IPv4 stack	ANO
6to4	ANO
ISATAP	ANO
Teredo	NE
DNS over IPv6	ANO
DNS dynamic update	ANO
DHCPv6	NE
Visual Studio .NET (VS.NET)	ANO
IPSec authentication	ANO

Tabulka 7: Aplikace ve Windows Serveru 2003 [19]

Název aplikace	**Podpora**
File sharing, printer sharing	ANO
Windows Media Server	ANO
Internet Information Services (IIS) 6.0 (http only)	ANO
Telnet server	ANO
FTP server	NE
Active Directory	NE
Microsoft® Exchange Server	NE
SQL Server™	NE

3 Jsou zde vybrány jen některé vlastnosti, kompletní přehled a více informací o Microsoft Serveru 2003 je v [19]

Jak je vidět z tabulek, podpora IPv6 tu je, ale tento server má dvě nevýhody: „Windows Server 2003 IPv6 also supports Internet Explorer. However, it does not include support for literal addresses.“ [19]
A druhá je že, v tomto typu serveru není možné IPv4 odebrat, tudíž není schopen pracovat pouze na protokolu IPv6.

V novější verzi – **Windows Serveru 2008** je již podpora IPv6 nastavena implicitně. Tento server obdržel i zlaté logo IPv6 Ready.

3.4.2 Linuxové servery

Alternativou k serverům od společnosti Microsoft mohou být servery, jejichž operační systém je založen na Linuxu. Tyto řešení jsou v některých případech levnější záležitostí. V jádrech linuxových distribucích je podpora protokolu IPv6 velmi dobrá. Například Red Hat Enterprise Linux podporuje IPv6 od verze 4. Jeho následná verze 5 je označena zlatým logem IPv6 Ready.

Další distribuce jako Debian nebo SUSE Linux také disponují dobrou podporou tohoto protokolu.

3.5 Podpora IPv6 v operačních systémech

V této kapitole je popsáno, jak jsou na tom nejpoužívanější operační systémy s podporou IPv6.

3.5.1 Operační systémy BSD a Linux

BSD – kvalitní implementaci protokolu IPv6 nabízí unixové operační systémy řady BSD a to i díky japonskému projektu KAME[4] které je implementováno v jádrech operačních systémů – konkrétně ve FreeBSD od verze 4.0, OpenBSD od verze 2.7 a v NetBSD od verze 1.5. Podrobný popis zprovoznění IPv6 v NetBSD je uveden v [12].
Linux – jako první přišel s experimentální podporou IPv6, ale posléze tento vývoj začal stagnovat až do roku 2000, kdy v Japonsku vznikl projekt *USAGI*, jehož cílem bylo vyvinout kvalitní implementaci IPv6 pro Linux. Distribuce s jádrem verze 2.6.15 mají zlaté logo IPv6

4 Projekt KAME se nezabývá pouze implementací jádra systému IPv6, ale i úpravou síťových aplikací. Součástí projektu je celá řada nástrojů pro řízení a diagnostiku provozu na síti a tyto balíky lze bez obav nasadit do provozu a přímého využití. Více o tomto projektu na http://www.kame.net/ .

Ready.

Zda daná distribuce podporuje IPv6 se dá ověřit tímto příkazem:

```
ifconfig
```

Pokud v systému je podpora protokolu IPv6, ve výstupu budou adresy jednotlivých rozhraní. Podrobné informace o podpoře IPv6 v Linuxu jsou obsaženy v Linux IPv6 HOWTO [13].

3.5.2 Operační systémy Microsoft Windows

Podle [1] se implementace protokolu IPv6 poprvé objevila v Service Packu 1 pro **Windows XP** v září 2002. Ovšem není implicitně nainstalována. Přes příkazový řádek se dá během jedné minuty nainstalovat tímto příkazem:

```
ipv6 install
```

Windows Vista – v novější verzi operačního systému od Microsoftu je podpora protokolu IPv6 zapnuta implicitně a dá se tedy využít automatické konfigurace.

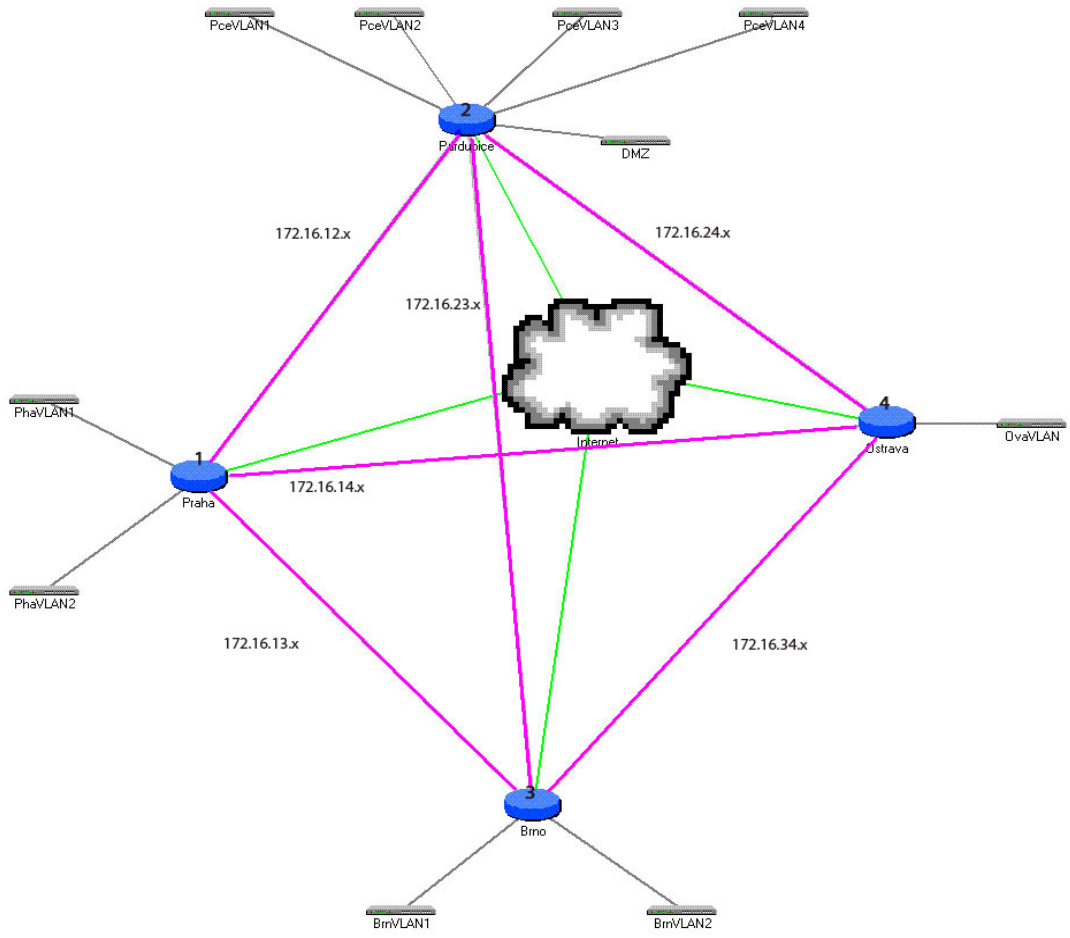
Veškeré informace o podpoře IPv6 v produktech Microsoftu jsou dostupné na jejich webových stránkách: *http://www.microsoft.com/ipv6/* .

4 Návrh na přechod ve firemní síti

V této kapitole je popsána současná infrastruktura sítě sledované firmy a možnosti přechodu na protokol IPv6.

4.1 Základní popis struktury

Na následujícím obrázku 7 je zobrazena základní struktura sítě včetně naznačené adresace sledované firmy.



Obrázek 7: Zjednodušené schéma sítě sledované firmy [Vlastní]

4.2 Popis aktivních prvků sítě

Pro další kapitoly je nezbytné vědět, jakými síťovými zařízeními každá pobočka disponuje. Přehled poboček a typů zařízení je v následující tabulce:

Tabulka 8: Přehled aktivních síťových prvků ve sledované firmě [Vlastní]

Zařízení	**Typ**	**Počet kusů**	**Podpora IPv6**
Pobočka Pardubice			
Cisco 2821	směrovač	1	ANO, od verze 12.4.(9)T
Cisco Catalyst 2950	L2 přepínač	5	NE
Nortel Baystack 350	L2 přepínač	5	NE
Pobočka Praha			
Cisco 2811[5]	směrovač	1	ANO, od verze 12.4.(9)T
Cisco Catalyst 2950	L2 přepínač	3	NE
Cisco Catalyst 2960	L2 přepínač	2	ANO
Nortel Baystack 350	L2 přepínač	5	NE
HP ProCurve 2626	L2 přepínač	2	NE[6]
Pobočka Brno			
Cisco 1750[7]	směrovač	1	ANO
Cisco Catalyst 2950	L2 přepínač	3	NE
Pobočka Ostrava			
Cisco 1750	směrovač	1	ANO
Cisco Catalyst 2950	L2 přepínač	3	NE

Z tabulky je patrné, že sledovaná firma využívá směrovače, které mají podporu IPv6.

„Cisco dává k dispozici IOS image pouze těm, kteří mají CCO Account, což pro velké organizace nepředstavuje takový problém. Verze IOS se dělí do mnoha větví a pro každý specifický typ Cisco hardware je k dispozici zpravidla několik verzí z každé hlavní vývojové větve, přičemž tyto verze se liší vlastnostmi které zahrnují a podle toho také vypadají nároky na hardware.“ [18]

5 Směrovače od firmy Cisco Systems řady 2800 mají uděleno zlaté logo IPv6 Ready.

6 Přepínače od firmy HP podporují IPv6 až od řady 2900. Upgrade možný není.

7 Směrovače od firmy Cisco Systems řady 1700 mají uděleno zlaté logo IPv6 Ready.

4.3 Popis serverů a služeb na nich běžících

Na všech pobočkách jsou připojené servery od společnosti Microsoft. Jaké typy, počet a přehled aplikací, které na nich běží jsou v následující tabulce. Červeně zvýrazněné jsou služby, které nemají na daném typu serveru podporu IPv6.

Tabulka 9: Přehled serverů a služeb pro sledovanou firmu [Vlastní]

Město	Windows server 2000	počet	Windows server 2003	počet	Windows server 2008	počet
PCE	DNS, printserver, VPN	3ks	DHCP, FTP, SQL, IIS, (web), LDAP, IIS (intranet)	7ks	CAS, Telnet, Exchange server, Backupserver	4ks
PRAHA	FTP, VPN, printserver	3ks	IIS (intranet), LDAP, CVS, SQL, DHCP	5ks	Backupserver, netboot	2ks
BRNO	printserver, VPN	2ks	FTP, SMTP, IIS (intranet), DHCP	4ks	Backupserver, netboot	2ks
OVA	printserver	1ks	DHCP, VPN, IIS (intranet)	3ks	Backupserver	1ks

Těmto serverům se věnuje podkapitola 3.4.1 , kde je jejich přehled a popsáno, které z nich mají podporu IPv6. V případě Windows Serveru 2003 i aplikace, které jsou podporovány.

4.4 Ostatní informace o sledované firmě

Na každé pobočce jsou zapojeny osobní počítače s operačním systémem od firmy Microsoft, konkrétně OS Windows Vista a Windows XP.

Podle podkapitoly 3.5.2 je možné IPv6 v MS Windows XP manuálně zapnout a v MS Windows Vista je již podpora implicitně zapnuta, tudíž zde by neměly nastat žádné problémy.

Počet pracovních stanic a na nich používaný operační systém udává tabulka 10.

Tabulka 10: Operační systémy na pobočkách [Vlastní]

Pobočka	OS XP - počet	OS Vista - počet
Pardubice	40	10
Praha	20	20
Brno	10	20
Ostrava	5	2

4.5 Možnosti přechodu na protokol IPv6

Tato podkapitola navazuje na část 3.2 , kde jsou obecně popsány možnosti přechodu na protokol IPv6. Zde jsou ukázány možnosti přechodu pro sledovanou firmu.

4.5.1 Nativní připojení a dual stack

Tyto dvě možnosti přechodu na protokol IPv6 jsou popsány v jedné kapitole, z toho důvodu, že v této době, kdy se IPv6 teprve zavádí, je stále potřeba počítat i s protokolem IPv4. Proto je vhodné, aby struktura sítě uměla pracovat s oběma protokoly zároveň. Pokud by bylo potřeba pouze protokolu IPv6, je možné podporu IPv4 vypnout.

Sledovaná firma využívá internetových služeb od společnosti GTS Novera. Z tabulky 5 je patrné, že společnost GTS Novera nativní připojení svým klientům neposkytuje. Podle dotazu na zákaznickou podporu ani nemají bližší informace, kdy by tato verze IP protokolu měla být nasazena do provozu.[8]

Z výše uvedeného plyne, že pokud by se sledovaná firma rozhodla pro nativní připojení IPv6, musí změnit poskytovatele, který tuto službu bude nabízet.

Pokud již nový poskytovatel připojení IPv6 poskytuje, je potom nutné přizpůsobit celou strukturu sítě tak, aby byla schopna pracovat i na protokolu IPv6.

Aktivní síťové prvky

V podkapitole 4.2 je uvedeno, že tato firma disponuje směrovači od firmy Cisco Systems, jejichž verze IOSu musí být nastavena minimálně na verzi 12.4.(9)T. Tuto verzi je

8 Tyto informace byly vykorespondovány e-mailovou komunikací k 11. březnu 2009.

možné stáhnout po přihlášení z oficiálních stránek Cisca. Je však nutné zkontrolovat, zda daný směrovač (popř. přepínač) disponuje dostatečně velkou pamětí nutnou k upgradu. Podle technických dokumentací jednotlivých prvků sítě od firmy Cisco, které tato firma využívá, není upgrade IOSu možný u přepínače Cisco Catalyst 2950. Tyto přepínače by bylo nutné vyměnit v případě, že by sledovaná firma chtěla, aby byly manageovatelné přes IPv6. Pokud by nebylo potřeba managementu, mohou být ponechány.
Jakmile budou koncová zařízení schopna komunikovat přes protokol IPv6, bude potřeba přizpůsobit i vnitřní strukturu sítě.

Pracovní stanice

V pracovních stanicích je nutné nastavit podporu IPv6 pouze u operačních systémů Microsoft Windows XP, kde tato instalace trvá okolo jedné minuty. Jak již bylo zmíněno, ve Windows Vista je podpora zapnutá automaticky, proto ji není potřeba nijak složitě konfigurovat.

Dalším krokem bude zkontrolovat aplikace, které využívají IP adres. Jedná se především o internetové prohlížeče a mailové klienty. Podle informací od sledované firmy se využívá služeb Microsoftu, tedy Internet Explorer, MS Outlook 2007 a ve Windows Vista je tzv. Windows Mail.
S Internet Exprorerem jsou co se týče IPv6 problémy, protože starší verze nepodporují literálový zápis adres. Pokud by sledovaná firma nadále chtěla využívat tento typ prohlížeče, bylo by vhodné, aby byl minimálně na verzi 7.0 (tato verze je dodávaná s operačním systémem MS Vista), kde je již podpora literálového zápisu adresy.
Mezi další prohlížeče, které mají podporu IPv6 patří například dnes velmi často používaná Mozilla.
Windows Mail má podporu IPv6, stejně tak i MS Outlook 2007. Mezi další klienty s podporou tohoto protokolu patří i Thunderbird, který má podporu od verze 1.5.

Servery a aplikace

Největším problémem bude již zmiňovaný Windows Server 2000, který nemá podporu IPv6. Zde se nabízí více variant řešení:

1. Nejméně nákladná varianta je ta, že se aplikace, které na tomto server pracují, přesunou na jiný server, tedy na Windows Server 2003 nebo na Windows Server 2008.

2. Další méně nákladná varianta by byla namísto Windows Serveru 2000 nainstalovat distribuci Linuxu, kde by bylo potřeba služby, které byly na Windows Serveru 2000 nainstalovat a následně nakonfigurovat.
3. Pokud by nebylo možné přesunout tyto aplikace na jiný server, tak poslední variantou, ale nejnákladnější, by byla koupě potřebného množství nových serverů Microsoft Windows, v tomto případě by se jednalo o nejnovější typ, tedy Microsoft Windows Server 2008.

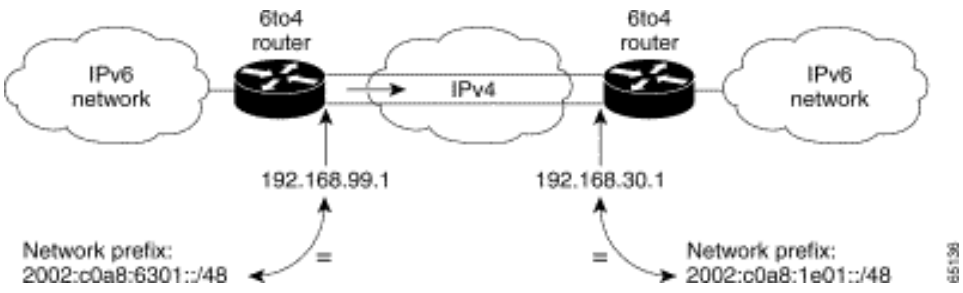
Z tabulek 7 a 9 je vidět, že na pobočce v Pardubicích by se daly přeinstalovat služby *sdílení tiskáren (printserver)* a *DNS* na Windows Server 2003 místo služeb DHCP a FTP, které zde nemají podporu IPv6. Tím by se v závěrečné kalkulaci ušetřilo na koupi nových serverů. Stejně tak by se přesunuly služby pro sdílení tiskáren i na ostatních pobočkách.

4.5.2 Tunelování 6to4

V případě, že vnitřní síť již dokáže pracovat i s protokolem IPv6 a je potřeba komunikace také s ostatními pobočkami, která je vedena přes IPv4 Internet, nabízí se mechanismus tzv. tunelování.

Zde je předpokládáno, že pracovní stanice a servery mají podporu tohoto protokolu, ale poskytovatel připojení neposkytuje.

Pro tento případ se nejlépe hodí mechanismus **6to4**, který je popsán v části 3.2.2 a je znázorněn na následujícím obrázku:



Obrázek 8: Použití 6to4 mezi dvěmi sítěmi [9]

Jednotlivé pobočky jsou propojeny tunely. Ty jsou podle [1] v IOSu přepínače představovány speciálními rozhraními `tunnel` *číslo*. Každému tunelu je přiřazeno právě jedno číslo. Tento tunel se vytvoří tak, že se mu přidělí IPv6 adresa a poté je nutné definovat oba konce tunelu jednoduchými příkazy:

`tunnel source` *rozhraní* nebo *IPv4 adresa*
`tunnel destination` *IPv4 adresa*

Například pro směrovač v Pardubicích, který má IPv4 adresu 172.16.24.2, bude IPv6 adresa fe80::ac10:1802, k ní se přidá prefix „2002“, který je rezervován právě pro mechanismus 6to4, a také adresa síťového rozhraní, a 6to4 směrovač si tuto adresu dokáže přeložit jako IPv4 a přenést ji tedy IPv4 Internetem. Na druhé straně si ji 6to4 směrovač opět přeloží do adresy IPv6 a podle adresy uzlu přesměruje kam je potřeba.

5 Návrh na přechod a kalkulace nákladů

V této kapitole je popsáno jakým způsobem by bylo nejvhodnější pro danou firmu přejít na protokol IPv6 včetně nákladů, jaké tento přechod bude obnášet.

5.1 Stanovení cen za práci

Ke stanovení odměny pro technického pracovníka (dále jen technika), jsou údaje čerpány z Českého statistického úřadu (ČSÚ). Zde byl k dispozici pouze průměrný hrubý plat za celý pracovní měsíc.

Cena za hodinu práce technika je vypočítaná následovně: průměrný plat/(42,5*4), kde 42,5 je počet pracovních hodin za týden a 4 jsou pracovní týdny v měsíci.
Ze stránek ČSÚ[9] bylo zjištěno, že v roce 2007 byl průměrný hrubý plat technika v oblasti IT 33 806,- Kč. V následující části je tedy uváděna průměrná hrubá mzda 200,- Kč/hod. Podle §10 zákona č. 143/1992 Sb. za hodinu práce přesčas v pracovních dnech zaměstnanci náleží příplatek ve výši 25% hodinové mzdy. V případě technika je tedy uváděna odměna 250Kč/hod přesčasu. Pokud by byla potřeba práce o víkendu, náleží mu příplatek ve výši 50% hodinové mzdy, tedy 300Kč/hod.

5.2 Náklady spojené s přechodem na IPv6

Sledovaná firma má, jak už bylo zmíněno, čtyři pobočky. Na centrální pobočce, tedy v Pardubicích, je provoz nepřetržitý – 24x7 (24 hodin, 7 dní v týdnu). Na ostatních pobočkách je provoz pouze v pracovních dnech – 9x5.

Na všech pobočkách, kromě Pardubic, může k upgradu zařízení, popř. výměně, dojít mimo pracovní dobu nebo o víkendu.
Na pobočce v Pardubicích bude potřeba tento proces udělat tak, aby neohrozil chod celé firmy, protože nabízí svým klientům nepřetržitou technickou podporu. Jelikož bude ale potřeba na krátkou dobu provoz přerušit, bude nutné, aby tuto pobočku zastoupila jiná pobočka. Rozhodně bude potřeba klientům oznámit, že se modernizuje síť, aby byli připraveni na možné krátkodobé komplikace.

9 Informace byla pořízena z webových stránek ČSÚ: http://www.czso.cz/csu/redakce.nsf/i/mzdy_it_odborniku_v_ceske_republice

Pro připojení přes protokol IPv6 bude nutné provést několik změn ve struktuře firmy, které budou provádět především technici dané firmy.
Na všech pobočkách bude nutné vyměnit Windows Servery 2000, které nemají podporu protokolu IPv6. Bylo by vhodné nakoupit již nejnovější typ tohoto serveru, tedy Windows Server 2008. Ceny, uvedené v tabulkách, jsou z internetového obchodu *Svět software*, který nabízí dostupnost produktu do tří pracovních dnů.

Dalším krokem bude instalace těchto serverů a také potřebných služeb, které na nich budou provozovány. V podkapitole 4.5.1 je zmíněno, že aplikace *printserver* a *DNS* je možné nainstalovat na Windows Server 2003, proto není potřeba nákupu nových serverů. Na odinstalování služby a nainstalování nové služby je předpokládaná doba práce 2 hodiny a na instalaci nového serveru a instalaci služby je tato doba stanovena na 3 hodiny.

Všechny výše uvedené kroky bude nutné provést mimo pracovní dobu, kdy nebude ohrožen chod firmy. V pracovní době je možné zapnout podporu v pracovních stanicích, které mají operační systém Windows XP. Pro tuto činnost je stanovena doba sedmi minut, ve které je započítáno přihlášení administrátora do systému a restartování systému po nainstalování protokolu IPv6.

Další náklady bude obnášet zastoupení pardubické pobočky, nejlépe pražskou, protože disponuje podobným vybavením, jako právě pardubická.
V tomto případě bude nutné zajistit pracovníky, kteří by tu pracovali do doby, než bude pardubická pobočka připravena na provoz. Protože se jedná o technickou podporu, budou tuto funkci vykonávat také technicky zaměření pracovníci, proto je dále uváděna také přesčasová mzda 250,- Kč/hod.

Veškeré náklady, které jsou potřebné k výměně, popř. k upgradu zařízení jsou uvedeny v následujících tabulkách, které byly rozděleny do dvou částí z důvodu přehlednosti.

Tabulka 11: Náklady na upgrade a výměnu zařízení, část 1 [Vlastní]

Položka	**Počet**	**Cena (s DPH)**	**Celková cena**
Pardubice			
Nákup Windows Serveru 2008[10]	3ks	30.575,- Kč (36.384,- Kč)	91.725,- Kč (109.152,- Kč)
Instalace serveru a nastavení služby	3x	9 hodin (přesčas)	2.250,- Kč
Přeinstalování služby	2x	4 hodiny (přesčas)	800,- Kč
Zapnutí podpory IPv6 v XP	20x	2,5 hodiny	450,- Kč
Zkušební provoz a doladění nedostatků		5 hodin (přesčas)	1.250,- Kč
Pracovníci zastupující pobočku		15 hodin (přesčas)	3.750,- Kč
Časová náročnost/Náklady za techniky/ Náklady za servery (s DPH)		**35,5 hodin**	**8.500,- Kč 109.152,- Kč**
Náklady za pobočku:			**117.652,- Kč**
Praha			
Nákup Windows Serveru 2008	3ks	30.575,- Kč (36.384,- Kč)	91.725,- Kč (109.152,- Kč)
Instalace serveru a nastavení služby	3x	9 hodin (přesčas)	2.250,- Kč
Přeinstalování služby	1x	2 hodiny (přesčas)	500,- Kč
Zapnutí podpory IPv6 v XP	20x	2,5 hodiny	450,- Kč
Zkušební provoz a doladění nedostatků		5 hodin (přesčas)	1.250,- Kč
Časová náročnost/Náklady za techniky/ Náklady za servery (s DPH)		**18,5 hodin**	**4.450,- Kč 109.152,- Kč**
Náklady za pobočku			**113.602,- Kč**

10 Jedná se o Windows Server 2008 Standard Edition, která obsahuje 10x CAL licencí. Celková nabídka je na adrese http://www.svetsoftware.cz/windows-2008-server-standard

Tabulka 12: Náklady na upgrade a výměnu zařízení, část 2 [Vlastní]

Položka	**Počet**	**Cena (s DPH)**	**Celková cena**
Brno			
Nákup Windows Serveru 2008	2ks	30.575,- Kč (36.384,- Kč)	61.150,- Kč (72.768,- Kč)
Instalace serveru a nastavení služby	2x	6 hodin (přesčas)	1.500,- Kč
Přeinstalování služby	1x	2 hodiny (přesčas)	500,- Kč
Zapnutí podpory IPv6 v XP	10	1,5 hodiny	300,- Kč
Zkušební provoz a doladění nedostatků		4 hodin (přesčas)	1.000,- Kč
Časová náročnost/Náklady za techniky/ Náklady za servery (s DPH)		**13,5 hodin**	**3.300,- Kč 72.768,- Kč**
Náklady za pobočku			**76.068,- Kč**
Ostrava			
Nákup Windows Serveru 2008	1ks	30.575,- Kč (36.384,- Kč)	30.575,- Kč (36.384,- Kč)
Instalace serveru a nastavení služby	1x	3 hodiny (přesčas)	750,- Kč
Přeinstalování služby	1x	2 hodiny (přesčas)	500,- Kč
Zapnutí podpory IPv6 v XP	5x	45 minut	150,- Kč
Zkušební provoz a doladění nedostatků		3 hodin (přesčas)	750,- Kč
Časová náročnost/Náklady za techniky/ Náklady za servery (s DPH)		**8,75 hodin**	**2.150,- Kč 36.384,- Kč**
Náklady za pobočku			**38.534,- Kč**
CELKOVÉ NÁKLADY			**345.856,- Kč**

Jak je vidět, největší náklady tvoří nákup nových serverů. Pokud by se tato firma rozhodla pro alternativní variantu, tedy serverů, které jsou založené na Linuxu, celkové náklady by byly podstatně nižší. V případě linuxových serverů by bylo pouze potřeba zaplatit za technika, který by tyto nové servery nainstaloval a nastavil na nich požadované služby.

Například firma AA Computer, s.r.o nabízí instalaci a nastavení jednoho linuxového serveru za cenu 3000,- Kč. Při počtu devíti serverů, které sledovaná firma bude muset zakoupit, by náklady vyšly na 27.000,- Kč. S přihlédnutím k odstavení pobočky v Pardubicích a k práci techniků je celková cena odhadována na 40.000,- Kč. Ve srovnání s předchozí kalkulací je to skoro 10x méně, proto by bylo vhodné o této variantě uvažovat.

6 Závěr

Na začátku této bakalářské práce byly stanoveny cíle seznámit čtenáře s novým protokolem IPv6 a také ukázat, jaké kroky je nutné podniknout k přechodu na tento protokol.

Výsledkem práce je zjištění, že přechod na tento prokol není nijak složitá záležitost. Existuje několik možností, jak se připojit přes protokol IPv6, ať už poskytovatel Internetu toto připojení poskytuje nebo ne. Největší překážkou implementace tohoto protokolu mohou být staré typy koncových zařízení, které nepodporují IPv6. Toto se týká především směrovačů a také některých druhů přepínačů. Jako další problém se ukázaly starší typy serverů od společnosti Microsoft, kde je buď jen částečná podpora tohoto protokolu nebo dokonce žádná. Naopak, zařízení, která jsou založená na linuxovém jádru se jeví pro implementaci protokolu IPv6 jako ideální řešení. Jsou zde minimální náklady na pořízení a podpora tohoto protokolu je na velmi dobré úrovni.

Fakt, že je potřeba vyměnit stará zařízení, což je velmi nákladná záležitost, podle mne odrazuje spoustu firem v implementaci tohoto protokolu. Další důvod může být ten, že v dnešní době velmi malá část poskytovatelů Internetu poskytuje připojení přes IPv6. Ovšem pokud firmy začnou s implementací protokolu IPv6 a tím pádem stoupne poptávka po nativním připojení, poskytovatelé budou nuceni reagovat a tyto služby častěji nabízet.

Zpracováním této problematiky jsem získala mnoho poznatků jak o protokolu IPv6 jako takovém, tak o jeho implementaci. Dle mého názoru by firmy neměly odkládat modernizaci své sítě na pozdní dobu. Mohlo by se stát, že pokud nebude zájem o tento protokol, výrobci zařízení, poskytovatelé Internetu a programátoři aplikací nebudou vyvíjet implementace IPv6 a až budou opravdu potřeba, tak nebudou k dostání. To by mohlo i způsobit, že zařízeních s podporou IPv6 bude málo a tudíž stoupne i jejich cena.

Pokud bych měla být správce sítě, který by se měl rozhodnout o nasazení nových serverů, určitě bych volila ty, které jsou založené na Linuxu, protože zde je podpora tohoto protokolu dle získaných poznatků výrazně vyšší než u serverů s operačním systémem od firmy Microsoft.

Seznam použité literatury

[1] SATRAPA, Pavel. IPv6. 2. aktualiz. vyd. Praha : CZ.NIC, z. s. p. o., 2008. 357 s. Dostupný z WWW: <http://knihy.nic.cz/ipv6/>. ISBN 978-80-904248-7.

[2] HINDEN, R., DEERING, S. RFC 1883: Internet Protocol, Version 6 (IPv6) Specification [online]. 1995 [cit. 2009-02-14]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc1883.txt>.

[3] IPv4 Address Report [online]. 2009 [cit. 2009-02-14]. Dostupný z WWW: <http://www.potaroo.net/tools/ipv4/index.html#r4>.

[4] HINDEN, R., DEERING, S. RFC 2460: Internet Protocol, Version 6 (IPv6), Specification [online]. 1998 [cit. 2009-02-14]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc2460.txt>.

[5] DOSTÁLEK, Libor, KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 2. aktualiz. vyd. Praha : Computer Press, 2000. 426 s. ISBN 80- 7226-323-4.

[6] HINDEN, R., DEERING, S. RFC 2373: IP Version 6 Addressing Architecture [online].1998 [cit. 2009-03-12]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc2373.txt>.

[7] PUŽMANOVÁ, Rita. TCP/IP v kostce. 1. vyd. České Budějovice : KOPP, 2004. 607 s. ISBN 80-7232-236-2.

[8] CONTA, A., DEERING, S., GUPTA, M. Internet Control Message Protocol (ICMPv6) [online]. 2006 [cit. 2009-03-12]. Dostupný z WWW: <http://tools.ietf.org/html/rfc4443>.

[9] KOTÁL, Vladimír. Strategie přechodu na IPv6 [online]. 2003 [cit. 2009-03-12]. Dostupný z WWW: <http://techie.devnull.cz/ipv6/ipv6-paper/transit-ipv6.html>.

[10] SATRAPA, Pavel. IPv6 - přechodové mechanismy (1) [online]. 2002 [cit. 2009-03-17]. Dostupný z WWW: <http://www.lupa.cz/clanky/ipv6-prechodove-mechanismy-1/>.

[11] EŠNER, Daniel. IP verze 6 - Implementace [online]. 2003 [cit. 2009-03-17]. Dostupný z WWW:<http://www.kiv.zcu.cz/~simekm.html>.

[12] IPv6 Networking FAQ [online]. 2001 [cit. 2009-03-12]. Dostupný z WWW: <http://www.netbsd.org/docs/network/ipv6/index.html>.

[13] BIERINGER, Peter. Linux IPv6 HOWTO [online]. 2009 [cit. 2009-03-17]. Dostupný z WWW: <http://tldp.org/HOWTO/Linux+IPv6-HOWTO/>.

[14] NORDMARK, E. RFC 4213: Basic Transition Mechanism for IPv6 Hosts and Routers [online]. 2005 [cit. 2009-03-18]. Dostupný z WWW: <http://tools.ietf.org/html/rfc4213>.

[15] PETERKA, Jiří. Aktivní síťové prvky - co jsou a k čemu slouží. Computerworld [online]. 1994, č. 38 [cit. 2009-03-31]. Dostupný z WWW: <http://www.earchiv.cz/a94/a438c500.php3>.

[16] SATRAPA, Pavel. Program IPv6 Ready je připraven [online]. 20. 12. 2007 [cit. 2009-03-31]. Dostupný z WWW: <http://www.lupa.cz/clanky/program-ipv6-ready-je-pripraven/>.

[17] IPv6 Deployment Guideline : ISP Segment [online]. 2005 [cit. 2009-04-09]. Dostupný z WWW: <http://www.v6pc.jp/pdf/en-08-v6trans-ISP.pdf>.

[18] KOTÁL, V.. Implementace IPv6 [online]. 2003 [cit. 2009-04-10]. Dostupný z WWW: <http://techie.devnull.cz/ipv6/ipv6-paper/implementation-ipv6.html>.

[19] Exploring IPv6 [online]. March 28, 2003 [cit. 2009-04-11]. Dostupný z WWW: <http://technet.microsoft.com/en-us/library/cc776103.aspx>.

[20] Přenos protokolu IPv6 mezi uzly v různých sítích v Internetu (6to4) [online]. 2005 [cit. 2009-04-12]. Dostupný z WWW: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003.html>.

[21] Automatická konfigurace [online]. 2008 [cit. 2009-04-14]. Dostupný z WWW: <https://www.ipv6.cz/index.php/Automatická_konfigurace>.

Seznam použitých zkratek

ARP	Address Resolution Protocol
CAL	Client Access License
ČSÚ	Český statistický úřad
DNS	Domain Name System
DUID	DHCPv6 Unique Identifier
EGP	Exterior Gateway Protocol
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
IA	Identity Association
IAID	Identity Association IDentification
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IETF	Internet Engineering Task Force
IIS	Internet Information Services
IGP	Interior Gateway Protocol
IOS	Internetwork Operating System
Ipng	Internet Protocol Next Generation
Ipsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISO/OSI	International Standards Organization / Open Systen Interconnection
ISS	Internet Information Services
LAN	Local Area Network
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAT-PT	Network Address Translation – Protocol Translation
ND	Neighbor Discovery
RFC	Request for Comment
RSVP	Reservation Protocol
SIIT	Stateless IP/ICMP Translation
TCP	Transmission Control Protocol

TRT	Transport Relay Translator
UDP	User Datagram Protocol
USAGI	Universal PlayGround for IPv6

Seznam obrázků

Seznam tabulek