Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

IPv6 aspekty migrace firemní IT infrastruktury

Karel Vyhlídka

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Vyhlídka Karel

Informatika

Název práce

IPv6 aspekty migrace firemní IT infrastruktury.

Anglický název

Aspects of migration business IT infrastructure to IPv6.

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku IPv6 a jeho implementaci ve firemním prostředí. Hlavním cílem práce je sumarizovat technické a ekonomické aspekty migrace firemního prostředí z IPv4 na IPv6.

Metodika

Metodika bakalářské práce bude založena na studiu a analýze odborných informačních zdrojů. Závěry bakalářské práce budou formulovány syntézou získaných teoretických poznatků.

Harmonogram zpracování

1. Příprava a studium Informačních zdrojů a upřesnění dílčích cílů práce: 2/2013 – 6/2013
2. Zpracování přehledu řešené problematiky dle informačních zdrojů: 7/2013 – 8/2013
3. Vypracování vlastního řešení, diskuse a zhodnocení výsledků: 9/2013 – 10/2013
4. Tvorba finálního dokumentu bakalářské práce: 11/2013 – 2/2014
5. Odevzdání bakalářské práce a teze: 3/2014

Rozsah textové části
30 - 40 stran

Klíčová slova
IPv6, síťové protokoly, směrování v sítích, migrace

Doporučené zdroje informací

1. Satrapa, Pavel:IPv6. Praha: CZ.NIC, z. s. p. o., 2011. 3.vydání. 407 s. ISBN 978-80-904248-4-5
2. McFarland, Shannon; Sambi, Muninder; Sharma, Nikhil; Hooda, Sanjay: IPv6. Brno: Computer Press, 2011. 1. vydání. 368 s. ISBN: 978-80-251-3684-3
3. Mehta, Naren; Healy, Rus; Odom, Wendell: Směrování a přepínání sítí. Brno: Computer Press, 2009. 1. vydání. 880 s. ISBN: 978-80-251-2520-5

Vedoucí práce
Vasilenko Alexandr, Ing.

Termín odevzdání
březen 2014

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr. h. c.
Děkan fakulty

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "IPv6 aspekty migrace firemního prostředí" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 11. 3. 2015 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Alexandru Vasilenkovi za odborné vedení, přínosné rady a připomínky při vypracování této práce.

IPv6 aspekty migrace firemní IT infrastruktury

Aspects of migration business infrastructure to IPv6

Souhrn

Práce sumarizuje informace nezbytné pro migraci firemního prostředí na IPv6, hodnotí možné postupy migrace, rozebírá různé důvody pro přechod na IPv6 a srovnává výhody a nevýhody takového kroku. Na základě těchto informací navrhuje konkrétní řešení pro různé modelové situace.

Summary

The submitted work summarized required information for IPv6 business infrastructure migration, evaluates possible methods of migration, analyzes different reasons for IPv6 migration and compares their advantages and disadvantages. On the basis of these information suggests specific solutions for different model situations.

Klíčová slova:

IPv6, síťové protokoly, směrování v sítích, migrace, autokonfigurace, DHCPv6, dvojí sada protokolů, přechodové mechanismy

Keywords:

IPv6, network protocols, routing, migration, auto configuration, DHCPv6, dual stack, transition mechanisms

Obsah

1 Úvod

Internetový protokol verze 6 (IPv6) je nový protokol, který by měl v internetovém (síťovém) provozu nahradit v současnosti používaný internetový protokol verze 4 (IPv4). Hlavní motivací pro jeho vývoj a zavedení do praxe je nedostatečný adresní prostor IPv4.

Vývoj IPv6 započal již v roce 1994. První definice byla představena světu v *RFC*[1] *1883: Internet Protocol, Version 6 (IPv6) Specification*, které vyšlo v prosinci 1995. Avšak změny provedené v protokolu IPv4, především beztřídní adresování a překlad vnitřních adres sítě, zbrzdily spotřebu adres natolik, že nebylo nadále nutné spěchat s vývojem nového protokolu. Práce na vývoji IPv6 dále pokračovaly až do roku 2004, kdy byla představena podpora mobility a v roce 2006 přibyla nová revize adresní architektury.

Nicméně, už v roce 1996 vznikla virtuální IPv6 síť s názvem *6 bone* propojující různé světové výzkumné instituce. Cílem této sítě bylo simulovat IPv6 internet v praxi a ověřit tak jeho fungování. Poté, co byly získány veškeré potřebné poznatky, byl její provoz dne 6. 6. 2006 ukončen.

V roce 1999 bylo založeno *IPv6 Forum*[2], které kromě propagace, sdílení a šíření informací o IPv6 představilo certifikační programy, jež zaručovaly schopnost jimi certifikovaných výrobků pracovat s IPv6 v daném rozsahu. Prvním z těchto certifikačních programů byl *IPv6 Ready* zaručující základní kompatibilitu zařízení s IPv6. Dalším z certifikačních programů IPv6 Fora je program *IPv6 Enabled* určený pro WWW servery a poskytovatele Internetu. U WWW serverů zaručuje jejich dostupnost prostřednictvím IPv6. Zatím posledním z řady certifikátů IPv6 Fora je *IPv6 Education* zaměřený na vzdělávání.

V roce 2008 představila Evropská komise Akční plán pro nasazení internetového protokolu verze 6 v Evropě a v roce 2009 zareagovala na celosvětový vývoj i vláda České republiky, která 8. června vydala Usnesení vlády č. 727: Zpráva o přechodu na internetový protokol verze 6 (IPv6), v němž stanovila časový harmonogram, podle kterého má státní správa přecházet na protokol IPv6.

[1] Request for Comments – ‚žádost o komentáře', sada dokumentů a standardů definující a upravující internetové protokoly a chování sítí.
[2] IPv6 Forum – organizace zaměřující se na rozšiřování povědomí o nasazení IPv6. Sdružuje poskytovatele internetu, experty a výzkumníky.

2 Cíl práce a metodika

Cílem práce je sumarizovat informace nezbytné pro migraci firemního prostředí na IPv6, zhodnotit různé možné postupy migrace a na základě získaných informací navrhnout konkrétní řešení pro vybrané modelové situace. Jako zdroje informací k danému tématu poslouží odborná literatura a především dokumenty Request for Comments (RFC), které jsou základními kameny a nosnými prvky většiny současného síťového provozu.

Přehled řešené problematiky si klade za cíl základní formou nastínit fungování internetového protokolu nové generace a osvětlit stěžejní funkcionality důležité pro další práci.

Analytická část práce pak představuje používané přechodové mechanismy a postupy užívané při migraci z IPv4 na IPv6. Dále jsou analyzovány důvody pro přechod na IPv6 a přínosy a úskalí tohoto kroku. Nakonec pak navrhuje řešení pro jednotlivé modelové situace.

3 Přehled řešené problematiky

Po celé dvě dekády je největší motivací pro vývoj IPv6 nedostatečný adresní prostor IPv4. Tento problém je v IPv6 vyřešen použitím 128 bitů dlouhé adresy, která přináší na rozdíl od té 32 bitové, jež poskytuje pouze necelé 4,3 miliardy adres, takových adres $3{,}4.10^{38}$. Toto množství by mělo i při opravdu velkorysém přístupu k jejich přidělování vystačit na velmi dlouhou dobu.

3.1 Adresy v IPv6

Prvním dokumentem specifikujícím adresy v IPv6 bylo *RFC 1884: IP Version 6 Addressing Architecture* z roku 1995, které bylo postupně nahrazeno několika dalšími. V současné době je v platnosti *RFC 4291: IP Version 6 Addressing Architecture* z roku 2006. To je dále doplněno o *RFC 5952: A Recommendation for IPv6 Address Text Representation* a *RFC 6052: IPv6 Addressing of IPv4/IPv6 Translators*.

3.1.1 Typy adres

Adresy jsou rozděleny do skupin pomocí prefixů. Většina z nich však zatím zůstává nepřidělená a čeká na budoucí použití. IANA[3] v současnosti rozděluje globální unicast adresy s prefixem 2000::/3. Rozdělení adresního prostoru IPv6 je uvedeno v příloze v tabulce 1. Dále existuje několik dobře známých (Well-Known) prefixů, jimž byla přiřazena specifická funkce. Jejich seznam je uveden v příloze v tabulce 2.

3.2 Formát IPv6 paketu

Pakety mají v IPv6 podobnou strukturu jako v předchozím protokolu IPv4, data jsou uvozena jednou, případně několika hlavičkami. Systém hlaviček se oproti dřívějšímu protokolu zásadně proměnil a to nejen kvůli výraznému prodloužení adres, ale i z pohledu stavby hlaviček a jejich řetězení.

3.2.1 Řetězení hlaviček

V IPv6 došlo k zásadní změně v koncepci hlaviček paketů. Každá hlavička je nyní samostatným, odděleným blokem dat uvozeným informací o tom, jaká další hlavička,

[3] Internet Assigned Numbers Authority – ‚autorita pro přidělování čísel na internetu', organizace zabývající se definicí a správou číselníků internetu.

případně typ dat za ní následuje. Veškeré principy řetězení a základní formáty hlaviček popisuje *RFC 2460: Internet Protocol, Version 6 (IPv6) Specification*. Pole další hlavička specifikuje kromě typu další hlavičky i druh nesených dat. V poslední hlavičce, za kterou již následují data, se tak v poli další hlavička nachází číslo protokolu přenášejícího obsah paketu. Tato čísla jsou většinou stejná jak v IPv4 tak v IPv6. Výjimkou je ICMP, který má v IPv4 číslo protokolu 1 a v IPv6 číslo protokolu 58. Všechna čísla rozšiřujících hlaviček jsou uvedena v příloze v tabulce 3, čísla vybraných protokolů jsou pak v tabulce 4.

3.3 Řídící zprávy IPv6 – ICMPv6

RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Versio 6 (IPv6) Specification definuje základy fungování ICMP v rámci IPv6. Tento protokol je zcela stěžejní pro hladký chod sítě. Zprávy ICMP mají společný tvar, který je uvozený 8 bity pro určení typu ICMP zprávy. V rozsahu 0 – 127 jsou chybové zprávy a v rozsahu 128 – 255 zprávy informační.

RFC 4443 definuje pouze 4 chybové a 2 informační zprávy. Další zprávy jsou definovány v jiných RFC spolu se souvisejícími funkcemi IPv6. Seznam všech ICMP zpráv a jejich kódů je uveden v příloze v tabulce 5.

Informačních zpráv je výrazně více než těch chybových. Většina z nich je však přímo svázána s funkcionalitou, se kterou byla definována. Význam většiny zpráv bude uveden u funkcionalit, ke kterým se vztahují.

Chybové zprávy

- **Cíl je nedostupný –** tuto zprávu posílá router, který není schopen předat paket dále.
- **Příliš velký paket –** tuto zprávu posílá router odesílateli, pokud je jeho paket zahozen z důvodu příliš malého MTU[4] pro průchod tohoto paketu.
- **Vypršel čas –** touto zprávou posílá router odesílateli informaci o vypršení času.
- **Problém s parametry –** tuto zprávu posílá uzel odesílateli, pokud narazí v hlavičce na data, se kterými není schopen pracovat.

[4] Maximum Transmission Unit – označuje maximální velikost paketu, který lze danou linkou odeslat.

Informační zprávy

- **Žádost o echo a odpověď na echo –** tyto dvě zprávy mají téměř totožný tvar a slouží především k diagnostickým účelům. Odesílatel odešle uzlu zprávu typu 128 a cílový uzel mu na ni odpoví zprávou typu 129.

3.4 Objevování sousedů a automatická konfigurace

Relativní nepřehlednost a délka IPv6 adresy ponechává množství prostoru pro chyby. Zadávání většího množství těchto adres je vcelku časově náročné, z čehož vyplývá potřeba mechanismů schopných provést ať již stavovou či bezstavovou konfiguraci uzlu v síti.

3.4.1 Objevování sousedů

Pro úspěšnou komunikaci po síti je kromě znalosti IP adresy nutné znát i adresu linkové vrstvy uzlu, se kterým se chystáme komunikovat. Tuto problematiku řeší objevování sousedů. To je v IPv6 definováno *RFC 4861: Neighbor Discovery for IP version 6*. Pokud uzel hledá adresu linkové vrstvy uzlu, pošle ICMP zprávu typu 135 (výzva sousedovi) na multicast adresu vzniklou kombinací prefixu ff02::1:ff00:0/104 a posledních 24 bitů hledané adresy. Tato výzva obsahuje adresu, kterou uzel hledá a případně i adresu linkové vrstvy odesilatele. Pokud tato výzva nalezne adresáta, jehož adresa odpovídá adrese hledané, ten odpoví ICMP zprávou typu 136 (ohlášení souseda), která kromě jeho adresy obsahuje i tři příznaky:

- **příznak R** – značí, že je odpovídajícím uzlem router,
- **příznak S** – značí, zda je tato zpráva odpovědí na výzvu či nikoliv,
- **příznak O** – značí, zda mají být přepsány současné informace.

Jak je již patrné z příznaku S, může uzel poslat i nevyžádanou ICMP zprávu ohlášení souseda. Učiní tak například ve chvíli, kdy dojde ke změně jeho adresy linkové vrstvy a pošle ji na multicast adresu ff02::1 (všechny uzly na lince).

Uzel si dále kontroluje dosažitelnost sousedů, se kterými byl v poslední době v kontaktu. Vyčkává a pokud dostane od vyšší síťové vrstvy informaci, že je s daným sousedem stále v kontaktu, považuje jeho adresu linkové vrstvy za dostupnou. Pokud po nějakou dobu toto potvrzení neobdrží, pošle sám výzvu sousedovi, aby zjistil jeho dostupnost.

3.4.1.1 Ohlášení routeru

Kromě jiného řeší RFC 4861 i ohlášení routerů jednotlivým uzlům. Pro tuto činnost definuje dva nové typy ICMP zpráv. Typ 133 výzvu routeru a typ 134 ohlášení routeru. Ohlášení routeru je pro každý nově příchozí uzel velmi důležitou zprávou. Sděluje uzlům, jakým způsobem probíhá v síti automatická konfigurace, kdo jsou implicitní routery, jaké jsou prefixy podsítě a mnohé další důležité informace. Tyto informace jsou obsažené přímo v úvodu zprávy jako takové nebo ve volbách, které jí následují. Její formát je uveden na obrázku 1.

<table>
<tr><td>8 b</td><td colspan="6">8 b</td><td>8 b</td><td>8 b</td></tr>
<tr><td>typ</td><td colspan="6">kód</td><td colspan="2">kontrolní součet</td></tr>
<tr><td>omezení skoků</td><td>M</td><td>O</td><td>H</td><td colspan="2">pref.</td><td>rezerva</td><td colspan="2">životnost routeru</td></tr>
<tr><td colspan="9">doba dosažitelnosti</td></tr>
<tr><td colspan="9">interval opakování</td></tr>
<tr><td colspan="9">volby …</td></tr>
</table>

Obrázek 1: Formát ICMP zprávy typu 134 ohlášení routeru

- **Omezení skoků –** říká uzlu na jakou hodnotu má u odesílaných zpráv nastavit položku maximum skoků.
- **M a O** – dva bity specifikující, jakým způsobem probíhá v síti automatická konfigurace. Pokud M nabývá hodnoty „1“ znamená to, že adresy i další nastavení jsou nastavovány pomocí DHCPv6. Pokud M nabývá hodnoty „0“ znamená to, že jsou adresy a směrovací prefix vytvářeny bezstavovou automatickou konfigurací. V případě získání adresy bezstavovou automatickou konfigurací určuje příznak O způsob, jakým jsou získávány informace o dalších nastaveních (např. adresy DNS serverů). Pokud příznak O nabývá hodnoty „1“, jsou tyto informace získávány z DHCPv6. Pokud je „0“ jsou informace získávány bezstavovou konfigurací.
- **H** – bit, určující zda router pracuje jako domácí agent pro počítače v této síti.
- **Životnost routeru –** určuje dobu v sekundách, po kterou má být router považován za implicitní v dané síti. Pokud je tato doba nastavena na hodnotu „0“, nemá být router používán jako výchozí.
- **Pref.** – 2 bitová volba, která upravuje preference při výběru implicitního routeru. „01“ značí vysokou, „00“ střední (výchozí), „11“ nízkou preferenci daného routeru jako implicitního. Kombinace „10“ je rezervována a nemá být používána. Pokud by použita byla, má s ní být naloženo jako s hodnotou „00“.

- **Doba dosažitelnosti –** upravuje dobu, po kterou má být cíl při objevování sousedů považován za dosažitelný.
- **Interval opakování –** nastavuje, jak dlouhá má být prodleva mezi výzvami sousedovi.
- **Volby –** rozšiřující prostor, pomocí něhož lze předat celou řadu informací o místní síti (např. MTU, místní prefixy, adresu linkové vrstvy routeru a mnohé další).

3.4.1.2 Automatická konfigurace směrování

Uzly jsou na základě informací, které si ukládají a které získávají díky funkcím definovaným v RFC 4861, schopny se sami naučit směrovat v síti, do níž jsou připojeny. Aby mohl uzel směrovat, musí si ukládat následující informace:

- **cache vazeb –** seznam uzlů, které jsou momentálně na cestách. Proto je třeba zaslat paket, určený těmto uzlům, na jinou adresu,
- **cache sousedů –** seznam uzlů (sousedů) na lokální lince, se kterými bylo nedávno komunikováno,
- **cache cílů –** seznam uzlů, se kterými bylo v poslední době komunikováno jak v rámci místní linky, tak i mimo ni. V případě lokálních uzlů odkazuje do cache sousedů. Jinak uchovává položku další krok (next hop), která určuje, kterému routeru má být paket předán, aby dorazil k cíli,
- **seznam místních prefixů –** určuje prefixy, které mají být považovány za místní,
- **seznam implicitních routerů –** určuje routery, které se ohlásily jako implicitní.

Samotný mechanismus směrování pak vypadá následovně:

1. Je zjištěno, zda je adresát v cache vazeb. Pokud ano, je změněna adresa cíle a je přidána hlavička směrování. Paket pak vstupuje do celého procesu znovu.
2. Je zjištěno, zda je adresát v cache cílů. Pokud ano, je paket poslán na adresu uvedenou v položce další krok, která je pro něj v této cache uvedena.
3. Je zjištěno, zda není jeho prefix uveden v tabulce lokálních prefixů. Pokud ano, je paket předán přímo adresátovi. Pokud ne, je paket předán jednomu z implicitních routerů.

Pokud dojde k situaci, že je takto paket nasměrován na router, který je součástí místní linky, nebo je poslán routeru, který ho musí v rámci místní linky předat dál, je odesílateli poslána ICMP zpráva typu 137 přesměrování. Tato zpráva obsahuje adresu cíle a adresu, kam má být pro příště paket pro tohoto adresáta poslán. Odesílatel si tuto informaci uloží do své cache cílů.

3.4.1.3 Zabezpečení objevování sousedů

Objevování sousedů, jak je nadefinováno v RFC 4861, poskytuje vcelku velký prostor pro útoky různého druhu. Tyto útoky probíhají tak, že se útočník vydává za jiný uzel nebo router. Případně může zablokovat bezstavovou konfiguraci adres tak, že bude o každé adrese tvrdit, že ji již používá. Reakcí na tento problém jsou různé formy zabezpečení objevování sousedů.

SEND

RFC 3971: SEcure Neighbor Discovery (SEND) definuje bezpečné objevování sousedů. Přidává další volbu pro ICMP zprávy objevování sousedů, která obsahuje digitální podpis. Jeho omezením je použití pouze ve spojení s kryptograficky generovanými adresami (CGA) a nelze ho použít pro ochranu standardně generovaných adres.

Jako další tento dokument řeší zabezpečení proti fungování neschválených routerů na nezabezpečené lince, které by na sebe mohly stahovat síťový provoz. Toto se řeší pomocí řetězení důvěry. Pokud uzel důvěřuje autoritě, která certifikovala router, případně autoritě jí nadřazené, důvěřuje i routeru jako takovému. K tomu používá dvě nové ICMP zprávy. Zprávu typu 148 výzva ke zjištění certifikační cesty a zprávu 149 ohlášení certifikační cesty.

RA-guard

RFC 6105: IPv6 Router Advertisement Guard definuje ochranu proti neschváleným routerům z opačné strany než SEND. Místo ochrany na straně uzlů chrání síťový provoz na aktivních prvcích. Aktivní prvek tak v rámci sítě propouští zprávy pouze routerům, které jsou schválené.

3.4.2 Inverzní objevování sousedů

Opačný účel, než objevování sousedů, má inverzní objevování sousedů definované v *RFC 3122: Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*. To, na základě známé adresy linkové vrstvy, zjistí IPv6 adresy uzlu. Pošle ICMP zprávu typu 141 výzva sousedovi pro inverzní objevování na adresu ff02::1, na linkové vrstvě tuto zprávu pošle pouze na adresu linkové vrstvy vybraného uzlu. V této zprávě musí být obsažena jak adresa linkové vrstvy dotazovaného, tak tazatele. Může také obsahovat IPv6 adresy rozhraní tazatele. Cílový uzel na tuto zprávu zareaguje ICMP zprávou typu 141 ohlášení souseda pro inverzní objevování. Tato zpráva musí obsahovat zdrojovou adresu linkové vrstvy a IPv6 adresy příslušného rozhraní vyzývaného uzlu.

3.4.3 Automatická konfigurace

Automatická konfigurace může probíhat několika různými způsoby. Bezstavová automatická konfigurace definovaná v *RFC 4862: IPv6 Stateless Address Autoconfiguration* na jedné straně spektra a konfigurace pomocí DHCPv6 na straně druhé. Lze použít i kombinaci obou těchto přístupů, kdy jsou některé informace uzlem získávány bezstavovou automatickou konfigurací a ostatní pak z DHCPv6.

Prvním krokem, který uzel po připojení do sítě učiní, je vytvoření vlastní lokální linkové adresy spojením prefixu fe80::/10 a ID rozhraní. Poté, co je tato adresa vytvořena, uzel zjistí, zda není tato adresa již v síti používána. K tomu využije funkci objevování sousedů, kdy se pokusí nalézt souseda s touto adresou. Pokud ho nenajde, adresu si přidělí. Poté vyčká na ICMP zprávu typu 134 ohlášení routeru, případně router sám požádá ICMP zprávou typu 133 výzva routeru o její zaslání.

Z příznaků v ohlášení routeru se dozví, zda má použít stavovou konfiguraci pro svou adresu a další parametry sítě. Dále pak je u každého ze zdejších prefixů uveden příznak, zda se pro tento prefix má použít bezstavová konfigurace adres. Pokud ano, připojí si k prefixu svůj identifikátor rozhraní a tuto adresu si přidělí. Už ji netestuje, protože jednoznačnost lokálního prefixu byla prověřena hned v počáteční fázi, když si uzel přiděloval lokální linkovou adresu [1 str. 123].

3.4.3.1 Bezstavová konfigurace DNS

Možnost bezstavové konfigurace je v *RFC 6106: IPv6 Router Advertisement Options for DNS Configuration* rozšířena o možnost předávat uzlům informace o DNS v síti. K tomu slouží dvě nové volby v ohlášení routeru a to volba typu 25, která obsahuje adresy rekurzivních DNS serverů, a volba typu 31, která obsahuje prohledávací seznam DNS. Tento seznam obsahuje přípony, které budou přidány za nekompletní doménové jméno v případě, nepodaří-li se ho přeložit.

3.4.3.2 DHCPv6

RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) definuje fungování protokolu DHCPv6. Ten v principu vychází z DHCP provozovaného na IPv4 sítích. Hlavním rozdílem je způsob identifikace uzlu, kterému je přidělována adresa. Zatímco DHCP používá k identifikaci uzlu adresu linkové vrstvy rozhraní, jehož prostřednictvím s ním komunikuje, DHCPv6 zavádí zcela nový identifikátor DUID. Tento identifikátor by měl podle definice zůstat po celou dobu fyzické existence uzlu neměnný a neměl by se měnit při změně rozhraní, kterým s DHCP serverem uzel komunikuje, ani při změně hardwaru nebo softwaru.

Účastníci DHCPv6 transakcí

Procesu přidělování adresy pomocí DHCPv6 se účastní tři druhy uzlů:

- **klient** – uzel získávající od serveru síťová nastavení,
- **server** – zařízení pověřené v síti správou a přidělováním IPv6 adres,
- **relay** – zařízení, které na lokálních linkách bez serveru přijímá a předává dále požadavky klientů.

Servery a relaye spolu tvoří skupinu takzvaných DHCPv6 agentů, což jsou zařízení, na která se může klient obrátit s žádostí o přidělení adresy.

Průběh přidělení adresy

Samotný průběh vyjednávání a přidělení adresy se od DHCPv4 příliš neliší.

1. Klient rozešle na multicast adresu všech DHCPv6 agentů na lince (ff02::1:2) zprávu s výzvou.
2. Zpráva (přímá nebo zprostředkovaná) vyvolá u serveru odpověď, ve které klientovi zašle svou preferenci a nastavení pro jednotlivá rozhraní.
3. Klient vyhodnotí všechny odpovědi, které od serverů dostane, a na základě uvedených preferencí vybere jeden, kterému pošle žádost o přidělení adresy.
4. Server na základě vlastního nastavení a lokální linky, v níž se klient nachází, vybere adresu nebo adresy, které klientovi pošle v odpovědi.
5. Klient ověří pomocí výzvy sousedovi, zda není adresa v síti již používána. Pokud není, přidělí si ji. Pokud je, pošle serveru zprávu s odmítnutím adresy.

Obnovování a rušení zápůjček adres

Adresy jsou klientům poskytovány pouze na omezenou dobu a v případě, že je klienti chtějí používat i nadále, musí server požádat o jejich prodloužení. Pokud server odmítne, může se klient pokusit najít jiný server a požádat ho o přechod pod jeho správu bez změny adresy pomocí žádosti o přechod. Pokud klient končí svou aktivitu v síti nebo chce zrušit zápůjčku své adresy, slouží mu k tomu zpráva uvolnění zápůjčky.

3.4.3.3 Bezstavové DHCPv6

Na nedostatky stavové i bezstavové konfigurace IPv6 adres reaguje *RFC 3736: Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*. Dokument kombinuje stavové a bezstavové získávání nastavení sítě. Uzel si v tomto případě sám nastaví adresu a směrování a od DHCP agenta obdrží doplňující nastavení, jako například adresy DNS serverů a další.

3.5 Směrování

Směrování v IPv6 nedoznalo zásadních změn, většina nejpoužívanějších směrovacích protokolů byla upravena tak, aby byla použitelná pro IPv6. Stejně jako v IPv4 jsou směrovací protokoly rozděleny do dvou rodin:

- **IGP –** slouží ke směrování uvnitř autonomních systémů a výměně informací nezbytných pro tento proces,
- **EGP –** slouží ke směrování v páteřní síti mezi jednotlivými autonomními systémy a výměně informací nezbytných pro tento proces.

3.5.1 IGP

Tato rodina protokolů slouží ke směrování uvnitř autonomních systémů. Je pro ně tedy výhodou rychlá reakce na změny v síti a celková nenáročnost.

RIPng

Routing Information Protocol next generation je definován v *RFC 2080: RIPng for IPv6*. Jedná se o úpravu RIPv2 pro IPv6 sítě. Princip funkce protokolu zůstal stejný. Stále se jedná o protokol založený na vektoru vzdáleností. Každé lince je přidělena cena a součtem těchto cen vznikne celková cena cesty, po které může paket putovat. Je vybrána linka s nejnižší cenou. Pro všechny RIPng routery na lince je používána multicast adresa ff02::9. Jasným omezením je rozsah ceny od 1 do 16, kdy cesta s cenou 16 je považována za neprůchozí. Díky této vlastnosti zbývá velmi málo prostoru pro samotné oceňování cest v závislosti na jejich průchodnosti. Ve většině případů je tak každá linka oceněna shodně cenou 1. Tento protokol je proto vhodný pro použití v menších a ne příliš komplikovaných sítích.

OSPFv3

Open Shortest Path First je protokol založený na stavu linek, verze pro IPv6 je definována v *RFC 5340: OSPF for IPv6*. Zásadní rozdíl oproti protokolům založeným na vektoru vzdálenosti spočívá v tom, že každý router pracující na tomto protokolu si uchovává mapu celé sítě (v případě větší sítě oblasti z ní vyčleněné) a z ní si vypočítává nejkratší cestu k cíli. Ocenění linek nabývá hodnot v rozmezí 0 – 65 535. Tento široký rozsah umožnuje správcům zohlednit při oceňování linek jejich prostupnost, stabilitu a další faktory

ovlivňující jejich preference. OSPFv3 používá dvě multicast adresy: pro všechny OSPF routery na lince adresu ff02::5 a pro všechny pověřené a záložní pověřené routery na lince adresu ff02::6.

IS-IS

Intermediate system to intermediate system je relativně starý protokol, který sloužil jako směrovací protokol v ISO/OSI modelu. Jeho použití pro TCP/IP definuje *RFC 1195: Use of OSI IS-IS for routing in TCP/IP and dual environments*. Tento protokol je velmi podobný protokolu OSPF, který z něj vychází. Stejně jako OSPF se jedná o protokol založený na stavu linek. Díky svému původu je tento protokol nezávislý na druhu provozu, který směruje, a tak byl jeho převod na IPv6 jeden z nejsnažších. Pro všechny IS-IS routery na lince je používána multicast adresa ff02::8.

EIGRPv6

Enhanced Interior Gateway Routing Protocol byl vyvinut společností Cisco Systems, Inc. Protokol je založený na vektoru vzdálenosti a snaží se odstranit některé nedostatky jeho předchůdců (RIP, IGRP) a přesto zůstat nenáročným a na změnu rychle reagujícím protokolem. V roce 2013 byl uvolněn jako otevřený standard. Funkcionalita EIGRP a EIGRPv6 není opět příliš rozdílná a jedná se především o úpravy umožňující práci v IPv6 síti. Pro všechny EIGRPv6 routery na lince je používána multicast adresa ff02::a.

3.5.2 EGP

Tato rodina protokolů slouží k směrování mezi jednotlivými autonomními systémy. Proto je u ní kladen důraz na zvládání velkých objemů směrovaných dat a na stabilitu.

MP-BGP4

Multiprotocol - Border Gateway Protocol je jediným používaným zástupcem rodiny EGP. Protokol BGP-4 je definován v *RFC 4271: A Border Gateway Protocol 4 (BGP-4)*. Podpora práce s IPv6 byla přidána v *RFC 4760: Multiprotocol Extensions for BGP-4*. Tento protokol je na rozdíl od protokolů rodiny IGP velmi konzervativní. Routery, se kterými si má vyměňovat informace nevyhledává sám, ale musí je zadat správce. Mezi routery se pak nevyměňují celé směrovací tabulky, ale pouze změny, ohlášení a zrušení cest. Protokol MP-BGP4 je možné použít i ke směrování uvnitř autonomních systémů, to však není příliš časté.

3.6 DNS

Podpora IPv6 v DNS je definována v *RFC 3596: DNS Extensions to Support IP Version 6*. Princip fungování je velmi podobný řešení použitému v IPv4. Je založen na principu dopředných a zpětných dotazů a AAAA a PRT záznamů.

AAAA

Tyto záznamy slouží k vyhodnocování dopředných DNS dotazů. Jejich ekvivalentem v IPv4 jsou A záznamy. Smyslem dopředného dotazu je zjištění IP adresy, případně IP adres ze známého doménového jména.

Pro počítač s doménovým jménem pocitac.example.org a IPv6 unicast adresou 2001:db8::1:211:22ff:fe33:4455 by AAAA záznam vypadal následovně:

pocitac AAAA 2001:db8::1:211:22ff:fe33:4455

Z principu IPv6 však vyplývá, že každý počítač má přiděleno hned několik IPv6 adres a je třeba rozhodnout, které adresy mají být zahrnuty do DNS a které nikoliv. V DNS by měly být především globální individuální adresy uzlu s dlouhodobější platností.

PTR

Slouží k přesně opačnému účelu než AAAA záznamy. Jejich úkolem je přeložit dodanou IPv6 adresu a tazateli vrátit doménové jméno uzlu, na který se ptá. Tento dotaz má formu doménového jména, které je složeno z převrácené IPv6 adresy a přípony ip6.arpa. V tomto případě nesmí být z adresy vynechány nuly. Zpětný dotaz na adresu 2001:db8::1:211:22ff:fe33:4455 pak bude vypadat následovně:

5.5.4.4.3.3.e.f.f.f.2.2.1.1.2.0.1.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2. ip6.arpa

Díky převrácení pořadí cifer adresy v dotazu lze oddělit prefix domény organizace a v PTR záznamech pak pracovat pouze se zbytkem adresy. Pokud má doména example.org prefix 2001:db8::/48, může pak PTR záznam našeho počítače vypadat následovně:

5.5.4.4.3.3.e.f.f.f.2.2.1.1.2.0.1.0.0.0 PTR pocitac.example.org

Existuje *RFC 2874: DNS Extensions to Support IPv6 Address Aggregation and Renumbering*, které přináší některé zajímavé změny. Ty však nebyly kladně přijaty, a proto byl jeho status změněn na experimentální.

4 Analytická část

Přechod firmy na novou verzi internetového protokolu je zásadní zásah do jejího ICT prostředí a je třeba k němu přistupovat s maximální obezřetností i s ohledem na možné dopady a minimalizaci možných problémů. Je třeba zvážit veškeré ekonomické, technické a právní aspekty migrace a na jejich základě se rozhodnout, v jakém časovém horizontu a v jakém rozsahu migraci provést.

4.1 Technicko-ekonomické aspekty migrace

Smyslem každého soukromého podnikání je generovat zisk a IT infrastruktura je k tomu ve větší či menší míře prostředkem. Je proto třeba zvážit možné ekonomické dopady migrace. Pokud podnik působí v oblasti, kde může z přechodu na nový protokol ekonomicky těžit, ať již získáním konkurenční výhody nebo naopak snížením nákladů na údržbu, je důvod přechodu zřejmý. Do této kategorie spadají kupříkladu poskytovatelé internetu a kabelové televize, mobilní operátoři, firmy provozující web hosting, datacentra a serverhousy. Pokud tyto firmy zjistí poptávku na trhu, budou se dozajista snažit převést alespoň část své infrastruktury na IPv6 tak, aby mohly poskytovat svým zákazníkům potřebné služby. Společnosti, kterým neplyne z přechodu na IPv6 žádný zřejmý přínos, nebo se v jejich případě jedná o zanedbatelnou úsporu v porovnání s vynaloženými prostředky na přechod, s tímto krokem váhají a implementace IPv6 pro ně není lákavá. Tyto společnosti by však měly učinit alespoň kroky nutné pro přípravu migrace tak, aby předešly zbytečným nákladům a případným právním a technickým problémům:

1. Zohlednit při plánování a pravidelné obnově informačních technologií možný přechod a nakupovat již produkty s podporou IPv6. Protokol IPv6 lze ve většině případů nasadit velmi ekonomickým způsobem v rámci přirozeného nákupu nových zařízení. Jestliže však nákupní proces nezohledňuje specifické požadavky protokolu IPv6, mohou vzniknout dodatečné náklady, když je později vyžadován rychlý přechod [2 str. 108].

2. Zajistit dostatečné proškolení zaměstnanců IT tak, aby byli připraveni na přechod a byli schopni předcházet nově vznikajícím problémům. V současné době již většina používaných operačních systémů i síťových prvků IPv6 podporuje. Na mnohých je tato funkce zapnuta a nastavena jako preferovaná, v sítích tak může probíhat čilý provoz založený na IPv6 bez vědomí správců těchto sítí, což přináší bezpečnostní a technická rizika, která mohou způsobit nemalé škody.

IPv6 trh v České republice

Penetrace IPv6 na českém trhu zatím není široká, ale leckteré odvětví by takový dynamický růst uvítalo. Podle statistik společnosti Google, Inc. přistupuje k jejich vyhledávači více jak 8% uživatelů z České republiky právě pomocí protokolu IPv6 [3]. Celosvětově se pak toto číslo pohybuje lehce pod 5%. V září 2013 přitom přistupovalo k tomuto vyhledavači z České republiky prostřednictvím IPv6 pouze 1,7% uživatelů [4].

Na v září 2013 bylo na českém internetu 1 062 383 domén. Z tohoto počtu bylo 200 288 domén dostupných prostřednictvím IPv4 i IPv6 a 33 domén bylo dostupných pouze pomocí IPv6. V září 2014 bylo z celkového počtu 1 140 046 domén 250 691 domén dostupných prostřednictvím obou protokolů a 36 domén dostupných pouze prostřednictvím IPv6 [5]. To znamená, že v září 2013 bylo 18,9% českých domén dostupných prostřednictvím IPv6 a v září 2014 to bylo již 22,9%.

Z těchto dvou ukazatelů vyplývá, že roste počet uživatelů schopných konzumovat obsah prostřednictvím IPv6 a stejně tak i nabídka toho obsahu. V případě uživatelů připojených prostřednictvím IPv6 je tento nárůst opravdu markantní.

4.2 Právní aspekty migrace

Evropská unie a spolu s ní i Česká republika se snaží na svém území podporovat rozvoj IPv6 a zvýšit jeho podíl na internetovém provozu. Snahy Evropské unie podporovat rozvoj IPv6 nejsou žádnou novinkou. V roce 2008 vydala Evropská komise Akční plán pro nasazení internetového protokolu verze 6 v Evropě [6].

Za účelem implementace IPv6 ve správních strukturách evropských zemí vznikl i Evropskou komisí podporovaný projekt *6GEN*. Česká republika patří mezi jeho účastníky

a na poli dostupnosti státní správy a samosprávy ČR je jedním z jeho nejprogresivnějších členů.

Česká ani evropská legislativa neupravuje a nespecifikuje chování soukromých subjektů ve vztahu k IPv6. Česká vláda však upravuje chování státní správy ČR, a to v usnesení vlády České republiky č. 727 z roku 2009. V tomto usnesení se uvádí:

II. ukládá ministrům a vedoucím ostatních ústředních orgánů státní správy zajistit

1. od 30. června 2009 při pravidelné obnově síťových prvků jejich kompatibilitu s internetovým protokolem verze 6 (IPv6),

2. do 31. prosince 2010 přístup k internetovým stránkám a veřejně dostupným službám eGovernmentu internetovým protokolem verze 4 (IPv4) i internetovým protokolem verze 6 (IPv6);

III. doporučuje hejtmanům a primátorovi hlavního města Prahy postupovat obdobně podle bodu II tohoto usnesení [7].

Toto usnesení je důležité nejen pro státní instituce, ale i pro soukromé podniky, které jim IT infrastrukturu a služby dodávají.

4.3 Mechanismy pro přechod

Mechanismy určené pro přechod z IPv4 na IPv6 se dělí do tří základních skupin:

- dvojí sada protokolů (dual stack),
- tunelování,
- překládání.

V případě, že nepůjde o nově postavenou infrastrukturu, která nebude připojená k internetu, bude zapotřebí použít k přechodu na IPv6 některý z těchto mechanismů. Nejspíše se však bude jednat o jejich kombinaci.

4.3.1 Dvojí sada protokolů

Dvojí sada protokolů je pravděpodobně nejběžnější formou přechodového mechanismu. Jedná se o používání jak IPv4, tak IPv6 v jedné síti. Uzly musí podporovat oba dva protokoly, mají oba druhy adres a mají v DNS jak A tak AAAA záznamy. Tento způsob je

relativně snadno implementovatelný, pokud všechny uzly na síti podporují IPv6. Je však pracnější na údržbu, protože je třeba spravovat dvě sady nastavení místo jedné.

4.3.2 Mechanismy tunelování protokolů

Tunelování umožňuje síťový provoz pomocí protokolu na síti, která jej nepodporuje. Tunely přenášející IPv6 pakety po IPv4 sítích již prokázaly svou hodnotu při testování IPv6 protokolu sítí *6bone*. V současnosti jsou využitelné pro připojení částí sítě, které zatím nejsou dosažitelné pomocí IPv6, ale se vzrůstající dostupností IPv6 připojení u poskytovatelů bude význam těchto tunelovacích mechanismů upadat. S budoucím postupným přibýváním čistě IPv6 sítí naroste potřeba tunelovacích mechanismů pro přenos IPv4 provozu po takovýchto sítích. Úskalím tunelů jsou možné problémy s výkonem a efektivitou připojení způsobené fragmentací. Zatímco IPv6 má nastaveno minimální MTU na 1280 bajtů, u IPv4 je to pouze 68 bajtů.

Manuálně konfigurované tunely

Tento základní způsob tunelování je popsán v *RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers*. Jde o způsob tunelování mezi dvěma body. Oba uzly musí tudíž mít dvojí sadu protokolů. Pro přenos se používá protokol 41 (IPv6 zapouzdření). Tento protokol podporuje většina routerů. Jeho nevýhodou je především složitější správa a s rostoucím počtem propojených oblastí rychle narůstá i počet potřebných tunelů.

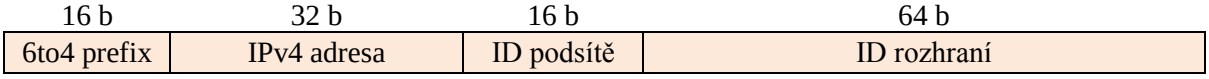
GRE tunel

Tento tunel, vyvinutý společností Cisco Systems, Inc., je definovaný v *RFC 2784: Generic Routing Encapsulation (GRE)*. Jedná se o univerzální tunelovací nástroj použitelný pro tunelování IPv6 provozu přes IPv4 síť. Jeho využití a omezení jsou podobná jako ta u manuálně konfigurovaných tunelů. Protokol spojuje dva uzly, které musí mít dvojí sadu protokolů.

6to4 tunel

RFC 3056: Connection of IPv6 Domains via IPv4 Clouds definuje další způsob tunelování. Cílem tohoto protokolu je propojení IPv6 sítí prostřednictvím IPv4 internetu. Předpokladem pro fungování takového tunelu je existence 6to4 routeru v síti, který má přidělenu veřejnou IPv4 adresu. Z IPv4 adresy si router vytvoří IPv6 prefix pro celou svou síť. Ten sestává z prefixu 2002::/16 společného pro všechny 6to4 sítě a 32 bitů IPv4

adresy. Takto vzniklé adresy mají formát popsaný na obrázku 2; za prefixem sítě o délce 48 bitů následuje 16 bitů pro rozlišení podsítí a 64 bitů ID rozhraní.



Obrázek 2: Formát 6to4 adresy

Poté, co si router takovouto adresu vytvoří, oznámí do své vlastní sítě, že je přes něj dosažitelná síť 2002::/16. Pokud je mu zaslán paket pro jinou 6to4 síť, zabalí ho do IPv4 hlavičky a odešle na IPv4 adresu uvedenou v IPv6 adrese. Použije k tomu protokol 41 (IPv6 zapouzdření). Problematika komunikace čistě IPv6 a 6to4 je řešena pomocí relay routeru, které jsou připojeny jak do IPv6, tak IPv4. Směrování z IPv6 sítě do 6to4 sítě probíhá pomocí standartních směrovacích postupů a relay router ohlašuje, že je přes něj dostupná síť 2002::/16. Po přijetí paketu pro tuto síť postupuje stejně jako jakýkoliv jiný 6to4 router. Směrování opačným směrem je však náročnější; původní specifikace navrhuje ke směrování použít BGP nebo statické směrování. *RFC 3068: An Anycast Prefix for 6to4 Relay Routers* přináší řešení tohoto problému. Podle této specifikace si 6to4 router nastaví jako výchozí adresu pro IPv6 komunikaci adresu 2002:c058:6301::. Tato adresa obsahuje IPv4 adresu 192.88.99.1, což je anycast adresa pro všechny 6to4 relay routery.

IPv6 nad MPLS

K přenášení IPv6 komunikace nad MPLS[5] infrastrukturou lze přistupovat dvěma způsoby:

- **tunelování mezi hraničními routery IPv6 sítí –** v tomto případě je vytvořen tunel v tunelu. Oba hraniční routery musí mít dvojí sadu protokolů a IPv6 paket je zapouzdřen dvakrát: nejprve do paketu IPv4 a poté do rámce MPLS [2 str. 77],
- **propojení IPv6 sítí pomocí IPv6 hraničních routerů poskytovatele** – tento způsob provozu IPv6 nad MPLS je definován v *RFC 4798: Connecting IPv6 Islandsover IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*. Hraniční routery poskytovatele připojení musí v tomto případě podporovat IPv6 a MP-BGP4 tak, aby byly schopny směrovat pakety ke správným hraničním routerům na druhé straně.

[5] Multiprotocol Label Switching – mechanismus pro směrování dat ve vysoce výkonných telekomunikačních sítích.

ISATAP

Tento mechanismus pro propojení jednotlivých IPv6 uzlů uvnitř IPv4 síti je definovaný v *RFC 5214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*. Princip tohoto propojení je velmi podobný 6to4, je však určený pro tunelování uvnitř sítí. Komunikaci IPv6 uzlů uvnitř IPv4 sítí řeší bez použití multicastu, který není v IPv4 sítích často implementován, a dalších speciálních požadavků. Adresa každého uzlu je tvořena prefixem podsítě a speciálním ID rozhraní, které obsahuje IPv4 adresu. Formát ID rozhraní je znázorněn na obrázku 3. Prvních 32 bitů identifikátoru má hodnotu 0000:5efe pro IPv4 lokální adresy a 0200:5efe pro IPv4 globální adresy. Tento rozdíl je způsoben přítomností „u“ bitu na sedmé nejvýznamnější pozici identifikátoru. Druhých 32 bitů ID rozhraní je tvořeno IPv4 adresou.

16 b	16 b	32 b
0000 00**u**0 0000 0000	5efe	IPv4 adresa

Obrázek 3: Formát ID rozhraní pro ISTAP

Uzel si z tohoto ID rozhraní vytvoří lokální linkovou adresu a adresy s prefixy sítí, do nichž patří. Komunikace po IPv4 pak probíhá jednoduše, odesílatel si z IPv6 adresy cíle vyjme jeho IPv4 adresu a na ni zašle IPv6 paket zapouzdřený do IPv4. Problémy spojené s absencí multicastu, a tím pádem nemožnosti získávat ohlášení routeru, jsou řešeny pomocí seznamu potenciálních routerů. Tento seznam má každý uzel a obsahuje IPv4 adresy ISATAP routerů, na které uzel v přednastavených intervalech posílá výzvu routeru. Routery nerozesílají svá ohlášení pravidelně, ale pouze na vyžádání od uzlu. Plnění seznamu potenciálních routerů probíhá většinou z IPv4 DNS, kde bývají adresy těchto routerů uvedeny v A záznamu pro jméno „isatap“. Tyto routery pak slouží jako druhé konce tunelů.

6over4

V *RFC 2529: Transmission of IPv6 over IPv4 Domains without Explicit Tunnels* je definován způsob propojování IPv6 uzlů; tyto uzly musí mít dvojí sadu protokolů. Výrazným omezením je skutečnost, že v síti musí fungovat IPv4 multicast. Unicast adresy uzlu jsou tvořeny 64 bity prefixu sítě a 64 bity ID rozhraní. ID rozhraní vznikne spojením 32 bitů naplněných nulami, za které je připojena IPv4 adresa uzlu. Pro mapování IPv6 multicast adres na IPv4 multicast adresy je použit jednoduchý mechanismus; poslední

2 bajty IPv6 multicast adresy jsou připojeny za IPv4 prefix 239.192.0.0/16. Pro zjišťování unicast adres se pak používá mechanismus objevování sousedů.

Teredo

Automatický tunelovací mechanismus umožňující průchod přes NAT[6]. Byl vyvinut společností Microsoft Corporation a je definován v *RFC 4380: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*. Je vhodný spíše pro otestování IPv6 a ve firemních sítích nemá přílišné uplatnění. Pomocí teredo serveru si klient otevře průchod skrz NAT, který využívá pro komunikaci s ostatními teredo klienty. Pro komunikaci s nativním IPv6 internetem používá klient teredo relay router.

6rd

Mechanismus umožnující poskytovatelům internetu nabídnout svým zákazníkům přístup k IPv6 bez nutnosti výměny infrastruktury. Je definován v *RFC 5569: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)*. Mechanismus sice umožňuje rychlé nasazení, klade však velké nároky na potřebné množství IPv6 adres. Každá 6rd adresa je uvozena prefixem sítě poskytovatele, který nesmí být delší než 32 bitů. Poskytovatel proto musí získat dostatečně velký blok adres pro použití 6rd.

Formát 6rd adresy je uveden na obrázku 4. Za 32 bity prefixu poskytovatele následuje IPv4 adresa routeru zákazníka. V případě, že se IPv4 adresy zákazníka dají sloučit do bloku se společným prefixem, může se jednat o prefix tohoto bloku adres. Bity, které zbydou po odečtení součtu délky prefixu poskytovatele a IPv4 adresy zákazníka od 64 bitů, mohou být použity pro definování podsítě. Za nimi následuje ID rozhraní o délce 64 bitů.

N(maximálne 32) b	M b	(64 - N - M) b	64 b
Prefix poskytovatele	IPv4 adresa	ID podsítě	ID rozhraní

Obrázek 4: Formát 6rd adresy

Dual-Stack Lite

Tento mechanismus tunelování IPv4 paketů přes IPv6 síť je definován v *RFC 6333: Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*. Je určen pro poskytovatele internetu, kteří se kvůli nedostatku IPv4 adres rozhodnou převést

[6]Network Address Translation – mechanismus překladu jednoho adresního prostoru na jiný. V praxi často slouží k přístupu počítačů z lokální sítě s neveřejnými adresami do internetu.

svou síť čistě na IPv6 a nadále chtějí zákazníkům poskytnout přístup k IPv4 internetu. Celý systém pracuje se dvěma prvky:

- **B4 –** Basic Bridging Broad Band je hraniční prvek v zákaznické síti,
- **AFTR –** Address Family Transition Router je hraniční prvek ústící do internetu.

Pokud chce uzel v domácí síti kontaktovat uzel v internetu, pro který existuje pouze IPv4 záznam, kontaktuje domácí B4. Ten jeho IPv4 paket zabalí do IPv6 paketu a odešle AFTR, který funguje jako NAT, což znamená, že pro celou poskytovatelovu síť došlé pakety rozbalí, přeloží a odešle cíli. Na rozdíl od IPv4 NAT si kromě IPv4 adresy a portu odesílatele poznamená i IPv6 adresu B4, který mu zprávu předal, aby byl schopen odpověď odeslat do patřičné zákaznické podsítě.

4.3.3 Mechanismy překladu protokolů

Obecný princip překladu mezi IPv4 a IPv6 adresami je specifikován v *RFC 6145: IP/ICMP Translation Algorithm*. Pro převod IPv4 na IPv6 používá adresy s vloženou IPv4 adresou. Překlad pak probíhá jednoduše tak, že je za prefix vložena IPv4 adresa. Překlad opačným směrem, a sice z IPv6 na IPv4, je specifikován pouze pro adresy s vloženou IPv4 adresou. Definici překladu jiných adres ponechává na jednotlivých překladových mechanismech. Kromě překladu adres řeší toto RFC i překlad mezi IPv4 a IPv6 hlavičkami a překlad zpráv mezi ICMPv4 a ICMPv6. Možné scénáře překladů a návrhy řešení těchto situací jsou pak popsány v *RFC 6144: Framework for IPv4/IPv6 Translation*. Z těchto situací jsou pro nás zajímavé především tyto:

- **situace 1: přístup z IPv6 sítě do IPv4 internetu –** uzly z čistě IPv6 sítě, které se snaží dostat k obsahu prezentovanému pouze na serverech dostupných prostřednictvím IPv4,
- **situace 2: přístup k IPv6 síti z IPv4 internetu –** servery běžící v čistě IPv6 síti snažící se zpřístupnit svůj obsah IPv4 klientům,
- **situace 3: přístup k IPv4 síti z IPv6 internetu –** servery běžící v čistě IPv4 síti snažící se zpřístupnit svůj obsah IPv6 klientům,
- **situace 5: přístup z IPv6 sítě do IPv4 sítě –** stejné jako v situaci 1 pouze internet je nahrazen intranetem,

- **situace 6: přístup z IPv4 sítě do IPv6 sítě –** stejné jako v situaci 2 pouze internet je nahrazen intranetem.

NAT64

Jedná se o komplexní překladač umožňující stavový i bezstavový překlad adres, který je definován v *RFC 6146: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers.* Ke svému fungování dále potřebuje DNS64 definovaný v *RFC 6147: DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*. V současné době se jedná o preferovaný překladový mechanismus na hranicích síti. Je možné jím realizovat všechny varianty překladů popsané ve výše uvedených modelových situacích. Situace 1, 2, 5 a 6 je možné realizovat stavově i bezstavově. Situaci 3 je možné řešit pouze nasazením stavového NAT64.

NAT-PT

Překladový mechanismus předcházející NAT64. Byl definován v *RFC 2766: Network Address Translation - Protocol Translation (NAT-PT)* a následně odmítnut v *RFC 4966: Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status*, kterým byl jeho status změněn na „zastaralý“. Základní principy fungování NAT-PT jsou podobné jako u NAT64. Hlavním rozdílem mezi nimi je práce s DNS záznamy. A byly to především problémy, které způsoboval provoz NAT-PT v DNS, jenž vedly k jeho odmítnutí. Tento mechanismus je však implementován v mnoha starších zařízeních, a tak může být nejekonomičtější volbou zprovoznění překladu protokolů. Proto se s jeho nasazením stále setkáváme.

BIH

Tento mechanismus je definován v *RFC 6535: Dual-Stack Hosts Using "Bump-in-the-Host" (BIH)* a je používaný na koncových zařízeních, kterým má umožnit provoz aplikací vyžadujících přítomnost protokolu IPv4. Pokud se taková aplikace obrátí na DNS s žádostí o A záznamy, BIH požádá o AAAA záznamy pro stejné doménové jméno jako aplikace. Pokud je aplikaci vrácena z DNS adresa IPv4, může komunikovat normálně. Pokud však není A záznam nalezen, přiřadí BIH ke každé IPv6 adrese, která se mu vrátí jako AAAA záznam, IPv4 adresu z privátního rozsahu, jež má pro tyto účely přidělen. Dvojice IPv4 a IPv6 adres jsou pak uloženy pro pozdější použití. Pokud se aplikace později snaží odeslat paket na některou z těchto IPv4 adres, paket je přebalen do

IPv6 hlavičky a je odeslán na IPv6 adresu, které byla příslušná IPv4 adresa přiřazena. V případě, že přichází naopak IPv6 paket pro aplikaci z venku, je opatřen IPv4 hlavičkou, odeslán z IPv4 adresy a dvojice IPv4 a IPv6 adres je uložena.

4.4 Provedení migrace

Samotné provedení migrace by mělo být organizované a jako každý významný projekt rozdělené do jasně definovaných částí. V přípravné fázi by mělo dojít k rozboru výchozího stavu, zhodnocení možných scénářů migrace a provedení kroků nezbytných pro hladký průběh samotné migrace. Po dokončení by mělo následovat její zhodnocení.

4.4.1 Příprava na migraci

Migrace je velkým zásahem do podnikové ICT infrastruktury, a proto je třeba ji pečlivě naplánovat tak, aby nedošlo k narušení provozu a finančním ztrátám. Pro správné rozhodování je třeba mít dostatek informací.

Rozbor výchozího stavu

Před samotnou migrací je třeba zhodnotit výchozí situaci v podniku tak, aby bylo možno kvalifikovaně rozhodnout:

- zhodnotit přínosy, které z migrace podniku vyplývají, a na základě toho stanovit, jakou prioritu má pro podnik přechod na IPv6,
- zhodnotit rizika, která sebou nese přechod na nový protokol, i rizika, která naopak plynou ze setrvání u stávajícího protokolu,
- provést inventuru veškerého vybavení postiženého migrací, a to jak hardwaru, tak i softwaru,
- na základě potřeb podniku navrhnout varianty migrace,
- stanovit TCO[7] pro jednotlivé varianty migrace na IPv6 i možnost setrvání u IPv4.

Na základě těchto kroků by mělo být nashromážděno dostatek podkladů, aby bylo možno rozhodnout o rozsahu a časovém horizontu migrace.

[7] Total Cost of Ownership – ‚celkové náklady na vlastnictví', souhrn všech nákladů spojených s provozováním systému do konce jeho životnosti. Mezi tyto náklady patří mimo nákladů na pořízení především náklady na údržbu, opravy, administraci a školení.

Pilotní projekt

Úkolem tohoto projektu je otestovat:

- připravenost používaných komponent ICT infrastruktury pro práci s novým protokolem,
- přechodové mechanismy použitelné pro navrhovaný způsob migrace a určit, které z nich budou nejvhodnější,
- chování aplikací v novém prostředí,
- chování síťových služeb na novém protokolu,
- nové funkce protokolu IPv6.

Toto testování je vhodné provést v testovacím prostředí tak, aby nedošlo k zásahům do produkčního prostředí.

Dále by mělo v rámci pilotního projektu dojít k návrhu adresního plánu a školení zaměstnanců tak, aby byla organizace plně připravena na migraci v době jejího plánovaného začátku.

Předmigrační příprava infrastruktury

Samotná síťová infrastruktura by měla být na migraci ještě před jejím spuštěním řádně připravena. Je vhodné, aby byla síť hierarchicky členěná a modulární, což umožňuje provádět migraci po jednotlivých modulech, případně pouze v modulech, kde bude mít migrace pro společnost přínos. Dále je také vhodné zajistit, aby co největší množství infrastruktury podporovalo IPv6 a nebylo tak spolu s migrací na nový protokol potřeba vyměňovat velké části infrastruktury. Podpory IPv6 lze mnohdy docílit instalací nového firmwaru nebo operačního systému zařízení. Pokud není tato volba dostupná, je vhodné zařízení nahradit v rámci pravidelné obnovy ICT infrastruktury zařízením s podporou IPv6. Je třeba si uvědomit, že v případě klíčových prvků infrastruktury, nesoucích velkou část provozu, nestačí pouze softwarová podpora IPv6, ale je třeba pořídit prvky s hardwarovou podporou. V opačném případě totiž hrozí ztráta výkonu, přetížení prvků a z toho vyplývající potíže.

4.4.2 Migrace podnikové sítě

Pro úspěšné provedení migrace je důležité, aby byly jasně delegované osoby zodpovědné za dohled nad průběhem migrace a pověřené jejím řízením. Tento přechodový tým by měl mít jak dostatečné technické zázemí, tak pravomoc pro prosazování požadavků nezbytných pro provedení migrace.

V závislosti na velikosti organizace a rozsahu plánované migrace pak přicházejí v úvahu různé možnosti provedení, ve kterých se ve větší či menší míře uplatní dvojí sada protokolů, tunelování, překládání a jejich kombinace.

Migrace celé sítě pomocí dvojí sady protokolů

Tento typ migrace je dobrým způsobem, jak převést celou společnost na protokol IPv6 a neztratit přístup k IPv4 internetu. Umožňuje odložit problémy s aplikacemi nepodporujícími IPv6 na pozdější dobu. V případě, že již před migrací celá infrastruktura podporovala IPv6, se jedná o levný způsob provedení samotné migrace.

Nevýhody tohoto přístupu jsou:

- potřeba podpory IPv6 v celé infrastruktuře, což může přinést nemalé náklady spojené s její obnovou,
- zvýšená pracnost údržby, kdy správa dvou protokolů namísto jednoho povede k navýšení provozních nákladů.

Migrace části sítě pomocí dvojí sady protokolů

Pokud je migrovaná síť strukturovaná a modulární, lze provést migraci pomocí dvojí sady protokolů pouze v částech, kde nám plyne z této akce přínos. Omezí se tak provozní i pořizovací náklady spojené s migrací. Příkladem může být zpřístupnění firemních webserverů návštěvníkům přistupujícím prostřednictvím IPv6. V takovém případě je třeba nasadit dvojí sadu protokolů v podnikové hraniční síti, v jádru podnikové sítě a v datovém centru nebo případně pouze v jeho části.

Migrace části sítě s použitím kombinace přechodových mechanismů

Tento způsob migrace umožňuje migraci pouze části infrastruktury. Zbytek je možné ponechat v původním stavu. V tomto případě jsou na dvojí sadu protokolů převedeny pouze ty části sítě, ve kterých přechod přináší přínos (např. datové centrum nebo hraniční

síť). Mezi těmito částmi jsou pak vytvořeny tunely, které zajistí přenos IPv6 provozu po stávající infrastruktuře.

- V případě propojení bloků, jakými jsou například podniková hraniční síť a datové centrum, je vhodné propojit je pomocí statických ručně konfigurovaných tunelů mezi routery, například tunely GRE.
- Pro propojení koncových stanic kupříkladu s datovým centrem nebo jádrem podnikové sítě je pak vhodnější použít automatické tunelovací mechanismy, jako je ISATAP.
- V případě, že by docházelo k nadměrné zátěži routerů, které jsou statickými konci ISATAP tunelů, nebo v případě, kdy není vhodné, aby byly routery jádra sítě takto využívány, je možno použít takzvaného modulu služeb. Tento modul obsahuje routery, které slouží jako ukončení ISATAP tunelů a současně je spojují s požadovaným modulem. V případě, že bude i tento spoj realizován tunelem, je možné ponechat i jádro sítě bez podpory IPv6.

Zpřístupnění obsahu dostupného pomocí IPv6 prostřednictvím překladu

Zpřístupnění obsahu dostupného pomocí IPv6 prostřednictvím překladu je minimalistická verze migrace, kdy dojde k migraci pouze v hraničním modulu sítě a podle potřeb společnosti je IPv6 provoz překládán ve směru dovnitř, ve směru ven, nebo i v obou směrech. V současné době je nejpravděpodobnějším scénářem potřeby zpřístupnění podnikových serverů návštěvníkům zvenčí. Pro všechny případy je však řešením nasazení překladového mechanismu NAT64 ve spojení s DNS64. Varianta nasazeni NAT-PT není doporučená. NAT-PT je však stále implementován v mnoha zařízeních, která nepodporují NAT64 a je tak mnohdy nejlevnějším a nejrychlejším řešením.

4.5 Modelové příklady migrace

4.5.1 Model 1 – Velká společnost s pobočkami

Charakteristika podniku:

- více jak 10 000 zaměstnanců
- 200 poboček v rámci České republiky
- oblast činnosti společnosti je finančnictví

ICT prostředí:

- Pracovní stanice:
  - více jak 10 000 ks
  - operační systém Microsoft Windows 7
  - sdružené v doméně Windows
  - spravovány a nasazovány pomocí Microsoft System Center 2012 R2
- Servery:
  - větší množství serverů s operačním systémem Microsoft Windows v rozsahu Server 2008 R2 až Server 2012 R2
  - poštovní servery Microsoft Exchange Server 2013
  - web servery ve vlastním datovém centru
- Podnikový informační systém:
  - operační systém AIX
  - databáze Informix
- Komunikace:
  - různé typy IP telefony od společnosti Siemens AG
  - ústředny Siemens AG
- Síťová infrastruktura:
  - různé typy síťových prvků společnosti Cisco Systems, Inc.

Důvody pro migraci:

- snaha zpřístupnit svůj obsah na webu prostřednictvím IPv6
- příprava na vývoj v IT tak, aby v budoucnosti nedošlo ke zbytečným nákladům

Rizika migrace:

- Microsoft System Center 2012 R2 podporuje IPv6 pouze částečně [8]
- aplikace informačního systému a klient informačního systému nepodporují IPv6
- neznámá podpora IPv6 u starších typů IP telefonů
- starší síťové prvky podporují IPv6 pouze na softwarové úrovni

Navrhovaná řešení:

Z ekonomického hlediska je nejvýhodnější provést zpřístupnění obsahu návštěvníkům z internetu prostřednictvím IPv6 překladem v hraničním modulu. Toto řešení sice není dlouhodobé, ale ve střednědobém výhledu splní dané požadavky a umožní tak odložit komplexnější migraci infrastruktury na pozdější dobu. Dále je vhodné začít s přípravou na tuto pozdější fázi migrace, a sice při pravidelné obnově infrastruktury zohlednit požadavky možné migrace a nakupovat prvky s podporou IPv6 v požadované úrovni, zajistit proškolení klíčových zaměstnanců a v testovacím prostředí začít testovat nasazení IPv6.

4.5.2 Model 2 – Malá firma

Základní vlastnosti podniku:

- přibližně 10 zaměstnanců
- centralizovaná kancelář, možnost práce z domova
- oblast podnikání společnosti je projekční činnost

ICT prostředí:

- Pracovní stanice:
    - operační systémy Microsoft Windows 2000 až Windows 8.1
    - pracovní stanice nejsou sdružené v jedné doméně
- Ostatní síťové komponenty:
    - síťové datové uložiště
    - několik tiskáren různého stáří, některé připojené pomocí printserveru
    - IP telefon
    - router dodaný poskytovatelem připojení
- prezentace společnosti na webu zajištěna třetí stranou

Důvody pro migraci:

- zabránění problémům v síti způsobených samovolným spuštěním IPv6
- minimalizace bezpečnostních rizik spojených s provozem nespravované IPv6 sítě

Rizika migrace:

- náklady spojené s obnovou staršího hardwaru nepodporujícího IPv6
- zvýšené náklady na provoz sítě způsobené správou dvojí sady protokolů

Navrhovaná řešení:

Pro takto malý podnik s natolik různorodým ICT prostředím není migrace v současné době ekonomicky výhodná. Hlavní prioritou je předcházení možným rizikům způsobených nespravovaným provozem IPv6. Řešením tohoto problému je provedení inventury IPv6 provozu v síti a jeho možné následné omezení. V případě rozhodnutí zpřístupnit web prostřednictvím IPv6 je možné si tuto službu vyžádat u dodavatele, nebo změnit dodavatele služby.

4.5.3 Model 3 – Lokální poskytovatel internetu

Základní vlastnosti podniku:

- lokální poskytovatel bezdrátového připojení k internetu působící na území několika obcí
- přibližně 200 zákazníků

ICT prostředí:

- WiFi infrastruktura připojující zákazníky v pásmech 2,4 GHz a 5 GHz pomocí protokolů 802.11b, 802.11g, 802.11a a 802.11ac
- spoje v páteřní síti realizovány protokolem 802.11ac
- infrastruktura realizována modulárním systémem síťových prvků Mikrotik

Důvody pro migraci:

- možnost nabídnout zákazníkům připojení pomocí IPv6
- prohloubení vlastních znalostí

Rizika migrace:

- možné výpadky poskytované služby
- možné snížení výkonu
- zvýšení pracovní vytíženosti obsluhujících pracovníků

Navrhovaná řešení:

Ačkoliv prvky sítě dle specifikací podporují IPv6, je vhodné před samotnou migrací provést testování. V případě příznivých výsledků v testovacím prostředí, pak provést samotnou migraci pomocí dvojí sady protokolů. Migraci je vhodné započít v jádru sítě. Při následném připojování dalších segmentů sítě je nutné průběžně monitorovat chování sítě a zatížení jednotlivých prvků.

5 Zhodnocení výsledků

Pozice internetového protokolu verze 6 jakožto nástupce internetového protokolu verze 4 je v dnešní době již nezpochybnitelná. V oblasti internetu pak jeho nasazování prožívá nebývalou konjunkturu a kromě stránek, které jsou tímto protokolem dostupné, přibývá i uživatelů, jež mohou tento obsah konzumovat.

Pro zavedení IPv6 ve vnitřní podnikové síti však zatím mnohdy chybí důvody. Z ekonomického hlediska nevyváží případné přínosy nového protokolu často samotné pořizovací náklady migrace a zvýšené provozní náklady spojené s provozem dvojí sady protokolů.

Častým řešením pro zpřístupnění obsahu klientům prostřednictvím IPv6 je tak pouze parciální migrace v hraničním modulu sítě realizovaná překladem z IPv4 na IPv6. Případně migrace pouze částí sítě tak, aby byly splněny požadavky pro přístup k IPv6 obsahu a současně byla migrace provedena s minimálními náklady.

I v případě, že se podnik rozhodne migraci v současnosti neprovádět, je vhodné, aby se průběžně připravoval na možný přechod. Pak nebude ve chvíli, kdy bude migrace nezbytná, docházet ke zbytečnému nárůstu nákladů a budou eliminována možná rizika s nekvalitně provedenou migrací na nový protokol. Řešením těchto případných problémů je nákup IPv6 kompatibilních komponent do podnikové sítě v rámci pravidelné obnovy infrastruktury a dosažení dostatečné úrovně znalostí v oblasti IPv6 u klíčových zaměstnanců. Tyto kroky by měly umožnit minimalizaci rizik a snížení nákladů spojených s migrací na nový protokol a usnadnit tak jeho nasazení.

6 Závěr

Práce sumarizuje informace z dostupných pramenů a představuje minimální nezbytné penzum znalostí potřebných pro porozumění internetovému protokolu verze 6. Následně pak hodnotí možné postupy migrace na nový protokol a navrhuje řešení pro vybrané modelové situace v rámci různých podniků.

V přehledu řešené problematiky bylo popsáno fungování IPv6 s ohledem na problematiku migrace z IPv4 na IPv6. Dále jsou v ní uvedeny funkcionality a mechanismy podstatné pro fungování současných podnikových sítí.

V analytické části jsou pak řešeny mechanismy určené pro přechod na nový protokol a jsou v ní také sumarizovány důvody pro přechod z IPv4 na IPv6 a možné problémy s tímto krokem spojené. Nakonec práce představila tři modelové situace v rámci různě zaměřených podniků rozdílné velikosti a bylo navrženo jejich řešení.

Výsledkem těchto modelových situací není jednoznačné řešení. Každé provedení migrace na nový protokol je závislé na velkém množství vstupních podmínek a je k němu proto třeba přistupovat s ohledem na konkrétní požadavky podniku a vzít v úvahu také ekonomické, technické a právní aspekty tohoto kroku. Teprve na základě důkladné analýzy je následně možné připravit konkrétní plán migrace vhodný pro danou situaci.

7 Seznam použité literatury

1. **Satrapa, P.** *Internetový protokol verze 6.* Praha : CZ.NIC, z.s.p.p., 2011. 978-80-904248-4-5.

2. **McFarland, S., Sambi, M., Sharma, N., Hooda, S.** *IPv6: Kopletní průvodce nasazením v podnikových sítích.* Brno : Computer Press, 2011. 978-80-251-3684-3.

3. **Google.** Per-Country ipv6 adoption. *www.google.com.* [Online] [Citace: 22. listopad 2014.] http://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption.

4. **Jakub, Čížek.** IPv6 používají 2 % surfařů. U nás ještě o něco méně. *www.zive.cz.* [Online] Mladá fronta a. s., 30. září 2013. [Citace: 22. listopad 2014.] http://www.zive.cz/bleskovky/ipv6-pouzivaji-2--surfaru-u-nas-jeste-o-neco-mene/sc-4-a-170745/default.aspx.

5. **CZ.NIC.** Statistiky - IPv6 domény. *stats.nic.cz.* [Online] [Citace: 22. listopad 2014.] https://stats.nic.cz/stats/ipv6_domains/?rd=2014-10-31&dr=3y&tp=i-1m&ss=0&ds=normal&da=chart.

6. **Evropská komise.** The platform for EU Interparliamentary Exchange. *www.ipex.eu.* [Online] [Citace: 24. listopad 2014.] http://www.ipex.eu/IPEXL-WEB/dossier/files/download/082dbcc530b1bf490130bbb9ab404e63.do.

7. **Vláda České republiky.** Usnesení vlády České republiky č.727. *kormoran.vlada.cz.* [Online] 8. červen 2009. [Citace: 6. listopad 2014.] http://kormoran.vlada.cz/usneseni/usneseni_webtest.nsf/0/6BFDE5B071A154C5C12575E5004024F1/$FILE/727%20uv090608.0727.pdf.

8. **Microsoft.** IPv6 Support in Microsoft Products and Services. *technet.microsoft.com.* [Online] 3. červen 2014. [Citace: 21. listopad 2014.] http://technet.microsoft.com/en-us/network/hh994905.aspx.

9. **IANA.** Internet Protocol Version 6 Address Space. *http://www.iana.org.* [Online] 15. únor 2013. [Citace: 15. listopad 2014.] http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml.

10. **IANA.** IANA IPv6 Special-Purpose Address Registry. *http://www.iana.org.* [Online] 22. září 2014. [Citace: 15. listopad 2014.] http://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml.

11. **IANA.** Internet Protocol Version 6 (IPv6) Parameters. *www.iana.org.* [Online] 25. listopad 2014. [Citace: 26. listopad 2014.] www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml.

12. **IANA.** Protocol Numbers. *www.iana.org.* [Online] 25. listopad 2014. [Citace: 26. listopad 2014.] http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.

13. **IANA.** Internet Control Message Protocol version 6 (ICMPv6) Parameters. *www.iana.org.* [Online] 22. září 2014. [Citace: 26. listopad 2014.] http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml.

14. **Cisco.** NAT64 Technology: Connecting IPv6 and IPv4 Networks. *www.cisco.com.* [Online] duben 2012. [Citace: 26. listopad 2014.] http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html.

15. **Mehta, N., Healy, R., Odom, W.l.** *Směrování a přepínání sítí.* Brno : Computer Press, 2009. 978-80-251-2520-5.

8 Seznam použitých obrázků

9 Seznam tabulek

10 Seznam zkratek

6PE	IPv6 Provider Edge Routers
6rd	IPv6 Rapid Deployment
AFTR	Address Family Transition Router
AIX	Advanced Interactive eXecutive
B4	Basic Bridging BroadBand
BGP-4	Border Gateway Protocol 4
BIH	Bump in the Host
CGA	Cryptographically Generated Address
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DNS64	Domain Name System six four
DUID	DHCP Unique Identifier
EGP	Exterior Gateway Protocol
EIGRPv6	Enhanced Interior Gateway Routing Protocol
FMIPv6	Fast Handovers for Mobile IPv6
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv4	Internet Control Message Protocol version 4
ICMPv6	Internet Control Message Protocol version 6
ICT	Information and Communication Technologies
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
ILNPv6	Identifier/Locator Network Protocol version 6
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
IS-IS	Intermediate System to Intermediate System
IT	Information Technology
MP-BGP4	Multiprotocol Border Gateway Protocol 4
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAT64	Network Address Translation Six Four
NAT-PT	Network Address Translation - Protocol Translation
OSPFv3	Open Shortest Path First version 3
PTR	Pointer Record

RA-guard	Router Advertisement Guard
RFC	Request for Comments
RIP	Routing Information Protocol
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIPng	Routing Information Protocol next generation
RPL	Routing Protocol for Low-Power and Lossy Networks
RSVP	Resource Reservation Protocol
SEND	SEcure Neighbor Discovery
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WWW	World Wide Web

11 Přílohy

IPv6 prefix	Přiřazení	Reference
0000::/8	rezervováno IETF	[RFC4291]
0100::/8	rezervováno IETF	[RFC4291]
0200::/7	rezervováno IETF	[RFC4048]
0400::/6	rezervováno IETF	[RFC4291]
0800::/5	rezervováno IETF	[RFC4291]
1000::/4	rezervováno IETF	[RFC4291]
2000::/3	globální unicast adresy	[RFC4291]
4000::/3	rezervováno IETF	[RFC4291]
6000::/3	rezervováno IETF	[RFC4291]
8000::/3	rezervováno IETF	[RFC4291]
a000::/3	rezervováno IETF	[RFC4291]
c000::/3	rezervováno IETF	[RFC4291]
e000::/4	rezervováno IETF	[RFC4291]
f000::/5	rezervováno IETF	[RFC4291]
f800::/6	rezervováno IETF	[RFC4291]
fc00::/7	unikátní lokální adresy	[RFC4193]
fe00::/9	rezervováno IETF	[RFC4291]
fe80::/10	lokální linkové adresy	[RFC4291]
fec0::/10	rezervováno IETF	[RFC3879]
ff00::/8	multicast adresy	[RFC4291]

Tabulka 1: Rozdělení adresního prostoru IPv6 [9]

IPv6 prefix	Přiřazení	Reference
::1/128	smyčka	[RFC4291]
::/128	nedefinovaná adresa	[RFC4291]
::ffff:0:0/96	IPv4 mapované adresy	[RFC4291]
64:ff9b::/96	IPv4-IPv6 přeložitelné adresy	[RFC6052]
100::/64	blok adres pro zahazování paketů	[RFC6666]
2001::/23	adresy pro testování v rámci IANA	[RFC2928]
2001::/32	TEREDO	[RFC4380]
2001:2::/48	adresy pro testování výkonu	[RFC5180]
2001:db8::/32	adresy pro příklady v dokumentech	[RFC3849]
2001:10::/28	odmítnuto (dříve ORCHID)	[RFC4843]
2001:20::/28	ORCHIDv2	[RFC7343]
2002::/16	6to4	[RFC3056]
fc00::/7	unikátní lokální adresy	[RFC4193]
fe80::/10	lokální linkové adresy	[RFC4291]

Tabulka 2: Dobře známé (Well-Known) prefixy [10]

Rozšiřující hlavička	Název	Reference
0	hlavička voleb pro každý krok	[RFC2460]
43	hlavička směrování	[RFC2460][RFC5095]
44	hlavička fragmentace	[RFC2460]
50	hlavička pro zabezpečení obsahu	[RFC4303]
51	hlavička autentizace	[RFC4302]
60	hlavička voleb pro cíl	[RFC2460]
135	hlavička mobility	[RFC6275]
139	hlavička protokolu identity hostitele	[RFC5201]
140	hlavička protokolu Shim6	[RFC5533]
253	určeno pro experimenty a testování	[RFC3692][RFC4727]
254	určeno pro experimenty a testování	[RFC3692][RFC4727]

Tabulka 3: Čísla a názvy rozšiřujících hlaviček [11]

Protokol	Název	Reference
6	TCP	[RFC793]
8	EGP	[RFC888]
9	IGP	
17	UDP	[RFC768]
41	IPv6 zapouzdření	[RFC2473]
46	RSVP	[RFC2205][RFC3209]
47	GRE	[RFC2784]
58	ICMP – ICMP pro IPv6	[RFC2460]
59	NoNxt – žádná další hlavička	[RFC2460]

Tabulka 4: Čísla a názvy některých protokolů [12]

Typ	Název	Reference
0	rezervováno	
1	cíl je nedostupný	[RFC4443]
2	příliš velký paket	[RFC4443]
3	vypršel čas	[RFC4443]
4	problém s parametry	[RFC4443]
100, 101	pro soukromé pokusy	[RFC4443]
102–126	nepřiřazené	
127	rezervováno pro rozšiřování chybových zpráv ICMPv6	[RFC4443]
128	žádost o echo	[RFC4443]
129	odpověď na echo	[RFC4443]
130	multicast dotaz na posluchače	[RFC2710]
131	multicast ohlášení posluchače	[RFC2710]
132	multicast odhlášení posluchače	[RFC2710]
133	výzva routeru	[RFC4861]
134	ohlášení routeru	[RFC4861]
135	výzva sousedovi	[RFC4861]
136	ohlášení souseda	[RFC4861]
137	zpráva přesměrování	[RFC4861]
138	přečíslování routeru	
139	ICMP dotaz na informace o uzlu	[RFC4620]
140	ICMP odpověď s informacemi o uzlu	[RFC4620]
141	výzva sousedovi pro inverzní objevování	[RFC3122]
142	ohlášení souseda pro inverzní objevování	[RFC3122]
143	multicast ohlášení posluchače verze 2	[RFC3810]
144	žádost o adresu domácího agenta	[RFC6275]
145	odpověď na žádost o adresu domácího agenta	[RFC6275]
146	výzva ke zjištění mobilního prefixu	[RFC6275]
147	ohlášení mobilního prefixu	[RFC6275]
148	výzva ke zjištění certifikační cesty	[RFC3971]
149	ohlášení certifikační cesty	[RFC3971]
150	zpráva pro experimentální protokoly mobility (např. Seamoby)	[RFC4065]
151	ohlášení multicast routeru	[RFC4286]
152	výzva multicast routeru	[RFC4286]
153	ukončení multicast routeru	[RFC4286]
154	FMIPv6 zprávy	[RFC5568]
155	řídící zpráva RPL	[RFC6550]
156	ILNPv6 zpráva o změně lokátoru	[RFC6743]
157	dotaz na duplicitu adresy	[RFC6775]
158	potvrzení duplicity adresy	[RFC6775]
159–199	nepřidělené	
200, 201	pro soukromé pokusy	[RFC4443]
255	rezervováno pro rozšiřování informačních zpráv ICMPv6	[RFC4443]

Tabulka 5: Seznam typů ICMP zpráv [13]