Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

BAKALÁŘSKÁ PRÁCE

Přechodové mechanismy IPv6

Anna Janáčková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Janáčková Anna

Informatika

Název práce

Přechodové mechanismy IPv6

Anglický název

IPv6 transition mechanisms

Cíle práce

Bakalářská práce se zabývá technologiemi pro implementaci protokolu IPv6 v současných IPv4 sítích. Dílčími cíli práce jsou

- shrnutí dostupných technologií (standardy vytvořené do roku 2012 včetně)
- srovnání parametrů jednotlivých technologií

Tyto informace budou poté využity pro hlavní cíl práce, tedy k vytvoření obecné metodiky pro volbu vhodné přechodové technologie (resp. kombinace technologií) pro konkrétní síť a užití.

Metodika

V teoretické části práce jsou technologie porovnávány na základě technických (výkon, dostupnost na konkrétních platformách, a jiné) a netechnických parametrů (snadnost nasazení a správy) s využitím odborných zdrojů, příp. vlastních měření.

Praktická část práce je zaměřena na vytvoření metodiky pro výběr vhodných přechodových mechanismů a ověření výsledku na případových studiích modelujících nejčastější typ infrastruktury (domácnost, firemní síť, síť v datovém centru).

Harmonogram zpracování

1, 10/2012 - studium odborných zdrojů
2, 11/2012 - výběr přechodových mechanismů k porovnání, volba metrik hodnocení, zpracování měření
3, 1/2013 - 2/2013 - dokončení teoretické části a vyhotovení případové studie
4, 3/2013 - dokončení a odevzdání práce

Rozsah textové části

30-40 stran

Klíčová slova

IPv6, přechodové mechanismy, počítačové sítě, bezpečnost IPv6 sítí

Doporučené zdroje informací

SATRAPA, Pavel. IPv6: internetový protokol IPv6. Praha: CZ.NIC, 2008, 357 s. CZ.NIC. ISBN 978-80-904248-0-7.

KOZIEROK, Charles M. The TCP/IP guide: a comprehensive, illustrated Internet protocols reference. San Francisco: No Starch Press, c2005, 1539 s. ISBN 15-932-7047-X.

CHASSER, John M. Security Concerns in IPv6 and Transition Networks. Information Security Journal: A Global Perspective. 2010-10-28, roč. 19, č. 5, s. 282-293. ISSN 1939-3555. DOI: 10.1080/19393555.2010.514653. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/19393555.2010.514653

PUNITHAVATHANI, D. Shalini a K. SANKARANARAYANAN. IPv4/IPv6 Transition Mechanisms. European journal of scientific research. 34.1 (2009): 110-124. ISSN 1450-216x. Dostupné z: Academic Search Complete.

LIMONCELLI, Thomas A. a Vinton G. CERF. Successful strategies for IPv6 rollouts. Communications of the ACM. 2011-04-01, roč. 54, č. 4, s. 44-. ISSN 00010782. DOI: 10.1145/1924421.1924438. Dostupné z: http://portal.acm.org/citation.cfm?doid=1924421.1924438

IETF. RFC4057: IPv6 Enterprise Network Scenarios [online]. [cit. 2012-05-13]. Dostupné z: http://www.rfc-editor.org/rfc/rfc4057.txt

IETF. RFC4942: IPv6 Transition/Coexistence Security Considerations [online]. [cit. 2012-05-13]. Dostupné z: http://www.rfc-editor.org/rfc/rfc4942.txt

Vedoucí práce

Lohr Václav, Ing.

Termín odevzdání

březen 2013

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

V Praze dne 15.1.2013

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci „Přechodové mechanismy IPv6“ jsem vypracovala 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 autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 24. listopadu 2014 Anna Janáčková

Poděkování

Ráda bych touto cestou poděkovala Ing. Václavu Lohrovi, PhD., za odborné vedení, trpělivost a pomoc při psaní této bakalářské práce a také své rodině za podporu a externí disciplínu.

Přechodové mechanismy IPv6

IPv6 Transition Mechanisms

Souhrn

Práce poskytuje přehled mechanismů pro přechod z internetového protokolu IPv4 na IPv6 a přináší diskuzi o vhodnosti jejich implementace v různých sítích. Na základě vlastního návrhu typologií sítí a jejich výkonových a provozních charakteristik doporučuje obecnou metodiku, jak pro konkrétní síť zvolit vhodný přechodový mechanismus nebo kombinaci mechanismů. Případová studie v závěru práce aplikuje tuto metodiku na implementaci IPv6 ve společnosti poskytující zakázkový vývoj a provoz komplexních webových aplikací velkým korporátním klientům.

Summary

This thesis provides an overview of mechanisms designated for transition from the IPv4 internet protocol to IPv6 and brings discussion about their implementation in different networks. Based on it's own definition of typology of networks and their performance and operational characteristics, the thesis recommends a generic methodics to choose a suitable transition mechanism or combination thereof for particular network. Included case study shows this methodics applied to IPv6 implementation in a company specializing in development and servicing of complex web applications for large corporate clients.

Klíčová slova

IPv6, přechodové mechanismy, metodika přechodu, počítačové sítě

Keywords

IPv6, transition mechanisms, transition methodics, computer networks

Obsah

1 Úvod

Původní internetový protokol IPv4, popsaný v RFC761 ze září 1981, byl zpočátku, dle slov otce zakladatele Vinta Cerfa, myšlen jako experiment a měl sloužit k ověření, zda podobná technologie může vůbec fungovat. Poté měla být vytvořena „produkční“ verze protokolu. Délka adresy byla stanovena na – z hlediska experimentálního účelu postačujících – 32 bitů. Z testovacího protokolu se ovšem stala masově využívaná technologie.

V devadesátých letech začaly IPv4 prefixy docházet (tehdejší odhad vyčerpání rozsahu byl 10 let) a bylo zřejmé, že je potřeba protokol pozvolna nahradit novějším. Problém s nedostatkem IP adres byl ale v té době zažehnán přechodem z třídního schématu na CIDR (Classless Inter-Domain Routing) adresování a zájem o IPv6, jehož základ byl definován už v roce 1995, na nějakou dobu opět opadl.

Původní odhad vyčerpání adresního prostoru s CIDR adresováním v roce 2020 se ukázal jako mylný – poslední prefix přidělila IANA, organizace spravující zdroje Internetu, v únoru 2012. Lokální registrátoři ještě mají své rezervy, přesto se čím dál naléhavěji mluví o přechodu na IPv6.

Dne 6. 6. 2011 proběhl Světový den IPv6, v rámci něhož participující společnosti, instituce i jednotlivci na jeden den spustili podporu IPv6 v rámci svých služeb. O rok později, 6. 6. 2012 proběhl opět světový den IPv6, tentokrát pod názvem Světový start IPv6 a s cílem služby opět zapnout a nechat je spuštěné, ke kterému se připojily nejen velké společnosti jako Google, Facebook, Akamai nebo Comcast, v České Republice např. Seznam, Centrum a CZ.NIC.

Z technologické hračky nadšenců s neexistujícími standardy a nedostatečnou implementací v zařízeních a systémech, jakou IPv6 v devadesátých letech bezpochyby byla, se stala robustní technologie čím dál lépe připravená k celosvětovému nasazení. K tomu přispěla i organizace IPv6 Forum, poskytující certifikaci IPv6 Ready pro implementace v zařízeních a operačních systémech. Evropská unie vydává směrnice o nutnosti podpory IPv6 v dotovaných projektech, vlády různých států ji nařizují zákony.

Přes všechen tento vývoj zůstává před IPv6 bariéra zavádění nové technologie se všemi svými ekonomickými, organizačními, sociálními, psychologickými aj aspekty. Podpora IPv6 v internetových službách je celosvětové stále poměrně nízká. Tato práce se věnuje technickým aspektům přechodu na IPv6 a klade si za cíl shrnout jeho technické možnosti a umožnit zejména menším a středním společnostem snazší průběh přechodu pomocí vlastní metodiky pro výběr přechodových řešení.

2 Cíle práce a metodika

Práce si klade za cíl porovnat technologie pro implementaci protokolu IPv6 v současných IPv4 sítích a navrhnout obecnou metodiku poskytující oporu pro výběr vhodné technologie nebo kombinace technologií pro konkrétní podmínky běžně se vyskytujících sítí. Odhlížíme od problematiky přechodu na protokol IPv6 ve specializovaných (např. z hlediska bezpečnostních požadavků) sítích typu uzavřených armádních, nebo průmyslových systémů, apod.

Jednotlivé technologie jsou ke srovnání vybírány na základě dostupnosti na nejpoužívanějších platformách pro některou ze čtyř kategorií: pracovní stanice, servery, mobilní zařízení a síťové prvky. Podmínkou je existující a produkčně použitelná implementace v mainstreamovém vydání softwarového, resp. hardwarového produktu (operačního systému, hardwarového routeru nebo programu).

Technologie jsou porovnány na základě několika kritérií:

1. *Výkon implementace.* Důležitá je schopnost zvládnout běžný datový tok v dané kategorii. V důsledku využití přechodové technologie by nemělo docházet k výrazné degradaci kapacity konektivity či přenosové rychlosti. Dalším kritériem je dodatečná latence, která vzniká použitím technologie pro přechod.

2. *Náročnost zavedení a další správy.* Posuzuje se technologická náročnost nasazení a další správy během provozní fáze a nutnost významně zasahovat do stávající infrastruktury.

3. *Náklady na zavedení a provoz.*

4. *Vhodnost pro provoz v dané kategorii* (vč. bezpečnosti) (delegace reverzních zón atp.).

Získané informace jsou využity pro následný cíl práce: vytvoření obecné metodiky pro volbu vhodné přechodové technologie (resp. kombinace technologií) pro konkrétní síť a užití.

Praktická část práce je tvořena případovou studií o přechodu na IPv6 v sítích nové vybudovaného datového centra společnosti Etnetera, a.s.

3 Stav poznání problematiky

V této části přiblížíme základní odbornou literaturu a prameny, které vymezují naši problematiku v širších souvislostech. V následujících kapitolách práce budeme využívat četných dalších pramenů, které se týkají úzce problematiky IPv6 a jednotlivých přechodových mechanismů.

Kozierok (2005) poskytuje ucelený přehled TCP/IP. V tomto rámci se zabývá také charakteristikami sítí (Kozierok 2005, s. 90–93), které v naší práci využijeme pro výběr vhodného přechodového mechanismu.

Satrapa (2011) přináší – v českém prostředí unikátní – souhrn problematiky IPv6. Kniha obsahuje nejen základní informace o protokolu, routování, IPSec, mobilitě aj., ale také praktické informace o nastavení IPv6 na nejpoužívanějších platformách. Pro naši práci je nejdůležitější kapitola o přechodových mechanismech, která velmi obsáhle popisuje dostupné alternativy.

V roce 2005 vyšlo informační RFC4057, „IPv6 Enterprise Network Scenarios“ (Bound 2005). Jeho cílem je popsat scénáře přechodu na IPv6 v rámci korporátních sítí. Kromě sady základních scénářů nabízí i kategorizované otázky týkající se technických i organizačních aspektů jež je třeba vzít v úvahu při volbě řešení.

Publikace „IPv6 Deployment Guide“ (6NET 2008) vznikla v rámci evropského projektu 6NET, probíhajícího od ledna 2002 do konce prosince 2004. Jeho cílem bylo mj. i testování strategií pro přechod z IPv4 na IPv6. Součástí publikace jsou případové studie implementace IPv6 v sítích univerzit a výzkumných institucí.

Přechodem na IPv6 v segmentu výzkumných a korporátních sítí se zabývají také

Amoss a Minoli (2008) v publikaci „Handbook of IPv4 to IPv6 transition: methodologies for institutional and corporate networks“. V práci kromě základních protokolů, úvodu do programování IPv6 aplikací a bezpečnosti IPv6 sítí uvádějí také stav podpory na straně poskytovatelů konektivity po celém světě. Zabývají se také hardwarovou a softwarovou podporou IPv6. V oblasti operačních systémů pro servery a uživatelské stanice bohužel uvádějí pouze systémy společnosti Microsoft.

Kapitola o řešení přechodu (Amoss a Minoli 2008, s. 161–168) vychází z poznatků projektu 6NET a zdaleka není tak obsáhlá jako 6NET (2008). Poskytuje konkrétní návod na přechod pro výzkumné a univerzitní sítě; pro naše potřeby jsou ale informace příliš zastaralé.

Výrazně novější je pak informační RFC6180 „Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment“ (Arkko a Baker 2011), ve kterém autoři uvádí mechanismy pro použití v konkrétních situacích a vyjmenovávají faktory, které doporučují zohlednit při návrhu přechodových řešení. Tato doporučení uvádíme v kapitole 5.5 jako doplnění námi navrhované metodiky výběru přechodových řešení.

4 Přehled řešené problematiky

V této kapitole shrneme jednotlivé přechodové mechanismy, základy jejich fungování a případné problémy. Na konci uvádíme stav implementace v hardwaru a softwaru na nejčastěji používaných platformách.

4.1 Teoretické možnosti řešení

Pro propojení IPv6 a IPv4 sítí existují tři metody: dual stack, tunelování a překlad. V praxi se pak používají ruzné kombinace těchto metod. Přechodové mechanismy založené na těchto metodách popisujeme v následujících podkapitolách.

V rámci jednotlivých mechanismů můžou mít konkrétní uzly dle definice RFC4213 (Nordmark a Gilligan 2005) tyto tři role:

- *IPv4-only* – uzel, který implementuje pouze IPv4;
- *IPv6-only* – uzel, který implementuje pouze IPv6;
- *dualstackový (IPv6/IPv4)* – uzel, který implementuje jak IPv4, tak IPv6.

4.1.1 Dual Stack (RFC4213)

Dual stack je označení souběžného nativního provozu IPv4 i IPv6, nejedná se tedy o přechodovou technologii v pravém slova smyslu. Ostatní mechanismy jej ale potřebují ke svému fungování – dualstackové zařízení slouží jako brána mezi IPv6 a IPv4 světem. (Nordmark a Gilligan 2005)

V režimu dualstacku poskytuje operační systém dva oddělené IP stacky, tj. jaderný mechanismus operačního systému pro práci se sítí, všechno ostatní se řeší na aplikační úrovni. Aplikace si musí poradit nejen se dvěma stacky, ale také s odlišnostmi implementace obou protokolů; ne všechny vlastnosti IPv4 bývají dostupné i pro IPv6 (v linuxovém kernelu například zcela chybí podpora socketové volby IP_FREEBIND pro IPv6 stack). Infrastrukturní služby jako firewall, DNS, SMTP relay, HTTP proxy či DHCP musí v dualstackových zařízeních podporovat oba protokoly.

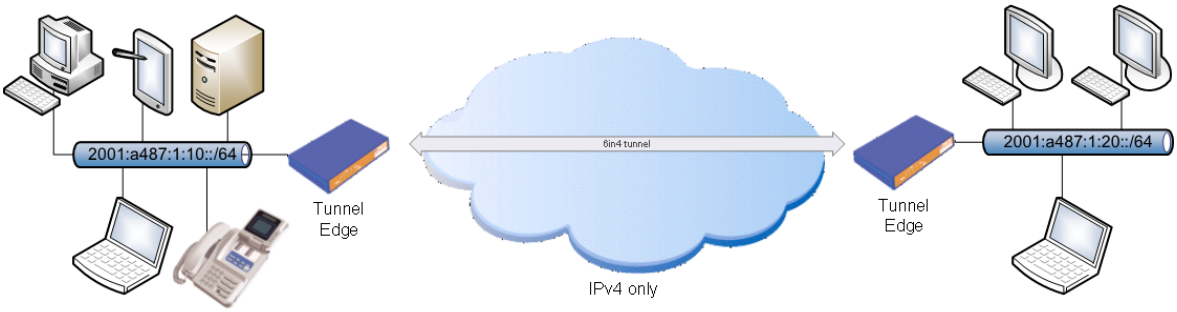
Implementace dual stacku na uzlu nebo v síti s sebou často přináší zvýšené nároky na správu – mnohá nastavení se musí dělat dvakrát (např. nastavení firewallů). Na druhou stranu je to jednoduché a přímočaré řešení, a jsou-li obě implementace srovnatelné kvality a s odpovídající infrastrukturou, nedochází k degradaci výkonu ani spolehlivosti. Odpovídající infrastrukturou máme na mysli, že v situaci, kdy například poskytujeme webovou službu pomocí obou protokolů, musíme disponovat stejně výkonnou farmou serverů jak pro IPv4, tak pro IPv6.

4.1.2 Tunelování

Tunelování je metoda, která řeší problém komunikace izolovaných uzlů, resp. sítí, IPv6 protokolem přes IPv4 sítě, nebo naopak IPv4 uzlů přes IPv6 sítě. Při tunelování se využívá kompozitního charakteru datagramu, který vždy sestává z hlavičky a z datové části, jejíž obsah je libovolný, může tedy obsahovat i celý datagram jiného protokolu. Celý nepozměněný datagram jednoho protokolu je tedy na jedné straně tunelu „obalen“ datagramem protokolu používaného přenosovou sítí a poslán na druhou stranu. Na té je datagram nalézající se uvnitř opět „rozbalen“ a zpracován, případně poslán dál nativní, tj. netunelovanou sítí.

Tunely mohou být statické nebo dynamické. Statický tunel vzniká nakonfigurováním speciálního síťového rozhraní, které zprostředkovává bránu do tunelu.

Původní standard pro tunelování počítá především se statickou konfigurací tunelu. Ta ale v prostředí dnešních sítí, kde se šetří IPv4 adresami pomocí dynamického přidělo-



Obrázek 4.1: Tunelovací mechanismus 6in4

vání a Carrier-Grade NATů, nefunguje správně. Proto vznikají nástroje pro dynamické nastavování tunelu, např. AICCU (*SixXS - IPv6 Deployment & Tunnel Broker* 2013). Ty jsou implementovány na klientské straně tunelu, komunikují se svým protějškem na opačném konci tunelu a provádí jeho dynamickou rekonfiguraci.

Nevýhodou tunelovacích mechanismů je především vyšší latence, zmenšování efektivní velikosti datagramů a tedy jejich fragmentace, a také nízká spolehlivost v důsledku špatného zpracování datagramů tunelu síťovými prvky na cestě (např. implicitní zahazování paketů s verzí 41 atd.). (Nordmark a Gilligan 2005; Satrapa 2011, s. 256–257)

Z těchto důvodů je třeba tunelování považovat pouze za krátkodobé řešení a mělo by co nejdříve být nahrazeno nativní konektivitou.

4.1.2.1 Tunelovací mechanismus 6in4 (RFC4213)

Norma RFC4213 popisuje tunelování IPv6 datagramů skrze IPv4 sítě, tzv. 6in4. Vstupní uzel tunelu sestaví datagram tak, že se k datagramu IPv6, který se stane datovou částí nově syntetizované jednotky, připojí hlavička protokolu IPv4. Koncový uzel tunelu původní datagram opět „vybalí“, tedy zbaví hlavičky IPv4, a dál jej posílá nativní IPv6 sítí. Aby síťové prvky po cestě poznaly, že se jedná o datagram 6in4 tunelu, v poli Protocol v IPv4 hlavičce se uvádí hodnota „41“ namísto „4“. (Nordmark a Gilligan 2005)

4.1.2.2 Tunelovací mechanismus 6to4 (RFC3056)

Mechanismus 6to4 je navržen pro propojování celých IPv6 sítí přes IPv4 konektivitu. (Carpenter a Moore 2001, s. 2) Výhodou protokolu je především nízká náročnost iniciální konfigurace – nevyžaduje změny v IPv4 síti, tunely jsou automatické.

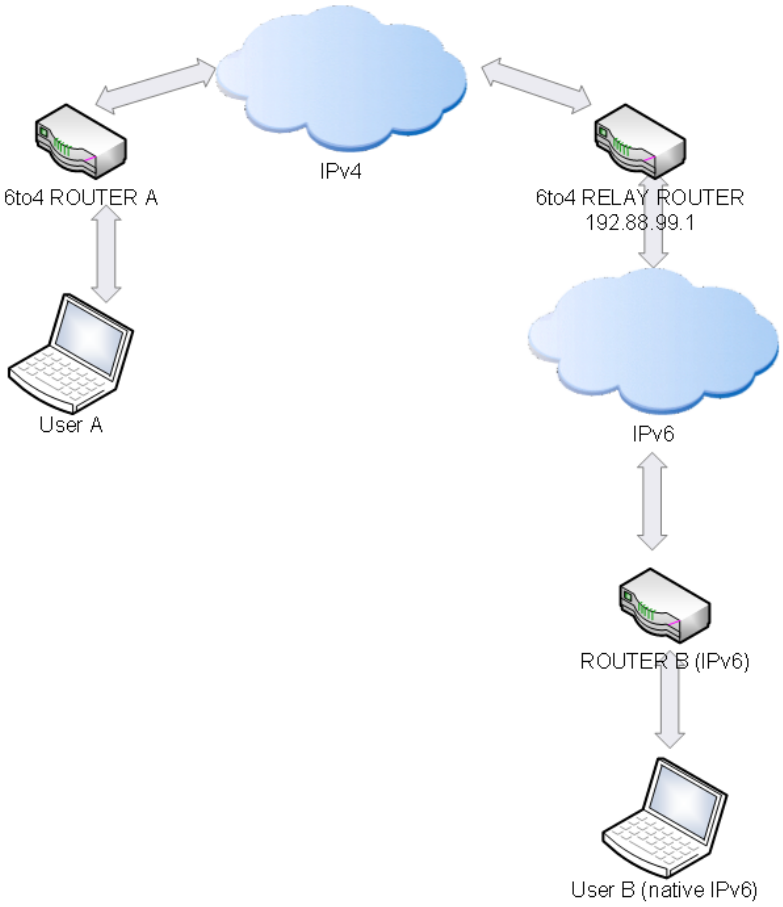
Bodem mezi IPv6 a IPv4 sítěmi je tzv. *6to4 router*. Jde o hraniční prvek sítě poskytovatele konektivity, který musí mít přiřazenou veřejnou IPv4 adresu. Pro sítě připojené přes 6to4 je vyhrazený prefix 2002::/16. Prefix sítě samotné je složen z obecného prefixu 6to4 (16 bitů) a IPv4 adresy *6to4 routeru* (32 bitů). Největší blok pro 6to4 sítě má tedy velikost /48.

Sítě používající 6to4 spolu mohou komunikovat napřímo. Pro komunikaci mezi 6to4 sítěmi a nativním IPv6 je potřeba zavést prostředníka – *relay router*. Relay router je normální router, který má jedno 6to4 rozhraní a druhé rozhraní připojené k nativní IPv6 síti. Relay routery mají přidělenu vyhrazenou anycastovou adresu, tím je zajištěn výběr nejbližšího relay routeru. (Huitema 2001)

Schéma komunikace je znázorněno na obrázku 4.2.

Zásadní problém 6to4, především pro připojení serverů do sítě poskytovatele konektivity (ISP), je delegace reverzních DNS záznamů. Protože se v tomto případě nedá očekávat spolupráce poskytovatele, byla vytvořena speciální zóna 2.0.0.2.ip6.arpa, v níž jsou delegace spravovány, bohužel nepříliš bezpečným způsobem, jak přiznává i G. Huston (2008), prostřednictvím služby umístěné na URL https://6to4.nro.net/. Na reverzních záznamech přitom v dnešní době závisí mj. i doručování e-mailů nebo některé typy Single Sign-On autentizace.

Tunelovací mechanismus 6to4 nebyl v praxi nikdy příliš využíván. Důvodem byla vysoká chybovost. Podle Abena (2014) z organizace RIPE NCC až 10–15 % 6to4 spojení nefunguje. To je způsobeno asymetrickým směrováním, které je pro tento mechanismus běžné, a zahazováním proto-41 na firewallech. Pracovní skupina v6ops organizace IETF se pokusila standard 6to4 vyřadit už v roce 2011, a to s tím, že kvůli chybovosti je vzhledem k potřebě uspíšit nasazení IPv6 spíš kontraproduktivní. Jako alternativa byl



Obrázek 4.2: Tunelovací mechanismus 6to4

touto pracovní skupinou doporučeno využívání 6rd (IPv6 Rapid Deployment). (Troan 2011)

4.1.2.3 Tunelovací mechanismus 6rd (RFC5969)

Mechanismus 6rd pochází z komerční sféry. V roce 2007 nasadila francouzská společnost Free, ve spolupráci s R. Desprésem, upravený protokol 6to4 nazvaný 6rd (IPv6 Rapid Deployment). Vývoj a nasazení trvaly rekordních pět týdnů. (Townsley a Troan 2010, s. 1–2) Tuto technologii záhy implementovalo velké množstvi poskytovatelů z celého světa, mezi nimi například i Comcast.

Mechanismus 6rd vychází ze 6to4, odstraňuje jeho hlavní nedostatky. 6rd nepoužívá speciální prefix, ale nativní prefix poskytovatele. Jde tedy o jedinou zásadní změnu, která však celému řešení dodala implementační robustnost a odstranila jeho hlavní nedostatky. ISP tedy zajišťuje routing pouze pro své klienty. Poskytovatel také má pod svou kontrolou relay routery a může na ně dát garanci kvality služby (SLA). Tím odpadají problémy se spolehlivostí způsobené asymetrickým routováním a dalšími vlastnostmi původního 6to4. Klient navíc nemusí mít veřejnou IPv4 adresu. (Townsley a Troan 2010, s. 3)

4.1.2.4 Tunelovací mechanismus 6over4 (RFC2529)

Norma RFC2529, celým názvem „Transmission of IPv6 over IPv4 Domains without Explicit Tunnels“, popisuje způsob, jakým propojit izolované uzly s IPv6 v IPv4-only doménách. Tento mechanismus není pravým tunelem. Spíš využívá IPv4 jako linkovou vrstvu nebo „virtuální ethernet“.

IPv4 adresy mohou být pro účely 6over4 jak globální unikátní, tak privátní (RFC1918). Mechanismus ke svému provozu potřebuje fungující multicast na IPv4 vrstvě. Spojujeme-li více fyzických segmentů, je nutné, aby síť umožňovala multicastové routování. (Carpenter a Jung 1999, s. 1) Multicast je ovšem v IPv4 sítích podporován jen zřídka. Zřejmě i proto se 6over4 prakticky nepoužívá a neexistuje mnoho implementací ve smyslu hardwaru nebo softwaru podporujícího tento mechanismus. (6NET 2008, s. 65)

4.1.2.5 Tunelovací mechanismus ISATAP (RFC5214)

Mechanismus ISATAP je komplexnější obdobou 6over4. Zkratka ISATAP znamená „Intra-Site Automatic Tunnel Addressing Protocol“. Řeší komunikaci dualstackových uzlů uvnitř koncových sítí. Komunikaci mezi těmito sítěmi protokol naopak neřeší.

V případě nasazení mechanismu ISATAP je IPv4 využíván v podstatě jako linková vrstva. Na rozdíl od 6over4 nepotřebuje ISATAP ke svému fungování multicast na

IPv4 vrstvě. ISATAP rozhraní mají lokální linkové adresy generované podle vlastního vzoru odlišného od nativního IPv6, kde první část je prefix fe80::0200:5efe::, pokud je IPv4 adresa přenosové vrstvy globální unikátní, resp. fe80::0000:5efe:: pro privátní IPv4 adresy; druhou část lokální linkové adresy tvoří pak IPv4 adresa rozhraní.

V důsledku nepřítomnosti multicastu musí být některé vlastnosti protokolu IPv6 v případě ISATAP řešení přizpůsobeny. Jde o některé složky konceptu mechanismu Neighbor Discovery, na němž je komunikace v IPv6 sítích založena. Především je absence multicastu kompenzována na bázi unicastového adresování. (Templin, Gleeson a Thaler 2008, s. 6–8)

Klíčovým rysem této kompenzace je, že si koncový uzel uchovává dostupné routery v *seznamu potenciálních směrovačů* (PRL). PRL může být nastaven manuálně, dále tím, že příslušné informace získáme z DNS (v takovém případě musíme nastavit A záznamy pro uzel „isatap“), případně z DHCPv4. Jiné způsoby norma předpokládá, ale nespecifikuje. (Templin, Gleeson a Thaler 2008, s. 7)

4.1.2.6 Tunelovací mechanismus Teredo (RFC4380)

Mechanismus Teredo, definovaný v RFC4380 a nejčastěji využívaný v systémech MS Windows, je variantou automatického tunelování. Je funkční i za situace, kdy se koncová síť nachází za NATem a je adresována pomocí privátních IPv4 rozsahů (RFC1918). V dnešní době je několikanásobný NAT běžný, neboť poskytovatelům obecně docházejí adresy a uchylují proto se k používání Carrier-Grade NATu.

Při aplikaci Tereda není IPv6 paket vložen jako data do datové části datagramu IPv4, jako je tomu například u mechanismu 6in4, ale je vložen do UDP datagramu. Uzel za NATem (*klient*) nelze v tomto případě napřímo adresovat zvenku. Proto musí Teredo nejprve otevřít spojení směrem ven a navázat ho s druhou stranou po IPv4. Toto spojení zprostředkovává všem sítím dostupný Teredo server v Internetu.

Vyvoláním komunikace mezi dvěma klienty prostřednictvím Teredo serveru dojde k „otevření“ obou NATů. Poté spolu oba Teredo klienti komunikují napřímo. Pro sní-

žení výkonové režie další komunikace si klienty ukládají routovací tabulku pro partnery, se kterými v nedávné době komunikovaly.

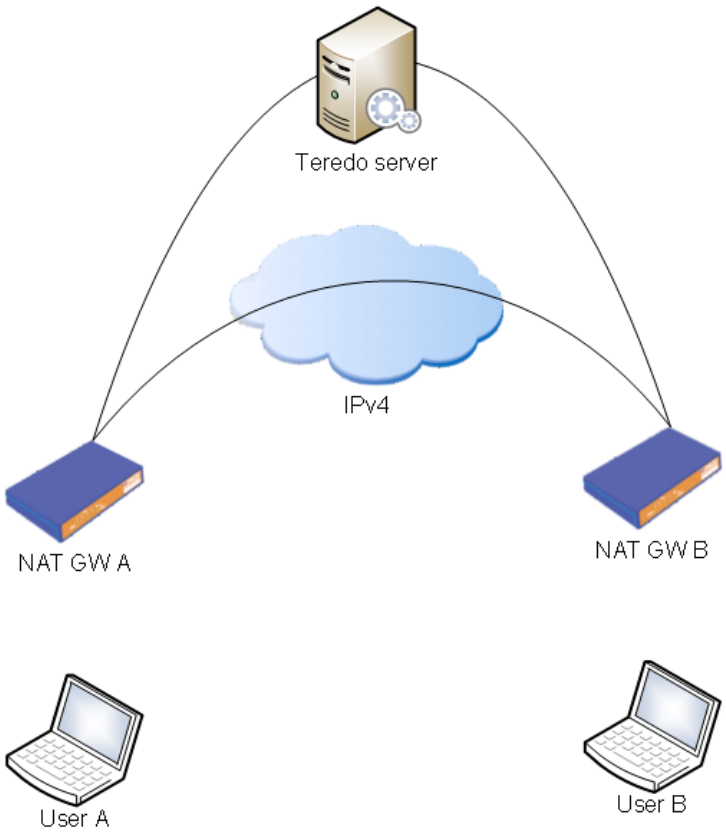
Mechanismus Teredo používá vyhrazený prefix 2001::/32. S nativním IPv6 světem komunikují klienti pomocí *Teredo relay serverů*, které mají jak Teredo rozhraní, tak rozhraní do nativní IPv6 sítě. Potřebuje-li Teredo klient komunikovat s uzlem v nativní IPv6 síti, jako první krok, ještě před navázáním spojení, pošle ICMPv6 Echo Request zprávu s adresou zamýšleného adresáta, pomocí které mechanismus najde nejbližší relay server. Z tohoto důvodu protokol vyžaduje, aby všechny koncové IPv6 uzly měly povolené ICMP Echo pakety. V opačném případě budou jejich služby pro uživatele připojené přes Teredo nedostupné.

Z uživatelského pohledu je použití protokolu Teredo velmi jednoduché. Pro mnoho operačních systémů existuje nativní klient. V internetu jsou Teredo servery i Teredo relay servery provozované různými skupinami, firmami a institucemi (mj. Microsoftem). V MS Windows je Teredo od verze Vista zapnuté v továrním nastavení.

Teredo má přesto své nevýhody. Mnohdy přináší uživatelům víc problémů, než výhod. Podle Hustona (2014) existuje celá řada důvodů, proč Teredo nedokáže navázat spojení. Z toho majoritní část selhává proto, že nefunguje ICMPv6 Echo při navazování spojení. Teredo spojení také dle měření tohoto autora mají při nejproblematičtější konstelaci latenci až o 3 vteřiny vyšší, než IPv4.

Tyto problémy lze částečně vyřešit přidáním různých Teredo prvků do sítí ISP. Poskytovatelům se však nabízejí výhodnější přechodová řešení, a tak tyto prvky neimplementují.

Spolu s vysokou výkonovou režií protokolu jsou zmíněné nedostatky důvodem, proč je Teredo bráno buď jako experimentální prostředek pro izolované domácí sítě, nebo jako poslední možnost, pokud jiný mechanismus není v daných podmínkách dostupný.



Obrázek 4.3: Tunelovací mechanismus Teredo

4.1.2.7 Tunelovací mechanismus Dual Stack Lite (RFC6333)

Dual Stack Lite (DS Lite) je poměrně nový (2011) mechanismus založený na principech relativně odlišných od jiných tunelovacích mechanismů. Aktuálně se nachází ve stavu Proposed Standard (předběžně navrhovaného standardu). Jeho cílem je umožnit využití IPv6 k překlenutí problémů s nedostatkem IPv4 adres a rozfázování implementace IPv6 v jednotlivých částech sítě poskytovatelů připojení tak, aby se celý přechod mohl dít postupně.

DS Lite infrastruktura se vyznačuje následujícími prvky:

- B4 (Basic Bridging Broadband) - prvek na straně zákazníka (CPE), často v roli SOHO routeru, který má na starosti tunelování, zároveň slouží jako brána a DNS proxy server;
- AFTR (Address Family Translation Router) - centrální NAT poskytovatele, případně navíc ALG (Application Layer Gateway).

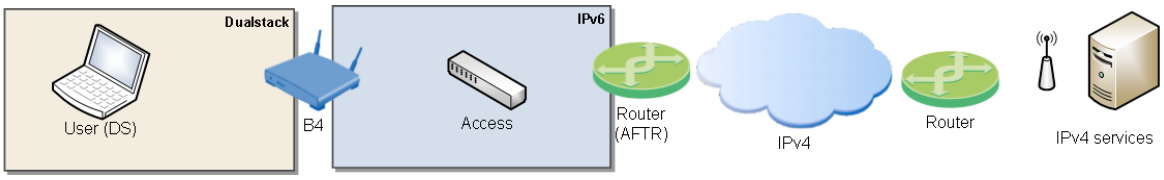
Kvůli možným problémům s fragmentací se doporučuje mít pro Dual Stack Lite na páteřní sítí MTU o 40b vyšší než ve zbytku sítě. Přenášený IPv4 paket nesmí být fragmentován, obalující IPv6 pakety fragmentovat lze. (Durand et al. 2011, s. 6)

Schéma infrastruktury přibližuje obrázek 4.4.

Koncová síť zákazníka může být buď dualstacková, nebo IPv4-only (pravděpodobně RFC1918).

Standard řeší tři možné modely provozu. (Durand et al. 2011, s. 3–5)

V *modelu přístupové sítě* se DS Lite používá namísto kaskády NATů na straně poskytovatele. Klientské uzly jsou dualstackové, přístupová síť používá IPv6. Důvodem tohoto nasazení bývá obvykle snazší správa řešení oproti NAT444, který neřeší nedostatek adres. Komunikace mezi koncovými uzly a internetem zůstává na stejném protokolu (IPv4 => IPv4, IPv6 => IPv6), není tedy potřeba ALG provádět překlad. Tunely mohou být terminované kdekoli v síti ISP, což umožňuje snadné horizontální škálování.



Obrázek 4.4: Tunelovací mechanismus Dual Stack Lite

V *modelu CPE* (Customer Premise Equipment) se DS-Lite používá k připojení domácí sítě, která zná pouze protokol IPv6. CPE v tomto modelu podporuje IPv6 a na WAN rozhraní implementuje B4 rozhraní. Klientské uzly jsou dualstackové. V tomto módu by CPE zařízení nemělo provádět NAT mezi lokální sítí a B4 rozhraním – funkce NATu je implementována na prvku AFTR. Tunelován je pouze IPv4 provoz, IPv6 je routováno nativní sítí.

V *modelu přímo připojeného zařízení* je v domácí síti pouze jedno zařízení připojené přímo k modemu (bez SOHO routeru) a fungující de facto jako CPE. Toto zařízení je dualstackové a chová se jako B4.

4.1.3 Překlad

Zatímco tunelování zajišťuje komunikaci oddělených IPv6, resp. IPv4 sítí přes páteřní síť druhého protokolu, *překladače* představují technologii pro komunikaci mezi IPv4 a IPv6 uzly. Hodí se především v situaci, kdy máme svoji IPv6 síť, ale potřebujeme komunikovat s IPv4 světem.

Nasazení těchto technologií je poměrně snadné – obvykle sestává ze zapojení hotového HW produktu od některého z dodavatelů routerů, nebo instalaci a pár příkazů u softwarové implementace. Většina z nich ke své práci potřebuje manipulovat s DNS. To přináší problémy s ověřováním DNS záznamů pomocí technologie DNSSEC a také s určováním cíle komunikace IP adresou.

U některých technologií je také nutné zasahovat do hlaviček aplikačních protokolů, kterým proto překladová brána musí být schopna rozumět. V praxi je v těchto zaříze-

ních podporována jen velmi omezená sada protokolů.

4.1.3.1 Překladový mechanismus NAT64 (RFC6146), DNS64 (RFC6147)

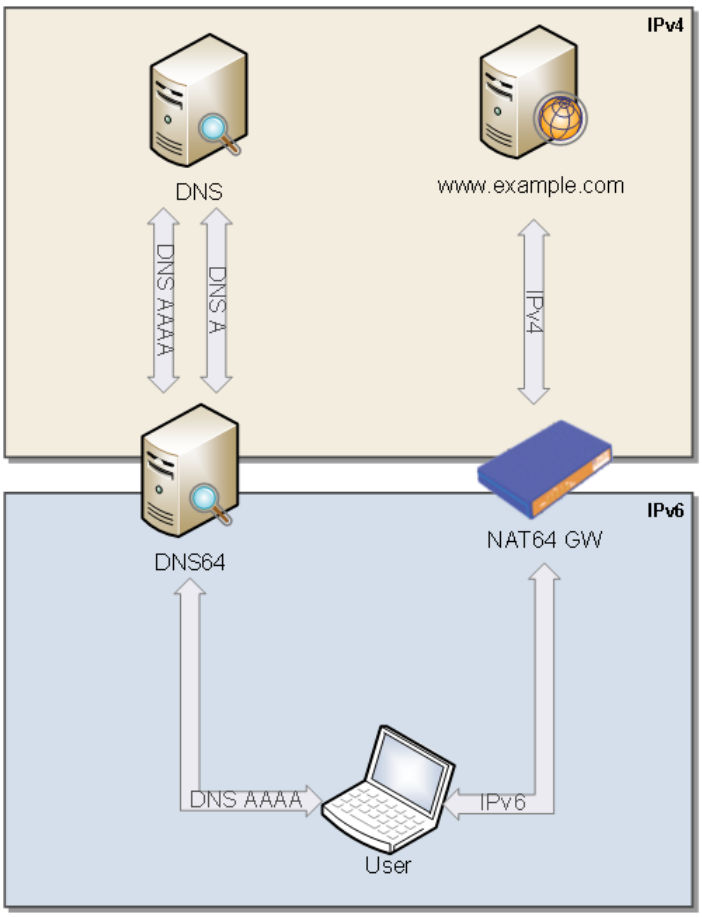
Jako NAT64/DNS64 označujeme mechanismus umožňující koncovým IPv6-only uzlům komunikovat s IPv4-only službami. Je schopný překládat protokoly TCP, UDP a ICMP. Hodí se pro jednoduché topologie s jednou defaultní bránou. Pro překlad hlaviček používá „IP/ICMP Translation Algorithm“ specifikovaný v RFC6145. (Bagnulo, Matthews a Beijnum 2011, s. 3)

NAT64 překladač je speciálni brána, která zprostředkovává překlad adres a protokolů z IPv6 na IPv4. Překladač má vyhrazený prefix, který používá pro IPv6-mapped IPv4 adresy a určitý rozsah IPv4 adres. Ostatní IPv6 prefixy brána směruje bez modifikace.

Tak jako u zaběhnutých IPv4 NATů, komunikaci lze iniciovat pouze směrem z IPv6 uzlů do IPv4 sítě. Předchůdce NAT64, označovaný NAT-PT, se snažil o vyřešení stavového překladu oběma směry. Pro svoji komplexnost a z ní plynoucí provozní problémy byl zavržen normou RFC4966 (Aoun a Davies 2007). Potřebujeme-li komunikovat z IPv4 dovnitř za NAT64 bránu, musíme na překladači staticky nadefinovat mapování adres.

Používáme-li doménová jména, je potřeba NAT64 doplnit o DNS64. Je-li pro dotazovaný IPv4 server k dispozici pouze A záznam, DNS64 služba z něj vytvoří IPv6-mapped adresu, kterou vrátí klientovi. Problémem se při modifikaci záznamů stává validace DNSSEC. Nedůvěřuje-li klient nejbližšímu rekurzivnímu DNS serveru, musí sám implementovat službu DNS64 a validaci provádět lokálně. (Bagnulo, Sullivan et al. 2011)

Schéma komunikace představuje obrázek 4.5.



Obrázek 4.5: Překladový mechanismus NAT64/DNS64

4.1.3.2 Překladový mechanismus Bump in the Host (RFC6535)

Mechanismus nazývaný Bump in the Host (BIH) umožňuje aplikacím, které znají pouze protokol IPv4, komunikovat s IPv6 sítěmi. Může být provozován jak na dualstackových uzlech, tak na uzlech, které mají pouze IPv6. BIH je implementován jedním ze dvou následujících způsobů: jako překladač na úrovni IP stacku, nebo na úrovni socketového API, což je doporučená varianta. (Huang, Deng a Savolainen 2012, s. 3)

Na síťové úrovni (Bump in the Stack) BIH zachycuje IPv4 pakety a pomocí mechanismu SIIT (RFC2765) je konvertuje na IPv6 pakety. Součástí procesu je modifikace DNS. Komunikuje-li aplikace směrem ven, vrstva Rozšíření DNS (ENR) pošle dotaz souběžně na A i AAAA záznam. Dorazí-li nazpět A, fáze překladu se vynechává. Vrátí-li se AAAA, dochází k překladu paketů a mapování IPv6 adres na privátní IPv4 adresy (RFC1918). Při komunikaci směrem dovnitř se s DNS záznamy nic neděje, pouze je vnější adresa namapována na odpovídající IPv4. (Huang, Deng a Savolainen 2012, s. 7–8) Potřebujeme-li funkční DNSSEC, musíme provádět validaci v rámci ENR.

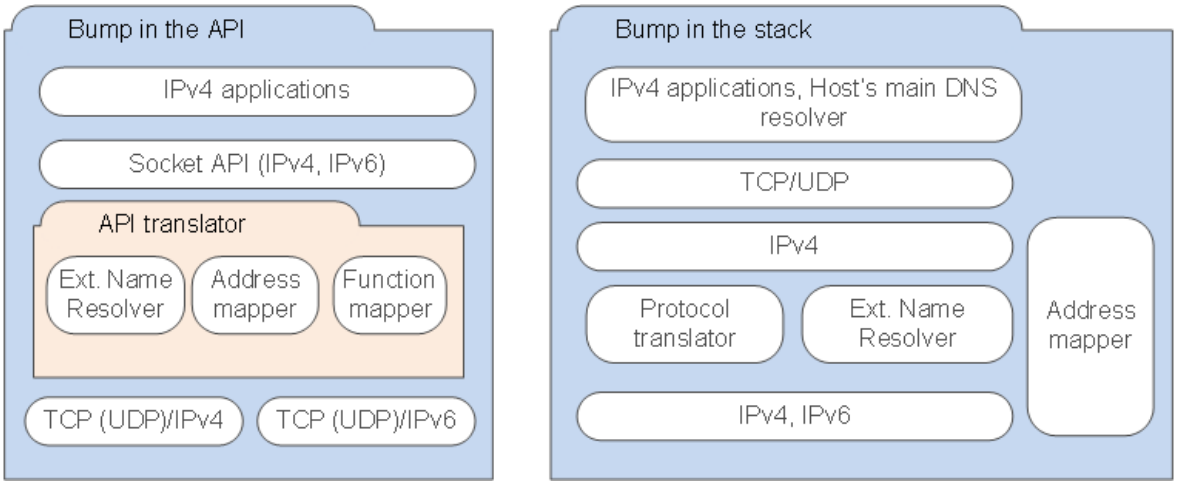
Je-li BIH implementován na vrstvě socketového API (Bump in the API), překladač zaměňuje IPv4 volání za volání univerzální anebo specifická pro IPv6. Validace DNSSEC v tomto případě nezpůsobuje potíže.

Používání BIH v kombinaci s dalšími překladovými mechanismy, především NAT64, se nedoporučuje. (Huang, Deng a Savolainen 2012, s. 3)

4.2 HW a SW podpora přechodu z IPv4 na IPv6

Instituce IPv6 Forum od roku 2003 provádí certifikaci hardwarových i softwarových implementací s názvem IPv6 Ready. Sdružení nabízí testování nejen základních protokolů, ale i protokolů pro routery a pokročilá síťová nasazení v několika testovacích laboratořích po celém světě. Pro veřejnost pak provozuje databázi certifikovaných implementací. (*IPv6 Ready Logo Program Frequently Asked Questions* 2014)

Jak se ukázalo při Světovém spuštění IPv6 (World IPv6 Launch) v roce 2012, pod-



Obrázek 4.6: Překladový mechanismus Bump in the Host

pora v současných počítačových systémech je v celkovém souhrnu dobrá, má však slabší místa.

Nedostatečná je prozatím v segmentu síťového hardwaru pro domácnosti. Systémy této kategorie, bývají založené na platformách s dobrou podporou IPv6, ale výrobci tyto možnosti platforem uživatelům nezpřístupňují. Sdružení CZ.NIC má projekt Katalog routerů, v jehož rámci testuje běžně dostupná zařízení. Výsledky jsou pro veřejnost dostupné v online katalogu (`http://www.katalogrouteru.cz/routers/all/`). Jeho záznamy potvrzují výše řečené.

Naopak na straně poskytovatelů připojení v ČR se situace zlepšuje. Datacentra, velcí poskytovatelé pro firmy a jiní důležití hráči v oboru nabízejí IPv6 jako běžnou součást svých služeb. V segmentu malých firem a domácností je podpora menší, ale i tak nikoli nevýznamná. K menším subjektům v tomto segmentu nedávno přibyly O2 Czech Republic a T-Mobile.

Dále uvádíme dvě tabulky zpracované pro účely naší práce, které ukazují dostupnost IPv6 a jednotlivých přechodových mechanismů na nejčastějších platformách.

Tabulka 4.1 ukazuje podporu základních protokolů v operačních systémech v roli koncového uzlu. Systémy pro uživatelské počítače a mobilní zařízení jsme do srovnání

vybrali na základě statistik webového provozu udávaných společnostmi StatsCounter a Net Applications (*Top 8 Operating Systems* 2014; *Operating system market share* 2014). Jde o nejvíce využívané systémy. Většina uvedených systémů používá jadernou implementaci USAGI (Linux, Android), nebo KAME (FreeBSD, Mac OSX). Částmi implementovanými v uživatelském prostoru, např. DHCP démony, se tyto systému mohou co do vybavenosti jednotlivými protokoly od sebe lišit.

Operační systém	Základní	Autokonfigurace	DHPCv6	ND-RDNSS
Linux (>= 2.6)	ano	ano	ano	ano
MS Windows (>= XP)	ano	ano	ano	ano [1]
Apple iOS	ano	ano	ano	ano
Apple Mac OSX	ano	ano	ano	ano
Android (>= 4)	ano [2]	ano	ne	ne

Tabulka 4.1: Podpora IPv6 v OS – koncové uzly

Tabulka 4.2 porovnává implementace přechodových mechanismů v nejběžnějších serverových systémech a síťových prvcích. Tak jako u koncových uzlů, některé funkce jsou dostupné přímo v jádře operačního systému, některé pomocí dodatečných programů v uživatelském prostoru. U síťových prvků tyto dvě kategorie v tabulce nerozlišujeme.

[1] Podpora s open source rozšířením rdnssd-win32.

[2] Částečná podpora, obsahuje řadu chyb.

SYSTÉM	6in4	DS Lite	6rd	NAT64, DNS64	Teredo
FreeBSD	nativní	ISC AFTR	nativní	tayga	miredo
Linux (>= 2.6)	nativní	ISC AFTR	nativní	ecdysis/jool, bind	miredo
MS Windows	nativní	–	–	MS Forefront UAG	nativní
Cisco IOS	nativní	nativní	nativní	nativní (v IOS XR)	–
Juniper JunOS	nativní	nativní	nativní	nativní	–

Tabulka 4.2: Dostupné softwarové implementace – routery

5 Návrh obecné metodiky

Žádný z mechanismů popsaných v předchozích kapitolách většinou nestačí k vyřešení přechodu v konkrétních podmínkách praxe sám o sobě. Především ve větších sítích, nebo v sítích se složitějšími podmínkami provozu, bývá nutné mechanismy kombinovat.

Tato kapitola popisuje metodiku, na jejímž základě lze navrhnout a volit optimální technické řešení pro přechod na IPv6 v libovolné síti.

Nejprve definujme termíny:

Přechodovým řešením rozumíme aplikaci jednoho nebo kombinace více přechodových mechanismů na konkrétní situaci sítě.

Pro účely metodiky rozdělujeme sítě na *koncové* a *tranzitní*, tj. takové, které slouží ke komunikaci koncových sítí.

Každá síť (resp. její podsíť) má následující části:

- upstream konektivitu;
- hraniční prvky sítě;
- uzly uvnitř sítě.

Každou komplexnější síť lze přitom rozdělit na podsítě o stejné struktuře.

Metodika je založena na tom, že s pomocí omezujících podmínek a srovnávacích kritérií, jež specifikujeme dále, lze jednoduchým algoritmem vybrat vhodné přechodové řešení.

5.1 Srovnávací kritéria

Podle Kozieroka (2005, s. 91–93) dělíme charakteristiky sítě na výkonové:

- rychlost,
- propustnost,
- latence,
- šířka pásma,

a ostatní nevýkonové (Kozierok 2005, s. 90):

- cena návrhu a implementace,
- kvalita, definovaná jako funkce kvality komponent a jejich vzájemného zapojení,
- využití standardních protokolů,
- spolehlivost,
- rozšiřitelnost, možnost úprav,
- snadnost správy a údržby,
- praktické otázky (premises, utility issues)

Porovnání takového množství ukazatelů je pro naše účely zbytečně složité. V praxi se ukazuje, že bude vhodné použít zjednodušený model a některé charakteristiky sloučit do jednoho kritéria.

Pro účely výběru přechodového řešení navrhujeme v této naší práci použití jednoho souhrnného výkonového kritéria, nazvěme ho *výkonnost*. Pomocí bodového ohodnocení udáváme, nakolik přechodové řešení odpovídá našim požadavkům zároveň z hlediska rychlosti, latence, šířky pásma i propustnosti.

Využití standardizovaných protokolů, které zmiňuje Kozierok, je pro nás automatickým předpokladem – vybíráme pouze z norem IETF, které jsou buď schváleny jako standardy, nebo se tomu limitně blíží. Tento postup doporučují i Arkko a Baker (2011, s. 7) v informačním RFC6180.

Praktickými otázkami nasazení (kabeláž atp.) se v této metodice nezabýváme.

Kritérium *pořizovací cena* v sobě zahrnuje náklady na pořízení nových prvků nebo programového vybavení potřebných pro přechod na IPv6 a na obnovu zastaralých technologií. Cena se liší případ od případu v závislosti na požadované kvalitě, množství a v neposlední řadě také cenové politice dodavatele. Jednotkou pro pořizovací cenu je nominální hodnota v používané měně.

Náročnost údržby technických prostředků se dle praktických zkušeností autorky nejsnáze stanovuje počtem zařízení a programových komponent (a případně vhodným přepočtem na hodiny, které je nutné údržbě věnovat). *Náročnost správy a údržby* přechodového řešení proto udáváme jako virtuální počet uzlů. Pro konkrétní přechodové mechanismy násobíme vhodným koeficientem na základě komplexnosti řešení (např. v případě dualstacku můžeme použít koeficient 2 – většinu komponent musíme nastavovat zvlášť pro každý z protokolů).

Náročnost správy a údržby je třeba doplnit kritériem *náročnost nasazení*. U tohoto kritéria je třeba zvážit prvky technické (např. komplexnost sítě a přechodového řešení) i netechnické (odbornost a zkušenost pracovníků). Jejich posouzení se opět promítne do bodového hodnocení.

Kritériem *spolehlivosti a stability* míníme především teoretické vlastnosti protokolů. Víme-li o nedostatcích zvolených technických prostředků v přechodovém řešení v této oblasti, zohledníme je v bodovém hodnocení.

Zjednodušený přehled kritérií uvádíme v tabulce 5.1.

kritérium	**jednotka**	**poznámka**
výkonnost	body	rychlost, propustnost, latence, šířka pásma
pořizovací cena	nom. hodnota	
náročnost na správu	body	počet uzlů vynásobený vhodným koeficientem
náročnost nasazení	body	
spolehlivost a stabilita	body	kvalita implementace, příp. ztrátovost, rozptyl latencí

Tabulka 5.1: Přehled srovnávacích kritérií

5.2 Situace sítí

Jako základní typologie sítí se často používá dělení na základě dosahu především na LAN (Local Area Network) a WAN (Wide Area Network). S rozvojem komunikačních technologií se k těmto kategoriím přidávají další, jako PAN (Personal Area Network), nebo MAN (Metropolitan Area Network). Toto dělení uvádí např. i Kozierok (2005, s. 81–83).

Sítě můžeme dále dělit podle účelu, za kterým jsou vybudovány, např.

- domácnosti a malé podniky,
- síť v datovém centru,
- firemní síť,
- průmyslové sítě,
- jiné sítě.

V praxi mají různé sítě rozdílné provozní charakteristiky, mezi než patří např. objem dat, které sítě přenášejí, aplikace a protokoly, které jsou v nich používány a v neposlední řadě i SLA (Service Level Agreement), tedy úroveň služby, kterou provozovatel garantuje svým zákazníkům.

Na počátku přechodu se sítě nacházejí v různých stavech a situacích. Tyto předpoklady je potřeba zvážit při konstrukci přechodových řešení. Zásadní pro volbu přechodového řešení je, zda stavíme síť novou, nebo potřebujeme nasadit IPv6 do sítě už existující. Volba řešení závisí také na organizačních limitacích provozované sítě.

5.3 Omezující podmínky

Omezujícími podmínkami rozumíme sourhrn požadavků a potřeb, které má přechodové řešení splnit. V rámci metodiky nám slouží k omezení výběru mechanismů na ty, které jsou v dané síti, resp. podsíti, reálně použitelné.

V první fázi eliminace vyřadíme mechanismy, jejichž nasazení v daném kontextu nemá význam. Máme-li například od poskytovatele nativní IPv6, není potřeba brát v úvahu mechanismy pro připojení naší sítě tunelem přes IPv4 od poskytovatele.

V druhé fázi eliminace vyřadíme mechanismy nedostupné na námi používaných platformách nebo takové, které v našich podmínkách nelze implementovat (např. nemáme-li multicast, nemůžeme použít 6over4).

Podstatnou omezující podmínkou je dostupnost implementace v produkční kvalitě.

Přechodové mechanismy popsané v kapitole 4 této práce doplňujeme v tabulce 5.2 o stručné charakteristiky pro podporu rozhodování podle naší metodiky.

5.4 Obecná metodika

Obecnou metodiku představíme jako algoritmus zapsaný vývojovým diagramem 5.1. V obecnosti jde o to rozdělit komplexní síť na základní celky (podsítě), popsat je pomocí

mechanismus	**použití**	**typ**	**jiné**
Dual Stack	souběžný provoz IPv4 a IPv6	nativní	zvýšené náklady na provoz
6in4	získání upstreamové IPv6	tunel	
6to4	získání upstreamové IPv6	tunel	nízká spolehlivost
6rd	získání upstreamové IPv6	tunel	
6over4	komunikace izolovaných IPv6 uzlů ve IPv4 síti	tunel	využívá multicast na IPv4
ISATAP	komunikace izolovaných IPv6 uzlů ve IPv4 síti	tunel	nepodporuje multicast
Teredo	získání upstreamové IPv6	tunel	nízká spolehlivost
Dual Stack Lite	tunelování IPv4 přes IPv6 páteř	tunel	
NAT64/DNS64	zpřístupnění IPv4 sítí pro IPv6-only uzly	překlad	omezená sada aplikačních protokolů
BIH	proxy pro nekompatibilní aplikace	překlad	

Tabulka 5.2: Shrnutí charakteristik přechodových mechanismů

charakteristik uvedených v tabulce 5.1 a vyjádřit tyto charakteristiky v příslušných jednotkách. Podle této kvantifikace se pak v průběhu výběru rozhoduje o vhodnosti jednotlivých řešení. Výběr se provádí metodami vícekriteriální analýzy variant.

5.5 Doporučení pro výběr přechodových řešení dle RFC

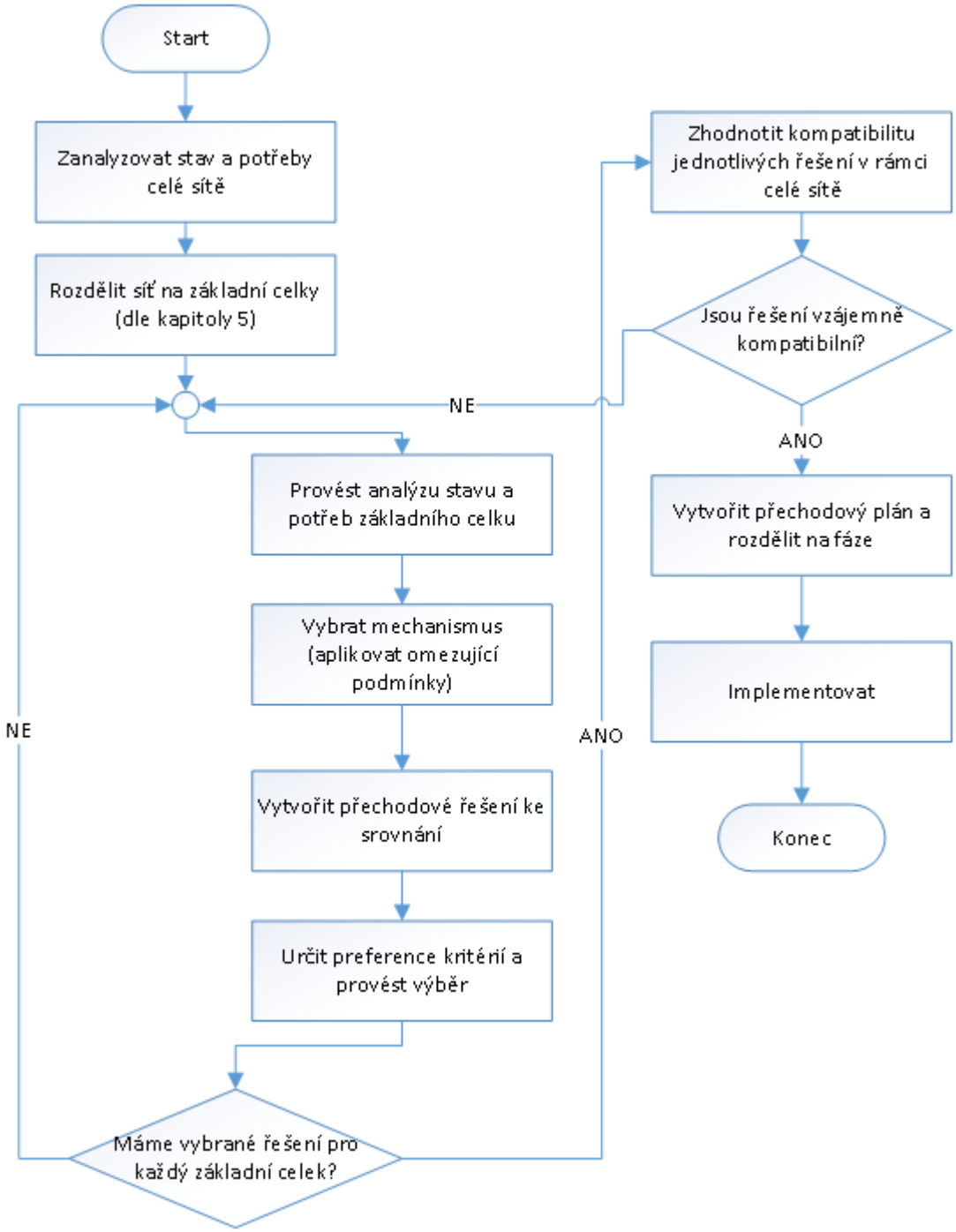
Naše metodika není jediná metoda, jak volit přechodová řešení. Nesystematická jsou doporučení pro volbu přechodových řešení pro jednotlivé typy sítě uváděná v různých normách RFC. Neexistuje ovšem jedna norma, která by podobnou metodiku navrhovala.

(2011) doporučují při tvorbě přechodových řešení následující body:

- pokud upstream neposkytuje IPv6 konektivitu, použít některý z tunelovacích mechanismů (Arkko a Baker 2011, s. 9);
- používat takové mechanismy, které nezpůsobí další navýšení ceny po ukončení přechodové fáze (Arkko a Baker 2011, s. 5);
- preferovat proxy před ALG (Application Layer Gateway) (Arkko a Baker 2011, s. 12);
- při obousměrné komunikaci dát přednost tunelům před překladem (Arkko a Baker 2011, s. 9) .

Kromě toho předkládá ke zvážení možnost inkrementálního zavedení, jednoduchost řešení, škálovatelnost, použití otevřených protokolů a implementací a zachování kompatibility s okolními sítěmi. (Arkko a Baker 2011, s. 5–6)

U nových sítí máme tu výhodu, že pořizujeme nové technické prostředky a programové vybavení. Mnoho organizací se v těchto případech kloní k IPv6-only sítím



Obrázek 5.1: Algoritmus pro obecnou metodiku přechodu na IPv6

s mechanismy pro poskytnutí kontaktu s IPv4 světem. Arkko a Baker (2011, s. 10) doporučují v těchto situacích Dual Stack Lite. Důvodem pro jeho nasazení je často velikost sítí a tedy praktická nemožnost přímého adresování uzlů. Tím se ve větších sítích komplikuje správa i adresovací schéma – je potřeba vytvářet malé subnety s překrývajícími se adresami (tento problém mají často poskytovatelé konektivity). Spravovat síť s jedním protokolem je výrazně jednodušší.

6 Případová studie: Přechod na IPv6 ve společnosti Etnetera

Etnetera je středně velká obchodní společnost, která dodává komplexní webové aplikace na zakázku. Mezi její klienty patří mj. společnosti Fortuna, O2 Czech Republic nebo Datart.

Podpora IPv6 je dnes pro poskytovatele podobných služeb důležitá. Současné problémy s nedostatkem veřejných IPv4 adres znamenají mnohdy zvýšené náklady na provoz složitých architektur a obtížné škálování technických prostředků. I z těchto důvodů nedostatek adres mnohdy brzdí růst byznysu společností jako takového.

Podpora IPv6 je také důležitá pro zakázky ze státní správy. Česká republika se účastní evropského projektu GEN6 (Governments ENabled with IPv6), jehož cílem je podpora IPv6 v eGovernmentu. Usnesení vlády ČR č. 727 z roku 2009 ukládá orgánům státní správy zajistit provoz jejich internetových aplikací i na protokolu IPv6. Tyto subjekty IPv6 v praxi skutečně poptávají.

V neposlední řadě se zvyšuje i využívání protokolu IPv6 v Internetu. K menším poskytovatelům a univerzitním sítím se v posledních dvou letech přidali i velcí poskytovatelé jako O2 a T-Mobile, kteří standardně dodávají IPv6 konektivitu v rámci klientských ADSL přípojek. Z toho vyplývá také požadavek na robustnost implementace IPv6 na straně Etnetery.

Prostředí sítě Etnenery je velmi různorodé. Kromě sítě v sídle firmy provozuje ještě sítě v několika datových centrech, kde se nachází infrastruktura pro služby, které spo-

lečnost zajišťuje pro klienty, mj. i privátní cloudové prostředí. Tyto sítě tvoří poměrně velký celek a mají rozdílné nároky na provoz. Z toho vyplynula potřeba rozdělit implementaci do několika fází. Úkolem byla pověřena autorka této práce spolu s týmem systémových administrátorů a správců sítě.

Z výše zmiňovaných důvodů vyplynulo jako nejdůležitější nasazení IPv6 na frontendových serverech a prvcích perimetru datových center, tedy tam, kam přicházejí návštěvníci. To se stalo prioritou ve fázi 1. Fáze 2 obsahuje přechod v sítích servisních, vč. firemní sítě, v rámci stěhování do nového sídla. Ve fázi 3 pak má dojít k implementaci IPv6 na uzlech uvnitř sítí v datových centrech. K datu dokončení této práce je zatím implementována pouze fáze 1.

V roce 2012 se firma rozhodla vybudovat vlastní privátní cloudové prostředí a zkonsolidovat několik zákaznických řešení do nového datového centra. Podpora IPv6 byla v návrhu tohoto DC už od počátku. Výhodou tohoto postupu bylo odstranění historické zátěže v podobě zastaralých systémů a aplikací.

Při volbě řešení bylo potřeba vzít v potaz následující podmínky.

- Všechny servery jsou pod správou Etnetery.
- Zhruba 90 % provozu zde tvoří protokoly používané pro webové aplikace (zejména HTTP a HTTPS). Zbývající provoz tvoří podpůrné služby jako DNS, SMTP, NTP aj.
- Přípojka je 1Gbps.
- Prostředí běží kompletně na GNU/Linuxu.
- Nebylo třeba řešit tunelování upstreamové IPv6 konektivity – provozovatel housingových služeb nám poskytl nativní IPv6 přípojku.
- Na služby je garantováno vysoké SLA, řešení tedy muselo mít maximální spolehlivost a stabilitu.

Po analýze požadavků a aplikaci omezujících podmínek zbyly dvě možnosti: NAT64 (příp. navíc BIH pro nekompatibilní aplikace) a Dual Stack.

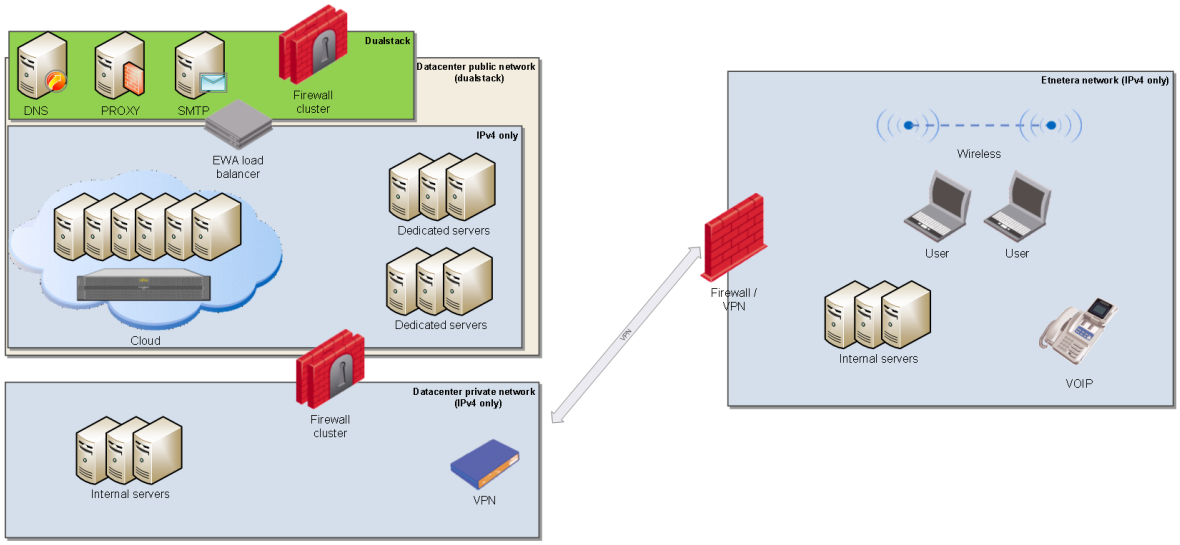
Implementace s NAT64 by vyžadovala nasazení IPv6 na všech uzlech uvnitř sítě. Mechanismus NAT64 je především určen pro komunikaci uzlů zevnitř sítě ven do Internetu. Proto by byl potřeba nákup dalšího zařízení, které by fungovalo jako NAT64 brána a provádělo DNAT, tedy statické mapování IPv4 adres na hraničních prvcích, aby se klienty z IPv4 Internetu dostaly na naše IPv6 servery. Na uzlech, kde se vyžaduje komunikace se službami třetích stran (a kde se málokdy dá předpokládat podpora IPv6), např. VPN spojení s backendovými servery klientů, by musel být použit Dual Stack. Zásadním problémem tohoto řešení bylo, že servisní sítě v té době neuměly IPv6 (s jejich přechodem se počítalo až ve fázi 2).

Proto byla zvolena varianta s čistým Dual Stackem. Toto řešení umožňuje stabilní provoz a nezpůsobuje degradaci výkonu. Na druhou stranu jsou s ním spojeny až dvojnásobné náklady na provoz. Tento problém lze ale eliminovat částečným nasazením dual stacku na hraničních prvcích sítě a na prvcích komunikujících s dalšími uzly v Internetu, např. SMTP relay servery, DNS servery (autoritativní i forwardovací), HTTP proxy, NTP atd. Servery uvnitř sítě jsou, až na výjimky, dostupné pouze na IPv4. Většina HTTP provozu prochází přes loadbalancery rozřazující klienty podle pravidel na sedmé vrstvě modelu ISO/OSI, které mají na vnějším rozhraní přiřazené IPv4 i IPv6 adresy. Komunikace s backendovými servery loadbalancované farmy probíhá pouze po IPv4.

Schéma tohoto zapojení je ve zjednodušené formě na obrázku 6.1.

Při postupu podle metodiky z kapitoly 5 se byla všechna alternativní řešení vyřazena na základě omezujících podmínek, nebylo tedy potřeba provádět vícekriteriální analýzu variant.

Uskutečnění fáze 2 předpokládáme v rámci stěhování společnosti do nového sídla na konci roku 2014. V roce 2015 bude potřeba postavit nové cloudové prostředí a zároveň vyřešit problém s nedostatkem veřejných IPv4 adres. K výběru řešení opět použijeme



Obrázek 6.1: Síť Etnetery po fázi 1 přechodu na IPv6

metodiku z kapitoly 5.

7 Závěr

Cílem práce bylo vytvořit přehled mechanismů pro přechod na IPv6, navrhnout metodiku pro výběr vhodného přechodového řešení v podmínkách konkrétní sítě a na příkladu ukázat reálné řešení této problematiky v praxi.

V kapitole 4 jsme byly popsány čtyři tunelovací mechanismy a dva překladové mechanismy, které mají oporu v normách IETF RFC a pro jejichž implementaci je dostupný sériový hardware a software. Zároveň byla provedena diskuse o možnostech nasazení těchto mechanismů. Mechanismy 6to4 a Teredo se ukázaly být v praxi jen omezeně použitelné z důvodu nízké spolehlivosti. Mechanismus 6over4 pro svoji složitost a nároky na IPv4 infrastrukturu není prakticky využíván. Naopak Dual Stack, Dual Stack Lite, NAT64 a 6rd se v komerčním světě těší poměrně velké oblibě.

V kapitole 5 bylo navrženo jednoduché členění sítí a jejich měření dle výkonových a nákladových kritérií tak, aby metodami vícekriteriální analýzy variant bylo možné vybrat vhodné přechodové řešení, tj, mechanismus nebo kombinaci mechanismů. Základním kamenem navržené metodiky je rozdělení dotyčné sítě na podsítě o úplné struktuře a výběr řešení pro každou podsíť zvlášť. Dílčí výsledky jsou spojeny do tzv. přechodového plánu, přechod je rozdělen na fáze a poté následuje samotná implementace.

Různé normy IETF RFC, např. Arkko a Baker (2011) nebo Bound (2005), nebo obsahují sadu doporučení pro nasazení IPv6 a přechodových mechanismů, systematickou metodiku pro výběr konkrétního řešení ale neposkytují. Publikace projektu 6NET (2008) (a jiných výzkumných projektů), případně knihy a články na podobné téma

(Amoss a Minoli 2008), popisují většinou konkrétní implementace IPv6 především v sítích univerzit a výzkumných institucí, nebo poskytují detailní technické postupy. Námi navrhovaná metodika oproti tomu nabízí oporu pro management přechodových projektů v sítích různých parametrů. Technické detaily implementace tato metodika neřeší. Zde ji mohou doplnit např. výše zmíněné normy a publikace.

V kapitole 6 byly představeny dosavadní výsledky projektu přechodu na protokol IPv6 na základech vlastní praxe z pohledu osoby odpovědné za tento úkol ve středně velké obchodní společnosti. Pro tento úkol byla využita obecná metodika navržená v kapitole 5. Hlavním benefitem použití metodiky v této společnosti bylo podstatné snížení množství variant pomocí omezujících podmínek. Možnost použití formalizovaného postupu, který je dílčím výsledkem naší práce, také výrazně zjednodušila řízení projektu přechodu na IPv6. V dalších fázích přechodu ve společnosti Etnetera je tato metodika rovněž aplikována.

Literatura

6NET (2008). *IPv6 Deployment Guide*. Ed. M. Dunmore. Javvin. ISBN: 16-026-7005-6.

Aben, Emile (2014). *6to4 - How Bad is it Really?* RIPE Labs. URL: `https://labs.ripe.net/Members/emileaben/6to4-how-bad-is-it-really` (cit. 15. 07. 2014).

Amoss, John a Daniel Minoli (2008). *Handbook of IPv4 to IPv6 transition*. Boca Raton: Auerbach Publications.

Aoun, C. a E. Davies (2007). *Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status*. RFC4966. URL: `http://tools.ietf.org/rfc/rfc4966.txt`.

Arkko, J. a F. Baker (2011). *Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment*. RFC6180. URL: `http://tools.ietf.org/rfc/rfc6180.txt`.

Bagnulo, M., P. Matthews a I. van Beijnum (2011). *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*. RFC6146. URL: `http://tools.ietf.org/rfc/rfc6146.txt`.

Bagnulo, M., A. Sullivan et al. (2011). *DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*. RFC6147. URL: `http://tools.ietf.org/rfc/rfc6147.txt`.

Bound, J. (2005). *IPv6 Enterprise Network Scenarios*. RFC4057. URL: `http://tools.ietf.org/rfc/rfc4057.txt`.

Carpenter, B. a C. Jung (1999). *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*. RFC2529. URL: `http://tools.ietf.org/rfc/rfc2529.txt`.

Carpenter, B. a K. Moore (2001). *Connection of IPv6 Domains via IPv4 Clouds*. RFC3056. URL: http://tools.ietf.org/rfc/rfc3056.txt.

Durand, A. et al. (2011). *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*. RFC6333. URL: http://tools.ietf.org/rfc/rfc6333.txt.

Huang, B., H. Deng a T. Savolainen (2012). *Dual-Stack Hosts Using "Bump-in-the-Host"(BIH)*. RFC6535. URL: http://tools.ietf.org/rfc/rfc6535.txt.

Huitema, C. (2001). *An Anycast Prefix for 6to4 Relay Routers*. RFC3068. URL: http://tools.ietf.org/rfc/rfc3068.txt.

Huston, G. (2008). *6to4 Reverse DNS Delegation Specification*. RFC5158. URL: http://tools.ietf.org/rfc/rfc5158.txt.

Huston, Geoff (2014). *The ISP Column. An occasional column on things Internet*. URL: http://www.potaroo.net/ispcol/2011-04/teredo.html (cit. 14. 07. 2014).

IPv6 Ready Logo Program Frequently Asked Questions (2014). IPv6 Forum. URL: https://www.ipv6ready.org/?page=faq (cit. 15. 10. 2014).

Kozierok, Charles M. (2005). *The TCP/IP guide. a comprehensive, illustrated Internet protocols reference*. San Francisco: No Starch Press. ISBN: 15-932-7047-X.

Nordmark, E. a R. Gilligan (2005). *Basic Transition Mechanisms for IPv6 Hosts and Routers*. RFC4213. URL: http://tools.ietf.org/rfc/rfc4213.txt.

Operating system market share (2014). NETMARKETSHARE: Market Share Statistics for Internet Technologies. URL: http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8%5C&qpcustomd=0 (cit. 15. 10. 2014).

Satrapa, Pavel (2011). *IPv6. internetový protokol IPv6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC. ISBN: 978-80-904248-0-7.

SixXS - IPv6 Deployment & Tunnel Broker (2013). *AICCU - Automatic IPv6 Connectivity Client Utility*. SixXS. URL: http://www.sixxs.net/tools/aiccu/ (cit. 02. 03. 2013).

Templin, F., T. Gleeson a D. Thaler (2008). *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*. RFC5214. URL: http://tools.ietf.org/rfc/rfc5214.txt.

Top 8 Operating Systems (2014). StatCounter GlobalStats. URL: http://gs.statcounter.com/#all-os-ww-monthly-201310-201409-bar (cit. 15. 10. 2014).

Townsley, W. a O. Troan (2010). *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification.* RFC5969. URL: http://tools.ietf.org/rfc/rfc5969.txt.

Troan, O. (2011). *Request to move Connection of IPv6 Domains via IPv4 Clouds (6to4) to Historic status.* Work In Progress. URL: http://tools.ietf.org/html/draft-ietf-v6ops-6to4-to-historic-05.

Seznam obrázků