Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

IPv6 aspekty migrace firemního prostředí

Jiří Krula

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Krula Jiří

Informatika

Název práce

IPv6 aspekty migrace firemního prostředí

Anglický název

Migration of corporate IT infrastructure to IPv6

Cíle práce

Bakalářská práce je zaměřena na problematiku protokolu IPv6 a aspektů migrace provozu firemního prostředí do tohoto síťového protokolu. Hlavním cílem práce je charakterizovat technické a bezpečnostní aspekty migrace firemního prostředí do protokolu IPv6. Dílčí cíle bakalářské práce jsou:

- analyzovat důvody a přínosy migrace firemního prostředí do IPv6;
- analyzovat požadavky na architekturu infrastruktury firemního prostředí z pohledu IPv6;
- navrhnout a implementovat řešení migrace firemního prostředí do IPv6.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Vlastní řešení je realizováno formou návrhu a implementace migrace vybrané firemní infrastruktury do IPV6. Na základě syntézy teoretických poznatků a výsledků vlastního řešení budou formulovány závěry bakalářské práce.

Harmonogram zpracování

1) Příprava a studium odborných informačních zdrojů, upřesnění dílčích cílů práce a volba postupu řešení: 06/2013
2) Zpracování přehledu řešené problematiky dle informačních zdrojů: 7/2013 - 9/2013
3) Vypracování vlastního řešení, diskuze a zhodnocení výsledků: 10/2013 -11/2013
4) Tvorba finálního dokumentu bakalářské práce: 12/2013 - 2/2014
5) Odevzdání bakalářské práce a teze: 3/2014

Rozsah textové části
30 - 40 stran

Klíčová slova
Internet Protocol version 6 (IPv6), TCP Transmission Control Protocol, TCP/IP Transmission Control Protocol/Internet Protocol, Internet

Doporučené zdroje informací

1) Satrapa, Pavel: Internetový protokol IPv6: CZ.NIC, z. s. p. o, 2008, 359 s, ISBN 978-80-904248-0-7
2) Blanchet, Marc: Migrating to IPv6 a practical guide to implementing IPv6 in mobile and fixed networks: John Wiley & Sons Ltd, 2005, 454 s, ISBN 0-471-49892-0
3) Ciprian P. Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete: Deploying IPv6 Networks: Cisco Press, 2006, 672 s. ISBN 978-1587052101
4) Silvia Hagen, IPv6 Essentials: O'Reilly Media, 2006, 438 s, ISBN 978-0596100582

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(a) 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(ka) uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil(a) autorská práva třetích osob.

V Praze dne 13. 03. 2014 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Alexandru Vasilenkovi za odborné vedení, za pomoc a rady při zpracování této práce.

IPv6 aspekty migrace firemního prostředí

Migration of corporate IT infrastrukture to IPv6

Souhrn

Práce se zabývá protokolem IPv6 a aspekty migrace firemního prostředí na tento protokol. Cílem práce je analyzovat problematiku protokolu IPv6 a aspektů migrace firemního prostředí k využití tohoto síťového protokolu, a v tomto rámci charakterizovat technické a projektové aspekty migrace.

Na základě těchto poznatků je navrženo a implementováno vzorové řešení migrace firemního prostředí do IPv6.

Summary

This work is focused on IPv6 protocol and aspects of corporate environment migration on this protocol.

The aim of this work is to analyze the issues of IPv6 protocol and the aspects of corporate environment migration to apply this network protocol, and then to characterize the technical and design aspects of migration within this framework.

Finally a model solution of corporate environment migration to IPv6 is designed and implemented based on these findings.

Klíčová slova: Internet protokol version 6 (IPv6), adresace, formát datagramu, autokonfigurace, DHCPv6, IPsec, přechodové metody, Dual stack, IPv6 over MPLS, ITIL

Keywords: Internet protokol version 6 (IPv6), addressing, header format, autoconfiguration, DHCPv6, IPsec, transition methods, Dual stack, IPv6 over MPLS, ITIL

Obsah

1 Úvod

Současná verze síťového protokolu, jenž se stal nosným protokolem pro každou síťovou infrastrukturu a zejména světovou komunikační síť Internet, Internet Protokol verze 4 (IPv4), byla vyvinuta již v průběhu sedmdesátých let.

Koncem šedesátých let vznikla velká poptávka v řadách amerických universit a výzkumných center po síti, která by umožnila celonárodní využití počítačových zdrojů a výměny dat. Na druhé straně zde existoval výzkum první praktické zkušenosti s návrhem, implementací a využíváním síťových technologií. Na základě této poptávky americká vládní organizace Advanced Research Project Agency (ARPA) zahájila budování sítě s názvem ARPANET, která dala v budoucnu vzniknout jak celosvětové síti Internet, tak jeho nosnému protokolu IPv4. Společně s bouřlivým rozvojem počtu uživatelů sítě Internet se již brzy objevil problém s blížícím se vyčerpáním adresního prostoru. Proto již v počátku devadesátých let byly zahájeny práce na novém síťovém protokolu budoucnosti, který by tento, a nejen tento, zásadní problém řešil.

Po více jak dvaceti letech od zahájení vývoje Internet protokolu verze 6 (IPv6) je dnes, vzhledem k realitě absence volných adresních prostorů a trvalému růstu připojených subjektů pro firmy důležité začít uvažovat o tom, zda zahájit přechod k novému protokolu a jakým způsobem tento přechod realizovat.

2 Cíl práce a metodika

Cílem práce je analyzovat problematiku protokolu IPv6 a aspektů migrace firemního prostředí k využití tohoto síťového protokolu, v tomto rámci charakterizovat technické a projektové aspekty migrace. Dílčím cílem bakalářské práce je analyzovat a definovat možné důvody a přínosy migrace firemního prostředí do IPv6. Na základě těchto poznatků následně navrhnout a implementovat řešení migrace firemního prostředí do IPv6. Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů.

V první části je všeobecně nastíněna problematika protokolu IPv6 a jeho hlavní technické funkcionality. V následujících částech jsou analyzovány a popsány možné důvody k přechodu a dále procesní, projektové a technické aspekty migrace.

V poslední části, je na základě zjištěných informací navrženo vlastní řešení, realizované formou návrhu a implementace migrace vybrané firemní infrastruktury k IPV6.

Na základě syntézy teoretických poznatků a výsledků vlastního řešení budou formulovány závěry bakalářské práce.

3 Přehled řešené problematiky

3.1 Historie IPv6

Vznik protokolu IPv6 sahá do roku 1992, kdy již bylo zřejmé, že stávající kapacita adresního rozsahu protokolu IPv4, bude vzhledem k rozrůstajícímu se Internetu dříve nebo později vyčerpána. IETF proto vyhlásila prostřednictvím RFC 1550 výzvu pro podávání návrhu Internetového protokolu nové generace (pracovně pojmenovaného IPng). Snaha vyústila koncem roku 1995 ve vydání RFC 1883: Internet Protocol, Version 6 (IPv6) Specification. Cílem tvůrců nebylo řešit pouze problém nedostatečného adresového prostoru, ale současně také vyřešit tehdy známé nejpalčivější problémy protokolu IPv4 [1; 2; 3].

Vývoj pokračoval po celá devadesátá léta a roku 1998 vyšla revidovaná sada RFC dokumentů s definicí základních protokolů a služeb, dále byly dokumenty aktualizovány a doplňovány. Poslední verze adresní architektury pochází z roku 2006. Internet protokol verze 6 přináší řadu nových vlastností, které mění dosavadní zvyklosti z užití IPv4. Tyto vlastnosti vycházejí ze zadání při zahájení návrhu a dále si je podrobněji přiblížíme [1; 3; 4].

3.2 Adresní prostor a adresace

Adresa IPv6 má délku 128 bitů, vzhledem k délce jsou zapisovány rozdílně od adres IPv4. Každé čtyři bity jsou prezentovány hexadecimálním číslem, adresa se tak skládá z 32 hexadecimálních znaků rozdělených do skupin po čtyřech [1]. Příklad plné adresy: ***2001:0b80:0000:0000:dead:face:0591:6804***

Jelikož je poněkud nepraktické vypisovat řadu nul, je ustanovena konvence, že lze vynechat každou první nulu v bloku znaků. Po úpravě pak lze předchozí adresu zapsat jako: ***2001:b80:0:0:dead:face:591:6804***

Dále jednu, a pouze jednu sérii nul a dvojteček lze nahradit sérií dvou dvojteček. Tedy předchozí adresu můžeme dále upravit, a jako výsledek v praxi používat: ***2001:b80::dead:face:591:6804***

Přesná pravidla pro notaci adres IPv6 jsou specifikována v RFC 5952. Adresa se dále rozděluje na adresu sítě a adresu uzlu. Identifikace adresy sítě probíhá na základě prefixu obdobně jako u IPv4 [1]. Tedy adresa sítě zapsaná ***2001:b80::/64*** určuje, že prvních 64 bitů je adresa sítě. Zápis identifikující jak adresu rozhraní, tak adresu podsítě je ***2001:b80::dead:face:591:6804/64***

Ze zápisu lze tak přehledně vyčíst jak adresu sítě, tak adresu uzlu. Pod pojmem uzel rozumíme síťové rozhraní zařízení. Každé síťové rozhraní - uzel, může mít několik různých adres. V protokolu IPv6 existují tři druhy adres, a to:

- Individuální *(unicas*t) adresa identifikuje právě jeden uzel.
- Skupinová (*multicast*) adresa identifikující skupinu uzlů kterým má být doručen datagram odesílatele. Touto skupinou lze částečně nahradit i všesměrové vysílání (*broadcast*) z IPv4, které bylo v nové verzi zrušeno.
- Výběrová (*anycast*) adresa identifikující skupinu uzlů, avšak datagram bude doručen pouze k nejbližšímu uzlu skupiny.

Individuální adresy unikátně identifikují uzel a lze je dále rozdělit na [2]:

- Individuální globální adresy (*global unicast*) – tj. veřejné adresy uzlu v IPv6 internetu. Organizace Internet Corporation for Assigned Names and Numbers (*ICANN*) prostřednictvím pěti regionálních registrátorů (pro oblast Evropy je odpovědná organizace RIPE NCC) alokuje adresní bloky.
- Lokální linkové adresy (*link-local*) – tj. adresy unikátní pouze na jedné lokální lince (např. jednom ethernetu, wi-fi buňce), tyto adresy může zařízení generovat samo.
- Smyčka (*loopback*) – je adresa nepřidělená fyzickému rozhraní a která umožňje odesílání paketů sama na sebe.
- Nedefinované adresy (*unspecified address*) – jedná se o v současnosti nepřiřazené adresy z rozsahu *::/8*.
- Unikátní individuální lokální adresy (*unique local*) – tedy adresy s omezeným rozsahem, kterým není dovoleno routování do IPv6 internetu, jsou obdobné k privátním adresám v IPv4. Každopádně je u nich velmi vysoká pravděpodobnost, přibližně 10^{-12}, že jsou globálně jedinečné. Toho se využívá v rozlehlých sítích se vzdálenými lokalitami.

Skupinové (Multicast) adresy se povětšinou užívají k distribuci dat v reálném čase, jako zejména videa a zvuku (videokonference, televizní vysílání), nebo síťových služeb určených pro celou skupinu uzlů, jako například časové služby NTP. Existují i další metody tvorby skupinových adres, například identifikátoru rozhraní adresy pro SSM (Source Specific Multicást) pro přenos internetových rádií a televize.

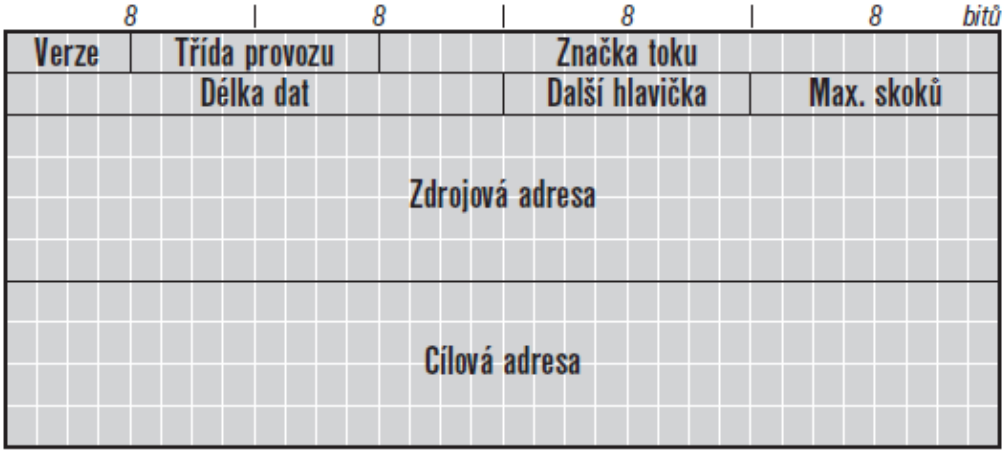
Výběrová adresa je adresa přiřazená více rozhraním. Pro výběr cíle zaslaného packetu na tuto adresu, je sítí vybrán nejbližší cíl dle routovacích tabulek. Tuto funkcionalitu lze

v praxi využít pro služby jako DNS nebo http a tak zajistit, že uživatel přistoupí k těmto službám pro něj nejkratší cestou [4].

3.3 Datagram

Datagram je v IP protokolech datový packet, blok dat, přenášející informaci v datové síti. Zpravidla začíná hlavičkami, následovanými pak nesenými daty. Na rozdíl od předchozí verze došlo k několika koncepčním změnám. Asi nejzásadnější je změna formátu a minimalizace standardní hlavičky [1]. Tím nutně došlo k omezení prvků hlavičky oproti předchozí verzi protokolu. Základní hlavička je 40B dlouhá, ostatní doplňující údaje jsou přesunuty do rozšiřujících hlaviček. Základní prvky hlavičky jsou [1; 5]:

- Verze (*Version*) – čtyřbitová hodnota, která identifikuje verzi protokolu. V případě IPv6 obsahuje hodnotu 6.
- Třída provozu (Traffic class) – osmibitové číslo, jenž vyjadřuje prioritu datagramu a



Obrázek 1: Základní hlavička datagramu [1]

jeho zařazení. Toto umožňuje směrovačům identifikovat datagramy, různě s nimi zacházet a řídit tok paketů s ohledem k jejich zařazení a prioritě.

- Značka toku (*Flow label*) – dvacetibitové číslo, v současnosti experimentální funkcionalita. Mělo by označovat tok paketů s určitými společnými vlastnostmi. Tedy směrovač jednoduše identifikuje pakety patřící do stejného toku a bude s nimi zacházet stejně.
- Délka dat (*Payload lenght*) - šestnáctibitové číslo reprezentující délku přenášených dat bez základní hlavičky, avšak s rozšiřujícími hlavičkami. Maximální délka je tedy 64KB, v případě potřeby většího datagramu se použije rozšiřující hlavička nazývaná jumbo.
- Další hlavička (*Next header*) – osmibitový identifikátor hlavičky následující za standardní hlavičkou, případně informací o typu dat nesených datagramem.
- Max. skoků (*Hop limit*) – osmibitové číslo, které je dekrementováno při každém průchodu směrovačem (uzlem) v síti. Dojde-li k vynulování po cestě paketu, odesílatel obdrží ICMP zprávu o vypršení maximálního počtu skoků.
- Zdrojová a cílová adresa (*Source / Destination address*) – stodvacetibitové adresy odesílatele a příjemce paketu.

Pro prezentaci rozšiřujících hlaviček protokol IPv6 používá postup řetězení (pořadí hlaviček je však v IPv6 předepsáno), kdy je každá hlavička samostatným blokem bitů, přičemž první bajt identifikuje položkou Další hlavička (Next header), tedy určuje jakého typu je hlavička následující za hlavičkou aktuální. Poslední hlavička z řetězce zde nese informaci o typu dat nesených datagramem. [1]

3.4 Zajištěná kvalita (QoS)

Zajištěná kvalita (QoS) je realizována pomocí již výše zmíněných polí v záhlaví, Třída provozu (Traffic Class Field) a Označení datového toku (Flow Label Field). Tak je umožněno identifikovat tok dat a tím umožnit směrovačům přistupovat k paketům tak, jak si vyžádal zdrojový uzel, případně jak je s daným typem dat v infrastruktuře pracováno. [5]

3.5 Bezpečnost

Velkou změnou IPv6 je řešení bezpečnosti na úrovni IP vrstvy. Tu zajišťuje IPsec, který je sice využitelný již u IPv4, ale pro IPv6 se jeho implementace stala povinnou.
Implementace je realizována pomocí dvou rozšiřujících bezpečnostních hlaviček:

- AH *(Authentication Header*) – ta zajišťuje autentizaci datagramu zejména ověření pravosti adres (totožnosti odesílatele) a obsahu paketu.
- ESP *(Encapsulating Security Payload)* – pak zajistí služby ekvivalentní funkci hlavičky AH a navíc přidá možnost zašifrovat obsah paketu.

Implementace hlavičky ESP je dle RFC 4301 v současnosti povinné, AH je dobrovolná a postupně se od ní upouští. Bezpečnostní hlavičky se doplňují ve dvou režimech, transportním (jako rozšiřující hlavička) a tunelujícím (stávající datagram se celý zabalí do nového) a tedy původní datagram je kompletně ochráněn [1; 5].

V IPsec vzniká virtuální spojení dvou uzlů, nazývané bezpečnostní asociace, jehož součástí jsou všechny informace pro toto spojení (bezpečnostní protokol, jeho režim, šifrovací algoritmus, platné klíče pro spojení a další), a to jednosměrně. Pro komunikaci je vždy samostatně ustaveno vysílání a příjem. Pro koordinaci obou komunikujících stran musí

dojít k dohodě o parametrech spojení, tedy kryptografických algoritmech, jejich parametrech a klíčích. K tomuto je využito protokolu IKEv2. Komunikace protokolu IKEv2 probíhá ve výměnách (exchange), skládajících se ze dvou zpráv (požadavek a odpověď). Protokol IKEv2 definuje čtyři výměny, dvě při zahájení, jednu pro správu bezpečnostních asociací a jednu pro vzájemnou výměnu informací. [1]

3.6 Podpora mobilních zařízení

Současný trend růstu počtu mobilních zařízení je jedním z pádných argumentů pro adopci IPv6. Požadavek na mobilitu v IPv6 byl již při počátečním zadání vlastnosti protokolu, a i přes pomalý postup při definici a implementaci této funkcionality bude jedním z klíčových faktorů při globálním přechodu k IPv6.

Podpora mobility je postavena na premise, že pro každé mobilní zařízení lze identifikovat jeho přirozený domov, tedy domácí síť, kde má registrovánu svou globální individuální adresu. Tato domácí adresa je konstantní a rozhraní je pod ní zavedeno v DNS a globálně dostupné. Pokud se stane zařízení mobilní a opustí svojí domácí síť, dostane dočasné adresy. V domácí síti si současně ustanoví domácího agenta (home agent), jenž přijímá datagramy směřující k mobilnímu uzlu a předává mu je tunelem. Tento stav je například vhodný pro případ, kdy chceme na komunikaci mobilního zařízení aplikovat firemní politiku a kontrolovat datový tok mobilního zařízení. Má to nevýhodu v zatížení domácí sítě, přes kterou probíhá dvojí komunikace (k domácímu agentu a k mobilnímu zařízení), proto dále existuje možnost optimalizace cesty, kdy cílový uzel při příchodu prvního datagramu od domácího agenta informuje korespondenta o své dočasné adrese a nadále komunikuje napřímo. Domácí adresa je vždy k dispozici a mobilní zařízení se na ni vždy může odkázat.

3.7 Autokonfigurace

V IPv6 rozlišujeme dvě základní podoby autokonfigurace, a to konfiguraci stavovou a bezstavovou.

Základem stavové konfigurace je centralizovaný server spravující konfigurační parametry, které následně na vyžádání poskytuje jednotlivým uzlům. K tomuto úkolu byl v IPv6 navržen protokol DHCPv6. Pro identifikaci klientů pro potřeby DHCP je ve verzi DHCPv6 zaveden pojem DHCP Uniqe Identifier (DUID). Ten je možné tvořit několika způsoby, jednak pomocí jednoznačné identifikace od výrobce (sériové číslo), dále doménou výrobce a zařízení si je nese po celou svoji životnost (za předpokladu, že zařízení disponuje pamětí s možným zápisem), nebo pomocí samotné linkové adresy případně kombinované s časem vytvoření. Pro identifikaci rozhraní zařízení se používá identifikační asociace (IA), což je souhrn konfiguračních informací pro rozhraní s jednoznačným identifikátorem (IAID). Získání síťových parametrů v DHCPv6, obdobně jako u verze DHCP pro IPv4, má čtyři fáze [1]:

1. Objevování - kdy klient vytvoří IA pro všechna svá rozhraní a na skupinovou adresu všech agentů a serverů zašle výzvu spolu se svou DUID a IA pro všechna rozhraní. Součástí výzvy je i jeho lokální linková adresa. V případě, že na lince je přímo server, odpoví po linkové adrese. Pokud je na lince jen agent, drží seznam všech serverů v síti (seznam může obsahovat skupinovou adresu DHCP serverů) a na ně předá požadavek, ten pak předá na linkovou adresu serverů, v tento okamžik zařízení nezná, obesílá s dotazy standardní skupinové adresy. Pro DHCPv6 jsou definovány dvě standardní skupinové adresy pro všechny:

- DHCP agenty a servery *ff02::1:2*
- DHCP servery *ff05::1:3*

2. Nabídka - odpovědí je v případě serveru ohlášení (advertist). To se skládá z preference, která oznamuje ochotu serveru poskytnout službu klientu a současně konfigurační parametry, které by přidělil jednotlivým IA. V případě zprostředkovatele tento předá požadavek na seznam jemu známých serverů, formou zprávy typu předání (relay forward) a nazpět obdrží zprávu odpověď k předání (relay reply). Zprostředkovatel tuto zprávu předá po linkové adrese klienta.
3. Žádost - klient z obdržených nabídek vybere poskytovatele z nejvyšší preferencí a odešle novou žádost, ve které uvede DUID cílového serveru. Tato zpráva je opět odeslána na skupinovou adresu. Servery, kterým není určena, ji ignorují a zaobírá se jí pouze server se správným DUID.
4. Obdržení - cílový server požadavek vyhodnotí a odpoví. Při přidělení adres je zohledněna linka, ze které je klient připojen, a DUIS klienta.

Adresy jsou obdobně, jako u původní verze, přidělovány na určitou dobu. V okamžiku uplynutí zapůjčení adresy musí klient požádat o její prodloužení. Požádá tedy server, který mu ji zapůjčil zprávou obnovení (renew). Pokud neobdrží odpověď, zeptá se ostatních serverů. V okamžiku ukončení činnosti by měl klient adresu uvolnit zprávou uvolnění (release), ta následně může být poskytnuta dalšímu zájemci.

Výše popsané činnosti jsou vyvolány ze strany klienta, protokol ovšem myslí i na situace kdy dojde ke změnám na straně serveru a tento potřebuje zajistit, aby se jím registrovaní

klienti se přizpůsobili nové situaci. V takovém případě server zašle zprávu rekonfigurace (reconfigure) svým klientům a klienti reagují zprávou obnovení.
Bezstavová konfigurace spočívá v automatickém určení vlastní adresy a vychází z předpokladu, že v každé síti lze najít směrovač, který v pravidelných intervalech rozesílá Ohlášení směrovače do všech sítí, k nimž je připojen. [1]

3.8 Domain Name System

Domain Name System (DNS) slouží k zjištění internet adresy pro známý symbolický název jmena zařízení (počítače, serveru atd.) a naopak umožňuje zjistit symbolický název ze známé adresy.

Kromě ukládání informací IPv6 je nově řešen i přenos protokolem IPv6 mezi autoritativními servery a dále v hierarchické struktuře. K lednu 2014 má již 100% autoritativních serverů pro doménu *.cz* registrovánu svou AAAA adresu. [1]

3.8.1 Dopředné dotazy

Zjištění adresy k danému jménu je realizováno pomocí dopředných dotazů. Pro IPv6 se zavádí, obdoba A záznamu u IPv4, nový záznam AAAA. Mnemotechnicky IPv6 má čtyřnásobnou délku oproti IPv6, tedy AAAA záznam oproti původnímu A záznamu.

Pokud tedy má zařízení vpn.example.org adresu 2001:b80::dead:face:591:6804, bude v zónovém souboru, který obsahuje definice dané domény, existovat záznam

vpn.example.org AAAA 2001:b80::dead:face:591:6804

V případě, že se dotazujeme na nějakou specifickou službu, jako například MX záznam pro danou doménu, můžeme v zónovém souboru nalézt, v „IPv4/v6 dual stack“ infrastruktuře, obdobný záznam[5]:

```
example.org.          IN MX   1  mx1.example.org.
                      IN MX   10 mx10.example.org.

vpn.example.org       IN AAAA 2001:b80::dead:face:591:6804
mx1.example.org.      IN A    1.0.0.1; IPv4/v6 dual stack
                      IN AAAA 3ffe:501:ffff::1
mx10.example.org.     IN AAAA 3ffe:501:ffff::2 ;  pouze IPv6
```

Záznam definuje dvě zařízení mx1 (dual stack, tedy přístupné jak po IPv4, tak IPv6) a mx10 (přístupné pouze pomocí IPv6), k těmto zařízením je přiřazen MX záznam s různou vahou a tedy jsou určené pro příjem pošty v dané doméně.
V současnosti nejvíce rozšířené DNS servery (např. BIND a KNOT DNS) jsou pro poskytování služeb v infrastruktuře IPv6 již připraveny.

3.8.2 Zpětné dotazy

Zpětný dotaz ze známé IP adresy vrací její doménové jméno. Stejně jako u IPv4 je k tomuto účelu použit záznam PTR. Takový dotaz je položen pomocí doménového jména sestaveného obrácením pořadí šestnáctkových číslic adresy a na konec je připojena doména ip6.arpa. Pro výše zmíněný případ zařízení se jménem vpn bude záznam vypadat následovně

4.0.8.6.1.9.5.0.e.c.a.f.d.a.e.d.0.0.0.0.0.0.0.0.8.b.0.1.0.0.2.ip6.arpa. PTR vpn.example.org

Pro PTR záznamy nelze vzhledem k formátu vynechat žádnou nulu ze zápisu, tento stav má nepříjemný dopad na značnou náročnost zápisu a snadné zanesení chyby při změně.

3.8.3 Adresy v DNS

Jak je již uvedeno v předcházejících kapitolách, rozhraní zařízení je v IPv6 identifikováno řadou adres, z nichž každá má jinou důležitost, význam a i životnost. Z tohoto důvodu je vhodné správně zvolit adresy, které budou prezentovány v DNS. Vhodně zvolené a pojmenované adresy umožní i ve velmi rozsáhlé podnikové síti zajistit konzistentní informace v DNS a tím mitigovat provozní a bezpečnostní rizika. Do DNS je vhodné zařadit veškeré globální individuální adresy a adresy přechodových mechanizmů [1].

Do DNS není vhodné zařazovat lokální linkové adresy a náhodně generované krátkodobé adresy (realizované za účelem krátkodobého spojení v rámci jedné relace např. mobilní). Zda zařadit adresy například realizované bezstavovou automatickou konfigurací, případně pomocí DHCPv6, záleží obvykle na politice dané společnosti, definované v lokální bezpečnostní politice. [1]

3.9 Integrační a přechodové technologie

I když v současné době IPv4 v některých oblastech nezvládá pokrývat narůstající adresní požadavky podnikových sítí a IPv6 je schopno tento stav řešit, je nicméně problematické

implementovat IPv6 do podnikové sítě. Tento stav je nutno řešit efektivně a s maximální mitigací rizik takovéto změny. Proto vznikly různé mechanizmy pro dosažení efektivního a bezpečného nasazení IPv6 do síťové infrastruktury. Tyto mechanizmy lze rozdělit [2]:

3.9.1 Nativní IPv6

V případě takovýchto sítí je IPv6 jediným protokolem v síti. Sítě lze nasadit nejčastěji v případech zcela nových sítí, kde je možné v maximální míře využít vlastností IPv6 bez potřeby řešit koexistenci s IPv4. Těchto sítí je v praxi naprosté minimum a v případě podnikových sítí lze o této variantě uvažovat obvykle v případě výstavby nové sítě [2].

3.9.2 IPv4/v6 dual stack

Dual Stack označuje síť, kde jsou současně provozována IPv4 a IPv6 zařízení. Jedná se o preferovaný mechanizmus při přechodu na IPv6, pokud existuje stálá potřeba přístupu i pomocí starého protokolu. V takovém prostředí jsou IPv6 a IPv4 provozována na všech klíčových síťových prvcích a některých koncových zařízeních zapojených v síti. V minulosti byl stejný mechanizmus využit při provozování IPv4 s některými proprietárními protokoly, jako například IPX/SPX (Novell/Xerox) nebo AppleTalk, kde tak byla zajištěna koexistence obou nekompatibilních protokolů [2].

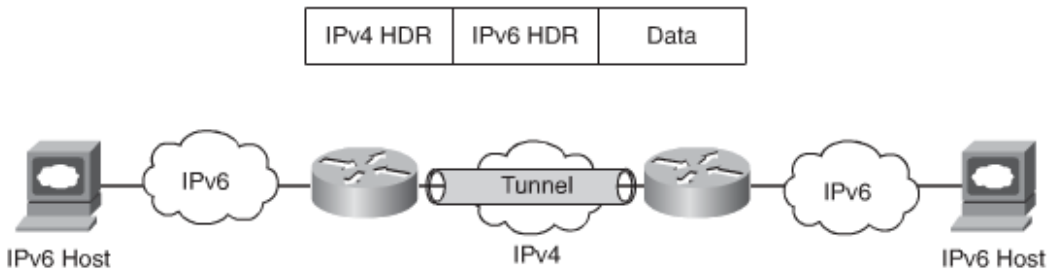
Dual stack představuje základní a nejhladší možnost přechodu mezi IPv4 a IPv6 v infrastruktuře sítě. Umožňuje postupnou migraci při současném zajištění všech klíčových funkcionalit poskytovaných uživatelům, potažmo obchodním zájmům společnosti, při možnosti využití všech klíčových vlastností nového protokolu. [2]

V zásadě tento model spočívá v nastavení IPv6 v již existující síti postavené na IPv4 protokolu. Klíčovou výhodou tohoto mechanizmu je absence nutnosti jakéhokoliv tunelování v síti. Oba protokoly jsou na sobě naprosto nezávislé a protokol, který bude pro komunikaci zvolen, závisí na dohodě klienta a serveru, přičemž v případě možnosti použití obou je obvykle přednostně vybrán protokol IPv6.

3.9.3 IPv6 over IPv4

Jelikož je IPv4 stále dominantní protokol ve firemních sítích i při vzrůstajícím nasazení IPv6 sítí, buď jako nativní či dual stack, přichází s tímto růstem nasazení nutnost zajistit současně end-to-end konektivitu IPv6 klientů, či celých sítí. Častým problémem v tomto okamžiku je síť v cestě, postavená na protokolu IPv4, kterou nelze rozšířit o IPv6. Příkladem takového stavu je připojení pobočky k firemní síti, kdy obě mají již nasazen protokol IPv6, ale WAN síť je stále postavena na IPv4 protokolu. [2]

IPv6 over IPv4 je přechodový mechanizmus, kdy datagram IPv6 je zapouzdřen (encapsulation) do datagramu protokolu IPv4, a pomocí protokolu IPv4 přenesen skrze jeho síť na cílové zařízení (do cílové sítě), kde je opětovně rozbalen. Obrázek 6 zobrazuje základní Framework pro zapouzdření IPv6 do IPv4. [2]



Obrázek 2: Tunel IPv6 skrze IPv4 [2]

Existující varianty možných typů takto vytvořených tunelů [2]:

- „Router-to-router“ – v tomto případě jsou dva hraniční routery IPv6 sítí propojeny tunelem vystaveným v IPv4 síti kterým je IPv6.
- „Host-to-router“ – v tomto případě dual stack host navazuje tunel s hraničním routrem, kde je ukončen a data dále pokračují do cílové IPv6 sítě.
- „Host-to-host“, v tomto scénáři komunikují dva hosté přímo svázaným IPv6overIPv4 tunelem. Tento scénář není ve firemním nasazení příliš častý.

3.9.4 IPv6 over MPLS

Jedná se o přechodový mechanizmus, kdy je IPv6 doména spojena dalšími doménami IPv6 pomocí MPLS (*MultiProtocol Label Switching*) mechanizmu. Jde o vhodné řešení v případě, kdy obvykle poskytovatel služeb nebo větší firma s několika pobočkami přechází k IPv6 a má mezi lokalitami vybudovánu IPv4 MPLS infrastrukturu (někdy taktéž označovanou jako MPLS VPN). [2]

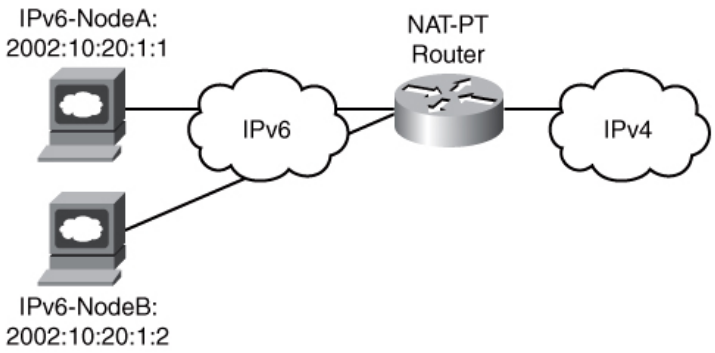
V tomto scénáři koncové routery (*PE routery*) mají schopnost routovat IPv6 protokol, ovšem routery providera (P) ji nemají. MPLS lze zjednodušeně popsat jako vkládání hlaviček před pakety, přesněji za hlavičku rámce linkové (L2) vrstvy. Tyto hlavičky mohou obsahovat jedno či více tzv. "Labels" – návěstí. Takto značené pakety jsou dále přepojovány pomocí tohoto návěstí a nikoliv dle IP tabulek. Vstupním a výstupním bodem MPLS sítě jsou hraniční směrovače (PE), jež zajišťují vložení či odebrání MPLS návěstí z paketů. Směrovače (P) pouze přeposílají (přepínají - switching) pakety dále v síti providera. Jelikož přepínání je realizováno na L2 vrstvě, je přenos plně transparentní pro IPv6 a není třeba na PE a P routrech realizovat žádnou změnu datagramu. To umožňuje

poskytovat IPv6 konektivitu (mezi IPv6 doménami) bez nutnosti povýšení operátorovi infrastruktury [2].

3.9.5 NAT-PT

Mechanizmus NAT-PT provádí překlad na L3 vrstvě mezi IPv4 a IPv6. Využívá se v případě, kdy zařízení nativní IPv6 sítě komunikuje s hostem v nativní IPv4 síti. Mechanizmus je v části obdobný s klasickým NAT mechanizmem u IPv4 sítí. Překlad pomocí NAT-PT využívá pool IPv4 adres a přiřazuje je IPv6 koncovým zařízením na hranici mezi IPv4 a IPv6. Mechanizmus je založen na bezstavovém IP/ICMP (SIIT) algoritmu, jež doplňuje o mechanismus pro mapování a překlad adres. Obvykle je postaven na jednom IPv6 prefixu (nejčastěji délky 96 bitů), do nějž mapuje IPv4 adresy tak, že je připojí na konec. Směrovací tabulky v IPv6 síti zajišťují, že se datagramy směřují na některou z adres daného prefixu stroje realizujícího NAT-PT. [2; 7]

Pro opačný postup zařízení využívá adresy z poolu IPv4 adres v okamžiku, kdy zařízení IPv6 odešle datagram do IPv4 sítě, vytvoří se pro IPv6 adresu a port odesilatele záznam v mapovacích tabulkách, datagram přeloží do IPv4 a nastaví v něm adresu a port podle tabulky. Když pak na tuto adresu a port přijde z IPv4 odpověď, přeloží ji do IPv6, opět s použitím mapovací tabulky pro určení cílové adresy a portu. Schéma sítě implementující NAT-PT je zobrazen na obrázku 2. [2]



Obrázek 3: Příklad sítě s využitím mechanizmu NAT-PT [2]

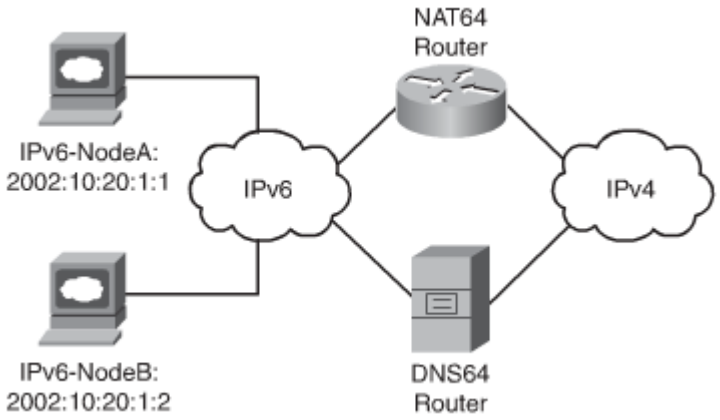
Omezení tohoto mechanizmu jsou obdobná jako u klasického NAT pro IPv4. Zejména mechanizmus nepodporuje asymetrické (například dual houming) směrování, jelikož je nutné spojení realizovat stále přes stejné zařízení realizující NAT-PT. Dále jsou zde problémy s DNS, při nutnosti změn A dotazů na AAAA a opačně při inicializaci komunikace.

Praktické nasazení tohoto mechanizmu v sítích ukázalo řadu problémů, z nichž většina pramenila z výše popsaných úprav DNS. NAT-PT byl v RFC 4966 odmítnut a prohlášen za historický. [6] Ovšem vzhledem k značnému rozšíření v zařízeních je i v současnosti hojně využíván zejména v sítích, kde existují prvky s jeho implementací, a nebylo prozatím rozhodnuto o jejich výměně.

3.9.6 NAT64

Mechanizmus NAT64 překládá IPv6 na IPv4, oproti NAT-PT je však iniciátor spojení vždy na straně IPv6 sítě. NAT64 implementuje další funkcionality jako NAT mapování, filtrování a umožňuje TCP simultánní otevření spojení. Obrázek 2 zobrazuje

zjednodušenou síť s NAT64 mechanizmem přechodu, IPv6, IPv4 zařízeními a DNS64 [2]. DNS64 je rozšíření DNS, obvykle implementované spolu s NAT64, které implementuje statické bez stavové mapování IPv4 adres na IPv6 adresy. Toto řeší problémy s DNS zmíněné v kapitole o NAT-PT. [2]



Obrázek 4: Příklad sítě s využitím mechanizmu NAT64 [2]

4 Analytická část

Plánování přechodu k protokolu IPv6 má řadů aspektů. Jakožto nosná technologie se dotýká všech aspektů fungování IT ekosystému firmy. Migrace má tedy za následek zásadní změny v architektuře firemní datové sítě.

4.1 Migrace firemního prostředí

Je nutné si uvědomit, co je vlastně firemní datová síť. Dle [2] je firemní datová síť platformou, jež spojuje uživatele, služby, zařízení a informační zdroje firmy za účelem podpory hlavní funkce podniku, tj. produkce statků nebo služeb určených k prodeji na trhu [8]. Přechod a jeho podoba tedy musí všechny tyto aspekty zohlednit.

4.1.1 Obchodní (hospodářský) důvod

Obchodní (hospodářský) důvod, z nejvyššího pohledu, definuje potřeby podniku, které daný projekt přechodu k IPv6 má řešit. Zabývá se důvody realizace, definuje očekávané hospodářské přínosy a rizika realizace, zvažuje možnosti a předpokládané náklady realizace přechodu na IPv6. Pod tímto pojmem si lze představit soubor faktorů stanovující a formulující hodnotu projektu.

Hodnotou projektu rozumíme přínosy, které organizace získá díky využití výsledku projektu. Hodnotu projektu vytváří koncový výsledek projektu získaný z vynaložených nákladů na projekt (projektovou investici), přičemž výsledek projektu může představovat finanční a nefinanční přínosy.[8]

Obecně se v projektovém řízení mluví o třech základních kategoriích výsledků:

- vytvořený produkt určený k dalšímu užití po ukončení projektu,
- vytvořená schopnost poskytovat službu po ukončení projektu,
- získaná znalost využitelná po ukončení projektu.

V řadě případů v současnosti pro podniky nelze tento důvod definovat. Při analýze může daný subjekt dojít k závěru, že vzhledem ke stávajícímu stavu IT ekosystému firmy, rizikům realizace a nákladům přechodu není v daný okamžik možné přechod realizovat. Při přípravě daného hospodářského důvodu by měla být klíčovým imperativem důkladná analýza rizik, která by mohla mít za následek zásadní narušení hlavní funkce podniku. Naopak pro řadu podniků lze identifikovat jasné potřeby nebo přínosy realizace přechodu k IPv6. V základu lze potřeby rozdělit na kruhy, a to legislativní, technické a ekonomické.

4.1.2 Legislativní požadavky na přechod

Jedním z pádných důvodů pro migraci může být legislativní povinnost firmy zpřístupnit své služby pomocí protokolu IPv6. V českém prostředí je řada podniků povinna zajistit soulad s legislativními požadavky kladenými zejména usnesením Vlády České republiky č. 727, ze dne 8. června 2009 [10], v němž uložila ministrům a vedoucím ostatních ústředních orgánů státní správy zajistit:

- **od 30. června 2009 při pravidelné obnově síťových prvků jejich kompatibilitu s internetovým protokolem verze 6 (IPv6),**
- **do 31. prosince 2010 přístup k internetovým stránkám a veřejně dostupným službám eGovernmentu internetovým protokolem verze 4 (IPv4) i internetovým protokolem verze 6 (IPv6).**

Z tohoto požadavku pak vyplývá povinnost přechodu všem podnikům, plánují poskytovat služby v oblasti zajištění provozu aplikací eGovernmentu [10].

4.1.3 Technické požadavky na přechod a přínosy přechodu

Původní předpoklady, při zahájení prací na novém protokolu, počítaly s vyčerpáním adresních rozsahů IPv4 do konce dekády. Následně byla přijata řada opatření (např. schválení a zavedení konceptu NAT), jež razantně snížila konzumaci jeho rozsahu tak, že se kolem roku 2000 předpokládal dostatek adres na 20 let. V posledních letech se však trend obrátil a došlo k razantnímu nárůstu alokací tak, že k vyčerpání IPv4 adres v podstatě došlo, pro oblast RIPE, dokonce již v roce 2012. Dne 14. září 2012, RIPE NCC začala alokovat IPv4 adresní rozsah z poslední /8 alokace ve svém držení. V praxi RIPE zahájilo alokaci dle speciálního, již dříve připraveného, předpisu a jeho členové mohou obdržet pouze /22 alokaci (1024 IPv4 adres), pokud řádně ospravedlní velikost alokace. Alokace je navíc podmíněna jen pro členy, a to v případě kdy již obdrželi IPv6 alokaci. Pro rozvoj stávajících služeb a zajištění zdrojů IPv4 je tedy nezbytné přistoupit nebo alespoň uvažovat i o souběžném zavedení nebo přechodu na IPv6.

Dále je zde řada dalších specifických důvodů pro přechod, zejména v oblasti poskytování služeb založených na průmyslových standardech, v oblasti mobilních služeb, poskytování obsahu a průmyslových sítí. Do těchto oblastí můžeme zařadit [3]:

- IMS (IP-Multimedia Subsystem) – je určen pro doručování multimediálních služeb mobilním uživatelům. Pro svoji funkcionalitu přímo vyžaduje IPv6.
- DOCSIS (Data Over Cable Service Interface Specification) – je určen pro kabelové operátory pro poskytování hlasových, datových a video služeb. Verze DOCSIS 3.0

rovněž nařizuje CMTS (Cable modem termination system) i kabelovým modemům být IPv6 kompatibilní.

- Nový fenomén Internet věcí („Internet of Things“) – pod názvem „Internet věcí“ se skrývá trend masivního nasazení malých zařízení pro kontrolu, komunikaci a vzdálené ovládání systémů, jako například metrologických čidel, nezávislých senzorů nebo ovládacích prvků. Tuto oblast obvykle řeší výzkumné a průmyslové organizace a dále dodavatelé v oblasti utilit.

Všechny tyto důvody vyvolávají potřebu velkého počtu IP adres pro zajištění provozu služeb. Všechny tyto kapacitní požadavky je ideálně vhodné řešit přechodem k IPv6.

Dalším důvodem může být zavedení specifické nové aplikace nebo služby, využívající výhradně protokol IPv6, která je vyžadována pro zajištění hlavních funkcí podniku.

4.1.4 Provozní a ekonomické důvody

Standardní síťová infrastruktura společnosti je navržena tak, aby pokryla potřeby organizace v horizontu pěti až osmi let v závislosti na strategii ICT, dlouhodobých plánech organizace a nastavení interních účetních předpisů. V okamžiku přiblížení se k horizontu obnovy infrastruktury je nutné do celkových plánů zařadit i posouzení možnosti migrace na IPv6 v porovnání na vynaložené náklady. Je vhodné do analýzy zařadit varianty TCO (*Total cost of ownerchip*, celkové náklady na vlastnictví, jedná se o ekonomický parametr zahrnující jak investiční, tak provozní náklady související s investicí v období zpravidla definovaném účetně odpisovou dobou) počítající s nasazením:

- IPv6 jako nativního protokolu (nativní IPv6).

- Dual Stack.
- Prvotní ponechání IPv4 a následnou migraci na IPv6 (v některé z možných variant).

Do této kategorie lze zařadit i migraci z důvodu nutnosti adaptace nových zařízení do infrastruktury (bez studie TCO). Vzhledem k současné praxi výrobců zařízení, kdy valná většina nových zařízení či nově instalovaných operačních systémů má ve výchozím nastavení zapnutou podporu IPv6, přičemž v souvislosti s vlastnostmi nového protokolu tento neřešený stav může mít za následek jednak výkonnostní problémy, ale hlavně přináší potencionální bezpečnostní rizika. Z tohoto důvodu je bezpodmínečně nutné minimálně porozumět aspektům IPv6 a zajistit odpovídající bezpečnostní a technická opatření, případně IPv6 v organizaci adoptovat.

4.2 Příprava a plánování migrace

4.2.1 Projektová a procesní příprava migrace

Řádně řízené ICT v organizaci má jasně definovanou strategii a nastavené procesy řízení infrastruktury ICT. Standardem v oblasti metodiky pro procesní řízení ICT organizace je knihovna *Information Technology Infrastructure Library* [11], v současnosti ve verzi 3 (ITILv3). ITILv3 je složena z několika knih, které popisují specifické oblasti řízení ICT služeb v organizaci pomocí procesů. Oproti například normě ISO 20000 nediktuje striktně, jak má proces vypadat, ale vede organizaci při návrhu procesů tak, aby mohla své procesy uzpůsobit své velikosti.

Potřebné procesy pro úspěšný přechod jsou obsaženy v ITIL knize Service Transition, kde jsou obsaženy dva klíčové procesy v řízení ICT organizace, a to je proces řízení změn a

proces uvolnění (change management, release and deployment management). Jejich zvládnutí je klíčovým předpokladem pro úspěšné zavedení tak významné změny, jako je přechod firemního prostředí na protokol IPv6 v odpovídající kvalitě.

Tak významná změna, jako je přechod IPv6, se dotkne každé části organizace, proto je nutné pro tento účel vytvořit projektový tým a zapojit všechny dotčené subjekty, včetně klíčových řídících orgánů společnosti. Řada organizací má již v současnosti nějakou zkušenost s projektovým řízením dle různých metodik (PRINCE2, PMP), stačí tedy využít zkušeností dané organizace. Důležité je stanovení účelu a cílů projektu tak, aby dodaná změna, přechod firemního prostředí na IPv6, byla realizována v požadované kvalitě. To znamená tak, aby splnil požadované technické parametry v souladu s bezpečnostní politikou organizace včas a při dodržení rozpočtu.
Účel projektu je definován důvody organizace pro přechod, jak je uvedeno v kapitole 3.1, cílem projektu je přechod společnosti na protokol IPv6 v požadované kvalitě. Důležitý je z tohoto hlediska pojem „požadovaná kvalita“. Jeho nedílnou částí je cena projektu, v našem případě cena realizace migrace tak, aby bylo vyhověno důvodu za maximálně efektivně vynaložené prostředky organizace. V praxi se tedy často děje, že organizace po analýze důvodů dojde k závěru, že přechod bude realizován pouze a jen v rozsahu zcela nezbytném pro zajištění okamžitých požadavků. Komplexní přechod na protokol IPv6 se obvykle realizuje v okamžiku celkové rekonstrukce infrastruktury v okamžiku účetního odpisu stávajících komponent infrastruktury, případně v okamžiku zásadních změn na aplikační úrovni nebo zásadních změn v strategii ICT organizace. Proto je vhodné vypracovat v rámci projektu dlouhodobou (v současnosti tří až pětiletou) koncepci přechodu k IPV6 a tu začlenit do strategie ICT organizace.

Celkem lze shrnout aspekty migračního projektu do čtyř základních oblastí [12]:

- Sladění se strategickými cíli, v tomto bodě je nutné identifikovat strategickou hodnotu změny. Tedy důvody a soulad s ICT strategií firmy;
- definovat projektové cíle, tedy čeho má být změnou (přechodem) dosaženo;
- definovat rozsah projektu, tedy identifikovat oblast IT infrastruktury, jež bude změnou dotčena;
- definovat harmonogram projektu, tedy identifikovat metriky a milníky projektu a jejich finanční a kapacitní nároky;
- důkladně analyzovat a popsat rizika projektu, současně navrhnout opatření k mitigaci těchto rizik.

Pro vypracování detailního migračního plánu musí být konkrétně identifikována každá dotčená komponenta ICT prostředí. K tomuto účelu je v knižnici ITIL definována komponenta CMDB (*a configuration management database*), což je databáze pro podporu procesů ICT organizace. Obvykle se skládá z jednotlivých položek (komponent) ICT infrastruktury jako například jednotlivá zařízení (servery, aplikace), dále ovšem obsahuje i informace o kontraktech, SLA a vazby mezi nimi. Tato informace nám dává ucelený přehled a umožní identifikovat dotčené položky.

Hlavní kroky pro přípravu plánu migrace lze shrnout na základě předchozích informací do těchto kroků [12]:

- Definovat cíle, identifikovat rozsah projektu, metriky a harmonogram implementace.
- Posoudit stávající IT prostředí, v tomto kroku provést inventarizaci IT z důvodu identifikace možností položek a jejich kompatibility s IPv6.

- Revize provozních a organizačních pravidel a politik, integrace se dotýká všech složek organizace, jejich zainteresování do projektu je klíčové pro úspěšnou realizaci projektu.
- Revize stávajících SLA (Service level agreement) a OLA (Operational level agreement).
- Řádné proškolení všech zainteresovaných, je nutné nejen řádně proškolit technický personál organizace, ale je zvláště nutné identifikovat klíčové uživatele (pokud nejsou definováni v rámci ICT politiky organizace), a tak maximálně usnadnit přechod uživatelům, kteří definují potřeby organizace.
- Poučit se ze zkušeností ostatních, adoptovat ověřené postupy (best practise), tím racionalizovat migraci, a tak mitigovat rizika neúspěchu projektu.

4.2.2 Technická příprava migrace

Technická část přípravy migrace zahrnuje volbu scénáře implementace závislého na aktuálním prostředí z hlediska koncových zařízení, operačních systémů, síťových prvků, jejich modelů a verzí, klíčových aplikací, architektury, rozpočtu, zdrojů, a harmonogramu migrace.

Typická firemní síťová infrastruktura se skládá z vrstev neboli modulů:

- Core (Jádro) - je část sítě která propojuje všechny níže vyjmenované části firemní sítě. Z tohoto důvodu je na ní kladen nejvyšší důraz na dostupnost a robustnost;
- Campus - zajišťuje připojení pro koncové uživatele a provoz konektivity skrze jádro k serverovým technologiím umístněným v datovém centru organizace;

- Datové centrum - zde jsou umístěny klíčové komponenty (servery, síťové prvky a úložiště) a provozovány informační systémy organizace;
- Edge - modul zajišťující komunikaci s vnějším okolím (internet, VPN a WAN).

Adresní plán IPv6, pro všechny typy adres, je nutné volit s ohledem k členění firemní sítě s dostatečnou rezervou pro růst organizace v plánovaném období dle ICT strategie organizace.

V technické části je zvolen scénář migrace, tedy v jakém pořadí a jakým směrem budou jednotlivé moduly migrovány. Typicky je zvolen první pilotní modul pro implementaci, následuje core modul a následně ostatní moduly v pořadí zvoleném na základě analýzy a cílů projektů.

Jako pilotní modul je v prvním kroku volen modul dle cíle projektu. Typicky v případě, že cílem je zajištění dostupnosti aplikace internetových uživatelů, první krokem je edge modul, následuje core a optimálně konečný je modul datového centra. V případě využití některého z překladových mechanizmů a na základě projektových cílů, může být projekt uzavřen po implementaci v edge modulu.

Jiným případem je postup směrem od campus sítě, čímž je zajištěn přístup koncových uživatelů uvnitř organizace protokolem IPv6 následně se postupuje opětovně do datového centra přes jádro infrastruktury.

Obecně migrace každé části (modulu) by měla být uzavřena, postup vyhodnocen a navržena případná opatření ke zlepšení postupu v další části. Jedná se o známý PDCA cyklus (z anglického *plan-do-check-act*) tedy plánuj, udělej, zkontroluj, jednej. Z tohoto důvodu by modul, kde změna bude celý proces migrace ukončovat, měl být definován na základě analýzy rizik tak, aby se rizika dopadu na organizaci mitigovala pomocí důkladného zvládnutí celého procesu.

5 Příklad reálného nasazení IPv6

V praktické části je popsána realizace nasazení IPv6 ve firmě provozující datové centrum. Jejími významnými zákazníky jsou subjekty veřejné správy, které jsou na základě legislativní povinnosti povinny zpřístupnit své služby pomocí protokolu IPv6. Vznikl tak požadavek zajištění takovéto služby. Pro implementaci požadavku vznikl projekt, který dostal za úkol připravit infrastrukturu tak, aby byl splněn legislativní požadavek v termínu daném vyhláškou, za minimální cenu a bez dopadu na stávající implementaci provozovaných aplikací. Harmonogram celého projektu počítal s devíti týdny od zahájení projektu do termínu předpokládané akceptace řešení před termínem daným legislativními požadavky.

Projektový tým tvořilo šest osob v obsazení sponzor projektu (zástupce managementu), zástupce úseku zodpovědného za následný provoz, projektový specialista, systémový specialisté.

5.1 Technické řešení nasazení

Po posouzení dopadu případné komplexní implementace IPv6 do všech vrstev DC, byla vypracována analýza infrastruktury v základních oblastech:

- podpory jednotlivých komponent infrastruktury protokolu IPv6;
- požadavků bezpečnostního týmu organizace a jejich dopad na bezpečnostní politiku organizace;
- požadavků kompetenčního týmu podpory aplikací;
- dopadů do provozních postupů.

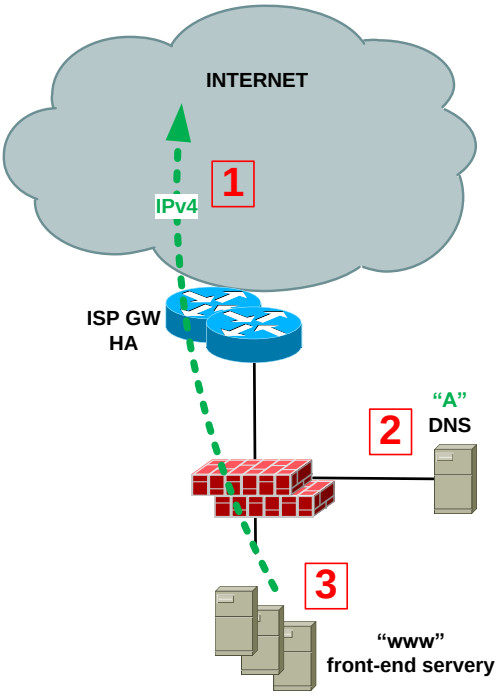
Na základě shromážděných informací, bylo pro volbu technického řešení, klíčové zjištění v oblasti předpokládaných provozních postupů. Předpoklad na základě analýzy počítal s až dvojnásobným nárůstem pracnosti v provozu infrastruktury. To by mělo za následek celkový nárůst provozních nákladů o cca 40%. Na základě těchto zjištění došlo ve spolupráci s vlastníkem aplikace k závěru, že by celková migrace měla značné provozní a bezpečnostní dopady, bez jakéhokoliv pozitivního efektu a jednalo by se o nehospodárně vynaložené prostředky. Proto, aby byl splněn zadaný úkol, bylo rozhodnuto implementovat IPv6 na perimetru datového centra tak, aby provozované aplikace byly pomocí IPv6 přístupny. Rozhodnutí o případném celkovém přechodu k IPv6 bylo přesunuto až do okamžiku obnovy infrastruktury po účetním odpisu stávajících zařízení infrastruktury.

5.2 Výchozí stav datového centra

Obecný výchozí stav nejen datových center veřejné správy ilustruje Obrázek 5.

Důležitá místa výchozího stavu jsou označena červenými čísly:

1. Spojnice (aktivní i záložní) k poskytovateli internetového připojení jsou ve výchozím stavu současnosti konfigurovány a provozovány výhradně na IPv4.
2. Na veřejném DNS serveru zajišťujícím veřejné jmenné služby pro IISSP existují pouze „A“ záznamy.
3. Vnitřní síťové prvky i front-end servery včetně webových prezentací jsou konfigurovány a provozovány výhradně na IPv4.



Obrázek 5: Výchozí stav datového centra

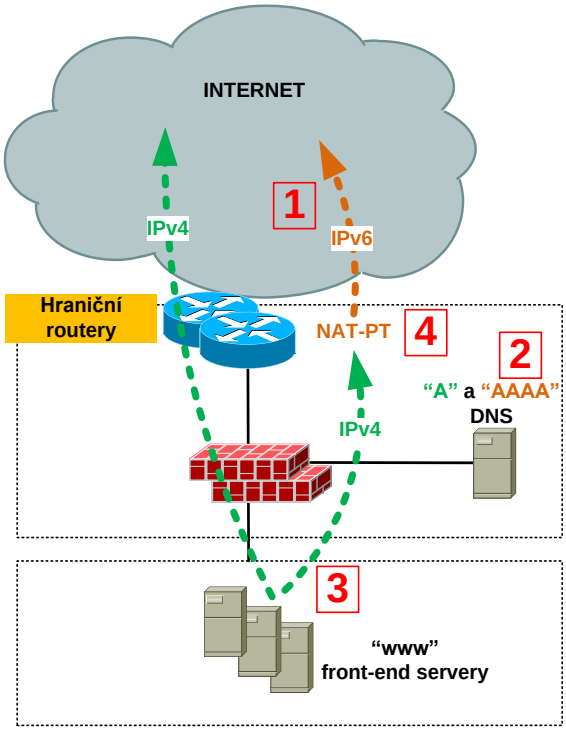
5.3 Cílový stav technické řešení

Celkový cílový stav relevantních částí datové komunikační infrastruktury ilustruje obrázek 6.

Důležitá místa v upravené infrastruktuře jsou opět označena červenými čísly:

1. ISP spojnice (aktivní i záložní) k poskytovateli internetového připojení jsou konfigurovány a provozovány zároveň na IPv4 i IPv6.
2. Na DNS serveru zajišťujícím veřejné jmenné služby pro datové centrum jsou současně „A“ i „AAAA“ záznamy.

3. Vnitřní síťové prvky i front-end servery včetně webových prezentací jsou nadále konfigurovány a provozovány výhradně na IPv4.
4. Na hraničních branách je spuštěný NAT-PT (Network Address Translation Protocol Translation), jenž zajišťuje vzájemné propojení a komunikaci světů IPv4 a IPv6. Z množiny NAT-PT je většinou použita funkcionalita „NAT64 packet translator“.



Obrázek 6: Cílový stav datového centra

5.4 Adresace a směrování

Provozovatel datového centra je člen RIPE NCC, od něhož má jednak přidělen vlastní IPv4 rozsah a současně je mu přidělena adresace IPv6 v bloku ::/32 adres globálních individuálních adres.

Tento blok je dále rozdělen na bloky po globálních ::/36 pro jednotlivá DC firmy. Dále je členěn do globálních ::/48 adresních bloků pro jednotlivé služby (provozované aplikace a zákaznické moduly). Následně je rozdělen do ::/56 bloků pro jednotlivá prostředí dle metodik organizací (například samostatná DC, produkční, testovací a vývojové prostředí atd).

Toto rozdělení bylo zvoleno jako strategické s vizí nasazení v celé infrastruktuře. Jelikož však byl projektem definován cíl pouze zpřístupnit aplikace pro internetové uživatele je z bloku pro produkční prostředí vyčleněn blok ::/64 a tento použit pro NAT-TP (viz kapitola 3.3.6). Tato volba není v rozporu se strategickými cíli, jelikož v budoucnu celý blok bude případně využit v externí DMZ.

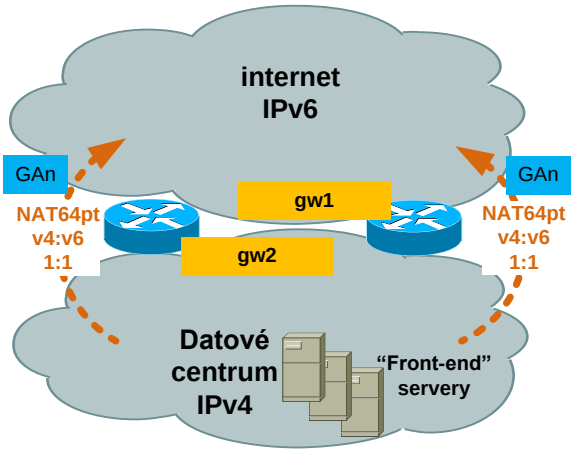
Stávající infrastruktura internetového perimetru je rozšířena pro IPv6. Konfigurační změny se týkají pouze internetových směrovačů. Pro směrování je zvolen protokol BGPv6, a stávající služby ISP providera rozšířeny o IPv6 konektivitu.

5.5 DNS

Jako DNS servery datového centra jsou provozovány servery BIND, zónové soubory jsou doplněny o „AAAA“ záznamy provozovaných doménových jmen a delegace pro reverzní domény (PTR). Způsob vytváření zónových souborů je uveden v kapitole 3.9.

5.6 NAT-PT

Jako přechodový mechanizmus byl zvolen překladový mechanizmus NAT-PT. Jak bylo výše zmíněno, nejedná se v současnosti o preferovaný mechanizmus, ale po vyhodnocení možností byl zvolen pro svoji jednoduchou implementaci a podporu na stávajících zařízeních. Na internetových branách je spuštěný NAT-PT (*Network Address Translation – Protocol Translation*), jež zajistí vzájemné propojení a komunikaci světů IPv4 a IPv6. Z množiny NAT-PT je použita funkcionalita „NAT64 packet translator“. Situaci v datovém centru ilustruje obrázek 7.



Obrázek 7: Funkce NAT-PT v řešení

Jak je uvedeno výše v kapitole 5.4, z adresního bloku pro produkční prostředí je vyčleněn blok ::/64 IPv6 adres použitý pro NAT-TP. IPv6 prezentovaných služeb je překládané 1:1 pro adresy na IPv4 v bloku /29.

Pro příklad cílová adresa IPv6 2001:b80:102:2c0:dead:face:0591:680F je pomocí mechanizmu přeložena na veřejnou adresu z bloku 5.145.104.48/29 pro komunikaci směrem ke zdrojům DC.

6 Zhodnocení výsledků

Použité řešení plně splnilo dané projektové cíle a v současnosti je úspěšně provozováno již téměř dva roky. Za tuto dobu narostl podíl přístupů z 0.2% na průměrně 2,5% z celkového objemu. Pro představu lze v příloze nalézt dva přehledové grafy přístupů, zpracované z dat měsíce října roku 2013. První zobrazuje průměrné hodinové přístupy za 24 hodin z měsíčních dat. Druhý pak celkové hodinové počty přístupů v tomtéž období. Pro porovnání jsou uvedeny jak údaje za protokol IPv6 tak protokol IPv4.

Obecně sledujeme malý, ale trvalý trend nárůstu přístupů pomocí IPv6, zapříčiněn zejména narůstající penetrací IPv6 u koncových uživatelů. Způsobenou nedostatkem adres IPv4 v kapacitách telekomunikačních operátorů.

Z provozu byla získána řada poznatků a doporučení pro budoucí rozvoj, zejména v oblasti bezpečnostních opatření a požadavků, dále požadavků na implementaci, které budou zohledněny při budoucí implementaci v okamžiku celkové rekonstrukce. Tato rekonstrukce je plánována z důvodu morální zastaralosti některých komponent a úplného konce podpory na další části infrastruktury. Ovšem i přes rozsáhlé změny prozatím není plánována migrace k IPv6 na všech vrstvách infrastruktury, ale jen na přístupovém perimetru zejména v oblasti bezpečnosti, jako například při využití aplikačních firewallů a dalších komponent.

7 Závěr

Ačkoliv z dlouhodobého hlediska je jasná budoucnost v internetovém prostředí v protokolu IPv6, a s tím související nutnost přizpůsobení firemního prostředí, stále se však v současnosti jen těžko hledají důvody pro realizaci koncepčního přechodu firemního prostředí na protokol IPv6.

Valná většina současných projektů již dnes po vyhodnocení všech aspektů migrace spočívá pouze v zpřístupnění IPv6 pro komunikaci v rámci internetu (jedná se o implementaci v edge modulu), a to pomocí některého z přechodových mechanizmů tak, jak bylo nastíněno v uváděném případu reálného nasazení.

Pro úspěšné zvládnutí přechodu je i tak nezbytně nutné zvládnout procesní a projektovou stránku řízení infrastruktury ICT organizace, jakožto dva klíčové aspekty migrace firemního prostředí k IPv6.

8 Seznam použitých zdrojů

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

2. **McFarland, Shannon, et al.** *IPv6 for Enterprise Networks.* Indianapolis : Cisco Press, 2011. 978-1-58714-227-7.

3. **Hagen, Silvia.** *Planning for IPv6.* Sebastopol : O'Reilly Media, Inc., 2011. 978-1-4493-0539-0.

4. **Graziani, Rick.** *IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6.* Indianapolis : Cisco Press, 2012. 978-1-58714-313-7.

5. **Blanchet, Marc.** *Migrating to IPv6: A Practical Guide to Implementing IPv6 in.* Chichester : John Wiley & Sons Ltd, 2006. 0-471-49892-0.

6. **Nakamura, M. a Hagino, J.** SMTP Operational Experience in Mixed IPv4/v6 Environments. [Online] http://tools.ietf.org/html/rfc3974.

7. NAT-PT. *IPV6.CZ.* [Online] 20. 8 2011. [Citace: 30. 1 2014.] https://www.ipv6.cz/NAT-PT.

8. **Žídková, Dana a Rosochatecká, Eva.** *Ekonomika podniků.* Praha : Česká zemědělská univerzita v Praze, Provozně ekonomická fakulta, 2011. 978-80-213-1886-1.

9. *Business Case: řízení hodnoty a rozsahu ICT projektu.* **Hujňák, Petr.** Prague : Proceedings of the 16th International Conference on Systems Integration 2008, 2008. 978-80-245-1373-7.

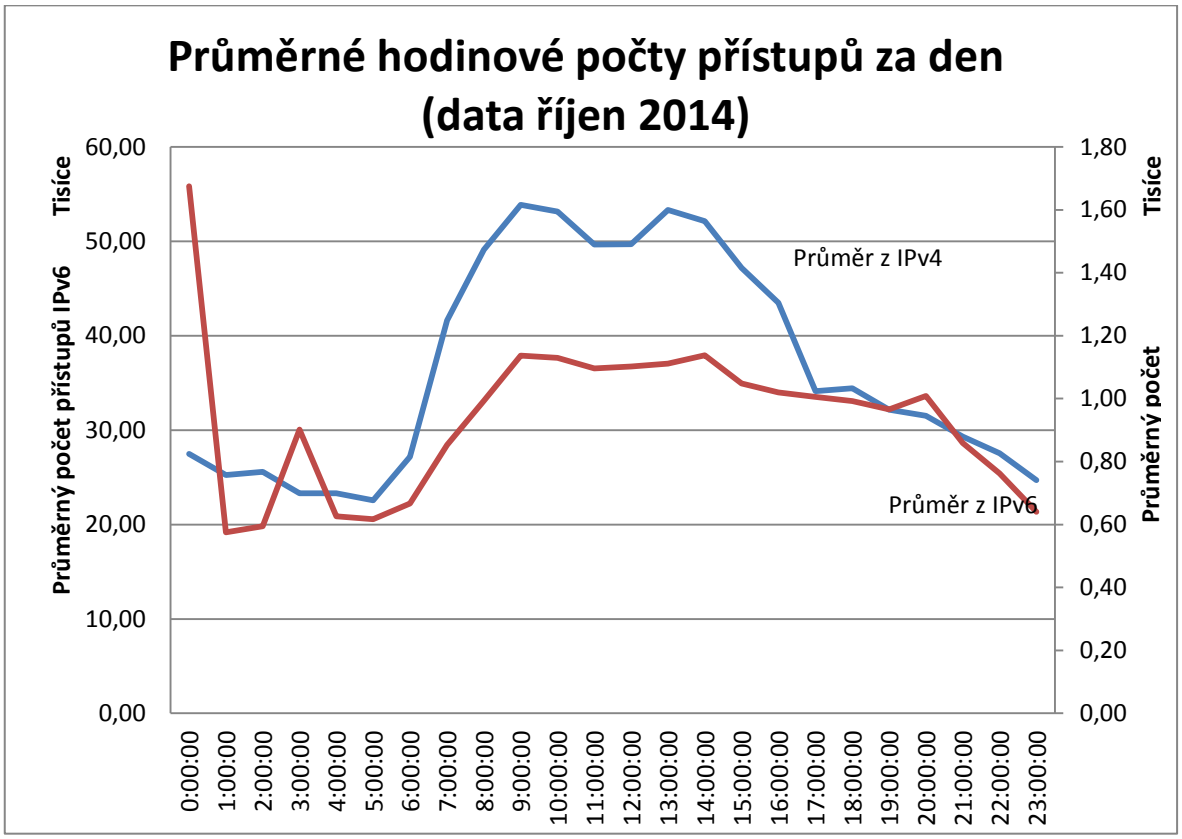
10. **VLÁDA ČESKÉ REPUBLIKY.** USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 8. června 2009 č. 727 ke Zprávě o přechodu na internetový protokol verze 6 (IPv6).

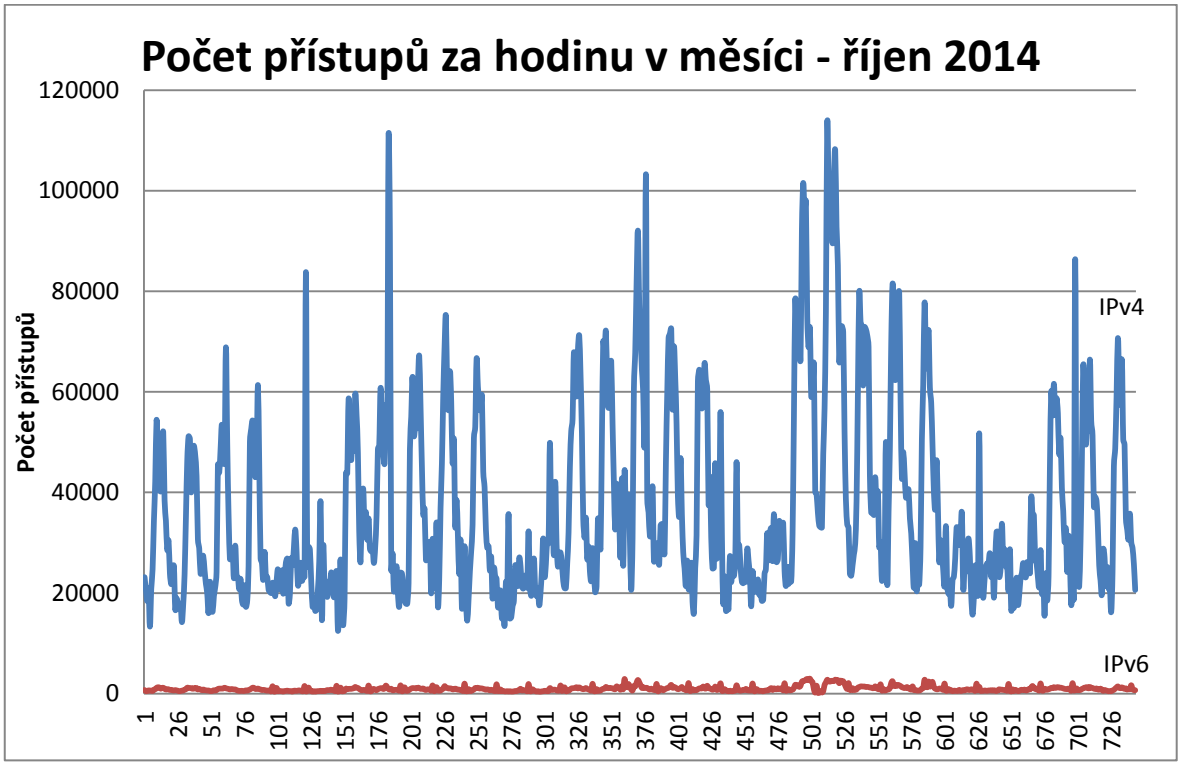
11. *THE OFFICIAL ITIL® WEBSITE.* [Online] AXELOS. [Citace: 27. 02 2014.] http://www.itil-officialsite.com/.

12. **Grossetete, Patrick, Popoviciu, Ciprian a Wettling, Fred.** *Global IPv6 Strategies: From Business Analysis to Operational Planning.* Indianapolis : Cisco Press, 2008. 978-1-58705-343-6.

9 Seznam obrázků

10 Příloha


Průměrné hodinové počty přístupů za den
(data říjen 2014)
Průměrný počet přístupů IPv6
Tisíce
Průměrný počet
Tisíce
60,00
50,00
40,00
30,00
20,00
10,00
0,00
1,80
1,60
1,40
1,20
1,00
0,80
0,60
0,40
0,20
0,00
Průměr z IPv4
Průměr z IPv6
0:00:00
1:00:00
2:00:00
3:00:00
4:00:00
5:00:00
6:00:00
7:00:00
8:00:00
9:00:00
10:00:00
11:00:00
12:00:00
13:00:00
14:00:00
15:00:00
16:00:00
17:00:00
18:00:00
19:00:00
20:00:00
21:00:00
22:00:00
23:00:00


Počet přístupů za hodinu v měsíci - říjen 2014
Počet přístupů
120000
100000
80000
60000
40000
20000
0
IPv4
IPv6
1
26
51
76
101
126
151
176
201
226
251
276
301
326
351
376
401
426
451
476
501
526
551
576
601
626
651
676
701
726