Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

IPv6 aspekty migrace firemního prostředí

Viktor Kult

! ! !

Místo této strany vložíte zadání bakalářské práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

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

V Praze dne 17. 3. 2014 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Alexandru Vasilenkovi za konzultace a vstřícný přístup při návrhu struktury a zpracování této práce. Poděkování patří také pánům Ing. Vladimíru Hrníčkovi a Dušanu Kolaříkovi ze společnosti Telefónica Česká Republika a.s. i dalším kolegům za ochotu spolupracovat na tvorbě bakalářské práce.

IPv6 aspekty migrace firemního prostředí

IPv6 migration aspects of business environment

Souhrn

Práce se věnuje problematice rozšíření IPv6 v prostředí současných počítačových sítí. V první části práce je přiblížena aktuální situace a důvod migrace na IPv6. Dále jsou představeny mechanismy, které podporují migraci a některá typická prostředí firemních sítí. Firemní prostředí je rozděleno do částí (běžná společnost, poskytovatel připojení, datacentrum, malá domácí kancelář). Ve druhé části jsou zpracovány související informace od poskytovatelů internetových služeb, výrobců technologií a vývojářů operačních systémů. Celkově má práce sloužit jako zdroj informací, upozornit na technické podmínky síťového prostředí související s migrací na IPv6.

Summary

The thesis is dedicated IPv6 extension in the current environment of computer networks. In the first part of the thesis is to describe the current situation and the reason for the migration to IPv6. The following are introduced mechanisms that promote migration and some typical corporate network environment. Corporate environment is divided into sections (normal company, ISP, Data Center, a small home office). The second part presents related informations from Internet service providers, technology vendors and developers of operating systems. Overall, the thesis serves as a source of information, to highlight the technical conditions of the network environment-related migration to IPv6.

Klíčová slova:

IPv4, IPv6, Firemní síť, Poskytovatel služeb, SOHO, CGNAT, Mobilní připojení, Fixní připojení, Datacentrum, ISATAP, Teredo, Dual-stack Lite

Keywords:

IPv4, IPv6, Enterprise network, Service provider, SOHO, CGNAT, Mobile connectivity, Wired connectivity, Data Center, ISATAP, Teredo, Dual-stack Lite

Obsah

1 Úvod 10
2 Cíl práce a metodika 11
3 Přehled řešené problematiky 12
3.1 IP (Internet Protocol) 12
3.1.1 Vznik, Historie, Vývoj 12
3.1.2 Funkce / Význam IP v OSI a TCP/IP modelu 12
3.1.3 Charakteristika IPv4 13
3.1.4 Výhody IPv4 13
3.1.5 Nevýhody IPv4 14
3.1.6 Problematika adresního prostoru 14
3.1.7 Statistiky využití IPv4 v Evropě 14
3.1.8 Charakteristika IPv6 15
3.1.9 Rozšíření IPv6 a výhody proti IPv4 15
3.1.10 Nevýhody a chyby IPv6 16
3.1.11 Současný stav využití IPv4/IPv6 16
3.2 Migrace IPv4 na IPv6 17
3.2.1 Důvody migrace 17
3.2.2 Technická způsobilost a podpora IPv6 17
3.2.3 Podpora IPv6 u aktivních prvků síťové struktury 18
3.2.4 Směrovací protokoly podporující IPv6 18
3.2.5 DNS (Domain Name System) 18
3.3 Mechanismy podporující migraci firemního prostředí 19
3.3.1 Tunneling 19
3.3.2 Překlady IP adres (IP/ICMP Translation Algorithm) 22
3.4 Migrace firemního prostředí 23
3.4.1 Definice sítě firemního prostředí 24
3.5 Migrace ISP 25
3.5.1 Mobilní internet (GPRS, UMTS, LTE) 25
3.5.3 DSL 26
3.5.5 Datacentra (Serverhousing, Serverhosting) 27
3.6 Migrace SOHO (Small Office Home Office) 28
4 PRAKTICKÁ ČÁST 29
4.4 Firemní prostředí 29
4.4.1 Pracovní stanice a servery 29
4.4.3 Síť 30
4.5 Sítě ISP 33
4.5.1 Mobilní Internet 33
4.5.4 DSL 35
4.5.5 Datacentra 35
4.6 Malé sítě SOHO 36
5 VÝSLEDKY A DISKUSE 38
6 Závěr 40
7 Seznam použitých zdrojů 42

1 Úvod

Pro současnou moderní společnost je typické využívání technicky vyspělých technologií. Tato skutečnost je zřejmá v řadě odvětví lidské činnosti. V průběhu dvacátého století došlo k největšímu rozvoji informačních technologií v historii lidstva vůbec. Informační technologie jsou současnou společností využívány pro podporu průmyslu, vojenství, obchodu, vesmírného výzkumu, kultury, sociálních vztahů a spoustu dalších činností. Výrazné navýšení efektivity informačních technologií lidstvo získalo vzájemným propojováním jednotlivých počítačů. Propojení počítačů do sítí umožňuje především výměnu a sdílení informací, což otevřelo nové možnosti jejich využití jako součástí komplexních informačních systémů. Potřeba sdílení informací stála za vývojem technologie počítačové sítě, která umožnila vzájemné propojení lokálních sítí mezi různě geograficky vzdálenými lokalitami. V šedesátých letech minulého století stála americká vojenská agentura za vznikem sítě známou jako ARPANET, která takové sdílení informací umožňovala. Síť ARPANET tak můžeme považovat za předchůdce systému vzájemně propojených počítačových sítí v současnosti známého jako Internet. Internet běžně využíváme především jako komunikační nástroj a zdroj informací pro účely studijní, pracovní i soukromé. Dostupnost Internetu běžným uživatelům obvykle zprostředkovává některý z poskytovatelů internetové konektivity ISP (Internet Service Provider). Připojení k internetu uživatelům poskytovatel zajišťuje nejčastěji prostřednictvím mobilních (WiFi, UMTS, CDMA, LTE) nebo fixních (xDSL, FTTX) služeb. Volba ISP a způsobu připojení k Internetu závisí na technických možnostech poskytovatele a požadavcích každého zákazníka. Jednotlivé služby se od sebe odlišují především ve využití fyzického přenosového média, mobilitě, přenosové rychlosti dostupnosti a v neposlední řadě také ceny. Pro funkční připojení uživatele k internetu nebo jakékoli jiné síti, je vždy nutné zprovoznit síťový protokol bez ohledu na typ připojení. Role sítového protokolu je popsána modelem síťové architektury ISO/OSI specifikovaného v doporučení ISO 7498 nebo jeho zjednodušenou verzí TCP/IP. V současnosti jako síťový protokol nejčastěji využívá IP (Internet Protocol). Aktuálnímu využití a problematice protokolu IP je věnována právě tato práce.

2 Cíl práce a metodika

Cílem práce je přiblížit kroky vedoucí k výhodám použití IPv6, zmapovat postupy migrace na IPv6 a usnadnit rozhodování o přistoupení k samotné migraci technickému personálu i podnikovému managementu. Dále má tato práce sloužit k vytvoření informačního zdroje, který účinně pomůže při plánování postupu migrace firemního prostředí na IPv6 tím, že přiblíží aktuální stav využití IP protokolu různých firemních sítí, shrnutí informací o podpoře za strany vývojářů operačních systémů a výrobců ICT.

Metodikou k dosažení výše uvedeného cíle je studium odborné literatury, internetových článků, statistik a konzultace s odborníky zabývajícími se danou problematikou v rámci zaměstnavatele a dále pak připojení poznatků získaných vlastní zkušeností.

3 Přehled řešené problematiky

3.1 IP (Internet Protocol)

Internetový protokol (IP) je protokolem síťové vrstvy, obsahující informace o adresování a další řídící informace, umožňující směrování paketů a dokumentován v RFC791. Protokol je primárním protokolem síťové vrstvy sadě internetových protokolů a společně komunikačním přenosovým protokolem TCP představuje základ internetových protokolů.[1]

3.1.1 Vznik, Historie, Vývoj

Internetové protokoly byly představeny uprostřed 70. let, kdy se americká obranná agentura DARPA (Defense Advanced Research Agency) začala zajímat o možnosti paketových sítí, které by usnadnily komunikaci mezi rozdílnými počítačovými systémy ve výzkumných institucích DARPA financovala výzkum na Stanfordově univerzitě s cílem dosáhnout heterogenní konektivity. Výsledek jeho snažení se stal světově nejpopulárnější sadou otevřených protokolů, protože mohou být použity ke komunikaci napříč mnoha propojenými sítěmi a jsou vhodné jak pro komunikaci sítí LAN, tak i WAN.[2]

3.1.2 Funkce / Význam IP v OSI a TCP/IP modelu

S nárůstem složitosti datových sítí se objevila potřeba uspořádat jejich požadavky na hardware, software, komunikační protokoly a různé typy přenosových médií. Za tímto účelem byl vytvořen univerzální síťový referenční model OSI. Model architektury OSI je složen ze sedmi vrstev, které zahrnují určité skupiny komunikačních protokolů. První vrstva popisuje protokoly a normy vztahující se k fyzickému přenosovému médiu (např. optická vedení nebo metalická vedení). Druhá vrstva zahrnuje protokoly linkové vrstvy (nejčastěji Ethernet). Do třetí vrstvy patří protokoly síťové, jako jsou třeba IPv4, IPv6 nebo směrovací protokoly. Čtvrtou vrstvu tvoří protokoly transportní (např. TCP nebo UDP). Pátá je vrstva relační, která zahrnuje protokoly navazující, provozující a ukončující komunikační relace mezi vyššími a nižšími vrstvami OSI modelu. Šestá – prezentační vrstva konvertuje data pro zpracování přenosu mezi aplikační a relační vrstvou. Sedmá vrstva se nazývá aplikační. Ta dokáže zprostředkovat komunikaci mezi uživatelskými

[1] (Jirovský str. 333)
[2] (Jirovský str. 333)

programy a síťovým prostředím. Zahrnuje také protokoly jako jsou Telnet, FTP nebo SMTP. Tento model je zjednodušenou variantou OSI a je tvořen pouze čtyřmi vrstvami. Jsou to vrstva síťového rozhraní, síťová, transportní a aplikační.

Vzhledem k modelům síťové architektury (TCP/IP a OSI) se IP protokol nachází na úrovni síťové vrstvy. Síťová vrstva umožňuje adresování a směrování. Zprostředkovává tak přenos dat mezi jednotlivými segmenty nižších vrstev síťové architektury. Pro úroveň síťové vrstvy je typické využívání aktivních síťových prvků, jako jsou směrovače (pro směrování datových toků), firewally (pro zabezpečení) nebo loadbalancery (pro rovnoměrné rozložení zátěže).

3.1.3 Charakteristika IPv4

IP protokol se nejprve objevil ve verzi 4 (dále jen IPv4). Tak je to v současnosti nejrozšířenější a nejznámější verzí protokolu IP. Jeho typickými vlastnostmi jsou: adresování hodnotami o velikosti 32 bitů, možnost využití řízení kvality služby QoS (Quality of Service), fragmentace paketů na definovanou maximální velikost, ochrana proti zacyklení TTL (Time To Live), uchování informace o protokolu vyšší vrstvy, zabezpečení integrity dat kontrolním součtem.

3.1.4 Výhody IPv4

Zavedení síťového protokolu IPv4 přineslo i jeho typické výhody. Za nejdůležitější považuji tyto:

- Unicast – komunikace mezi jednotlivými hosty
- Broadcast – komunikace ke všem dostupným hostům
- Multicast – komunikace mezi hosty ve specifických skupinách
- Bezpečnost – přenosy dat v zašifrovaném stavu pomoci IPSec
- Fragmentace paketů – umožňuje rozdělení paketů na menší části (fragmenty) pro přizpůsobení paramerům přenosového média
- Proměnlivá délka síťového prefixu VLSM (Variable-Length Subnet Mask) – díky VLSM je možné vhodným plánováním efektivně ušetřit velké množství veřejných IP adres

3.1.5 Nevýhody IPv4

Největší nevýhodou je nedostatečně velký adresní rozsah, který IPv4 poskytuje. Právě tento problém stál za vznikem protokolu IPv6. Pro zabezpečení dat při přenosu přes veřejné segmenty sítě je nutno použít bezpečnostní rozšíření IPSec. Zašifrování dat není základní vlastností IPv4. Směrovače internetové páteře musí spravovat velké směrovací tabulky. To klade velký nárok na hardware páteřních síťových prvků.

3.1.6 Problematika adresního prostoru

Pokud je adresou IPv4 32 bitová hodnota, tak z toho vyplývá, že $\mathbf{2^{32}}$ jedinečných hodnot vytváří **4.294.967.296** unikátních adres. Každá adresa IPv4 je složena ze sekvence čtyř osmibitových částí (oktetů). První oktet rozděluje celkový rozsah do 256-ti bloků po 16.777.216 adresách. Tyto bloky jsou dále rozděleny jednotlivým světovým regionům.

Přidělování adres jednotlivým regionům spravuje organizace Regional Internet Registry (RIR). Regiony tvoří pět částí označených jako AfriNIC (pro Afriku), ARIN (pro USA Kanadu, část Karibiku a Antarktidu), APNIC (pro Asii, Austrálii a Nový Zéland), LACNIC (pro Latinskou Ameriku a část Karibiku) a RIPE NCC (pro Evropu, střední Východ a centrální Asii).

Je třeba zdůraznit, že z celkového počtu IPv4 adres je poměrně výrazná část adresních bloků určena ke zvláštním účelům a není proto možné je přidělovat uživatelům nebo je využít jinak než je učeno standardem. Tyto rozsahy adres zmiňujeme jako tzv. **rezervované** adresy. Konkrétní výčet rezervovaných adres je specifikuje doporučení **RFC5735**, které zároveň určuje, pro jaké účely jsou tyto rozsahy rezervovány. Množství rezervovaných IP adres, tak tvoří 35.078 celých 24 bitových bloků celkového adresního rozsahu a ještě několik menších adresních bloků určených pro speciální účely. Pro využití v síti Internetu, tedy zbývá **219.452** bloků veřejných IP adres z celkového počtu.

Je zřejmé, že současné nároky vytvořené nárůstem počtu uživatelů Internetu jsou skutečně dlouhodobě neudržitelné a proto je třeba se tímto problémem zabývat.

3.1.7 Statistiky využití IPv4 v Evropě

Pro přiblížení aktuální situace využití adresního rozsahu IPv4 jsou v této části práce uvedeny některé statistické údaje vztahujících se k regionu RIPE NCC, do kterého spadá i ČR. V regionu RIPE NCC, bylo ke dni 31. ledna 2014 volných veřejných 15,73 milionů

IPv4 adres. Státy s největším množstvím přidělených veřejných IP adres tvoří: Velká Británie 12%, Rusko 12%, Německo 10%. Při uvážení počtu evropských zemí, které spadají do kompetence RIPE NCC je zřejmé, že v blízké budoucnosti dojde k vyčerpání zbytku adresního rozsahu, kterým RIPE NCC v současnosti disponuje. NIX.CZ umožňuje propojení sítí pomocí protokolu IPv6 svým členům a zákazníkům od roku 2003. V současnosti této možnosti využívá 86 z celkového počtu 117 připojených sítí.

3.1.8 Charakteristika IPv6

V průběhu devadesátých let, začalo být zřejmé, že stávající počet adres protokolu IPv4 nebude dostačovat. Odhady předpovídaly dostatek adres současného IP na dobu zhruba deseti let. Protože se jednalo o relativně dlouhý časový interval, tak se organizace IETF (Internet Engineering Task Force) rozhodla pro návrh nového protokolu, který bude poskytovat výrazně větší adresní rozsah a zároveň poskytne i další užitečné vlastnosti.
Na základě těchto specifikací bylo v roce 1995 vytvořeno doporučení RFC1883 (Internet Protocol, Version 6 Specification), které položilo samotný základ doporučením souvisejícím s aktuální podobou IPv6.

3.1.9 Rozšíření IPv6 a výhody proti IPv4

- Dostatečně rozsáhlý 128 bitový adresní prostor disponuje počtem 2^{128} adres. To umožňuje připojovat větší množství síťových zařízení bez nutnosti překládání adres.
- Autokofigurace adres – Host připojený do sítě IPv6 získává od routeru automaticky nastavení síťových parametrů prostřednictvím zpráv ICMPv6. Je možné také vyžít DHCPv6 nebo ruční nastavení.
- Multicast – Do IPv6 byl doplněn později. Dokáže nahradit broadcast například na místní lince multicastem pro skupinu all-hosts.
- Jumbogramy – Stávající IPv4 umožňuje standardně přenášet pakety do velikosti 64 kB. Novější IPv6 podporuje přenos větších paketů až do velikosti 4GB. To má za následek efektivnější přenos velkých objemů dat bez narůstajících režijních přenosů. Avšak v případě citlivého přenosového média jako WiFi mohou velké pakety a rušení způsobit neprostupnost sítě.

Rozhodujícím faktorem však zůstává nastavení MTU (maximální dovolená velikost přenášených paketů) souvisejících síťových prvků.

- Zabezpečení síťové vrstvy – Šifrování protokolu IPv4 používá jako přídavná vlastnost. U IPv6 se však jedná o vlastnost integrovanou do samotného protokolu. Podle dostupných informací je v současnosti tato náhrada za IPSec využívána především směrovacím protokolem BGP.
- Mobilita – Podpora mobilních zařízení ze strany IPv6 byla dodatečně vytvořena později. Jejím cílem je zajistit dostupnost mobilních zařízení na stále stejné adrese. Toho je dosaženo prostřednictvím směrovače v domácí síti, který vykonává roli domácího agenta (Home Agent). Ten zajistí, aby následně došlo ke změně směrování paketů mezi komunikujícími stanicemi napřímo. V současnosti se tato vlastnost využívá pouze v testovacích prostředích.
- Zrušení CRC – Současná chybovost datových sítí umožňuje vyloučení kontrolního součtu ze struktury IP paketu. Přenášená data tak nezatěžují síťové prvky přepočítáváním CRC při každém průchodu síťovým zařízením.

3.1.10 Nevýhody a chyby IPv6

Mezi nevýhody by bylo možné zařadit nárůst přenosů režijních dat, který souvisí s rozšířením počtu adresních bitů IPv6 paketu. To je však spíše problém sítí s nízkou datovou propustností.

Obsah adresy s délkou 128 bitů se stává pro člověka hůře zapamatovatelným. Tento problém se však týká především síťových administrátorů. Z tohoto důvodu je nutno při provozu IPv6 více využívat záznamů DNS.

Objevuje se jisté riziko napadení sítě v okamžiku, kdy případný útočník začne do sítě vysílat falešné zprávy router advertisement.

3.1.11 Současný stav využití IPv4/IPv6

V současnosti je rozšíření IPv4 stoprocentní v celém rozsahu Internetu. Zatímco IPv6 používají řádově jednotky procent všech uživatelů internetu na celém světě. V Evropském měřítku uživatelé IPv6 tvoří přibližně 2,5%. V České republice byl za první polovinu roku 2013 zaznamenán nárůst až na 27%. Takový počet uživatelů internetu tvoří 2,12% ze

všech uživatelů na světě. ČR se tak dostala na desáté místo ve světovém žebříčku. Z dostupných statistických údajů je patrný neustálý nárůst použití IPv6.

3.2 Migrace IPv4 na IPv6

Řešením problematiky nedostatku veřejných IP adres je to, že se IPv6 začne používat jako běžný provozní protokol síťové vrstvy. Při návrhu síťové struktury je důležité zohlednit využití IPv6 buďto přímo při výstavbě sítě, nebo alespoň pro budoucí migraci ze stávajícího IPv4. V případě migrace ze stávajícího IPv4 je nutno zvažovat způsoby provedení a vhodné naplánování samotného přechodu k IPv6.

3.2.1 Důvody migrace

Hlavním důvodem, proč migrovat na IPv6 je již zmiňovaný nedostatek adres stávajícího protokolu IPv4. Další důvody k migraci přinášejí vlastnosti, které jsou přímo součástí IPv6, jako jsou: zabezpečení, řízení šířky pásma, podpora mobility, efektivnější přenosy dat prostřednictvím navýšení maximální velikosti paketů. Migraci na IPv6 si může také vynutit vnější prostředí, jako jsou třeba: obchodní partneři, technologická vybavenost poskytovatele konektivity, obchodní politika a technická podpora výrobců ICT. Možnost vyžívat IPv6 pro připojení obchodních partnerů nebo zákazníků zvyšuje technickou flexibilitu samotného podniku a dokazuje tak schopnost reagovat na požadavky vyvíjejícího se trhu. To následně zvyšuje konkurenceschopnost a rozšiřuje i obchodní příležitosti podniku.

3.2.2 Technická způsobilost a podpora IPv6

Protože se v případě IPv6 jedná o poměrně málo rozšířený síťový protokol, je třeba si uvědomit, že jeho využití závisí mimo jiné i na podpoře výrobců síťové technologie a vývojářů operačních systémů. K tomuto důležitému aspektu je nutné přihlédnout při nákupu nové ICT technologie i při investicích do rekonstrukcí stávajících prvků výpočetní techniky.

3.2.3 Podpora IPv6 u aktivních prvků síťové struktury

Je zřejmé, že pokud budeme uvažovat o IPv6 jako síťovém protokolu je musíme vyžadovat jeho plnou podporu v aktivních prvcích síťové struktury. U aktivních prvků sítě je vhodné posuzovat podporu protokolů IPv4 i IPv6 současně v jedné síti. Zprovoznění obou protokolů IP, tak umožňuje uživatelům využít vlastnost zvanou DS (Dual-stack). Zejména je vhodné se zaměřit na směrovací protokoly, možnosti překladů adres a podporu tunelovacích mechanismů.

3.2.4 Směrovací protokoly podporující IPv6

Rozvoj IPv6 byl do této doby příčinou vzniku celé řady nových protokolů nebo modifikací stávajících. Důležitou část těchto protokolů tvoří směrovací protokoly. V oblasti směrovacích protokolů došlo k rozšíření k dosažení možnosti směrování IPv6.

- RIPng – Routing Information Protocol next generation je rozšířením předchozího RIPv2. Byl vyvinut především pro podporu IPv6. RIP ve všech verzích je historicky omezen na maximální počet uzlů 15. Jeho popis je obsahem doporučení RFC 2080.
- OSPFv3 – Je určen přímo pro směrování IPv6 prefixů. Byl specifikován doporučením RFC 2740.
- BGP – Protokol BGP byl pouze rozšířen (RFC 2858) o schopnost pracovat s IPv6 prefixy (address family).
- EIGRP – Enhanced Interior Gateway Routing Protocol vyvinula společnost Cisco systems a je ho možné využívat pouze v souvislosti s technologií tohoto výrobce. Jedná se o jeden z nejpropracovanějších dynamických směrovacích protokolů, který také získal rozšíření pro podporu IPv6.

3.2.5 DNS (Domain Name System)

DNS je službou sítě. Pro funkčnost datových přenosů není aktivita této služby nezbytně nutná. Je to služba, která zajišťuje překlady jmenných adres na IP adresy. O DNS lze tvrdit, že vznikla pro usnadnění práce uživatelů a personálu technické podpory. DNS uživatelům umožňuje zadávat adresy požadovaných síťových služeb prostřednictvím slovních adres. (např. www.seznam.cz). Překlady adres jsou prováděny na základě záznamů v seznamu překladů. Vzhledem k velikosti adres IPv6, které jsou pro člověka

hůře zapamatovatelné než adresy IPv4, je zřejmé, že význam DNS v souvislosti IPv6 narůstá.

Z pohledu sítě je možné rozdělit problematiku DNS na dvě části:

- Nejprve je důležité, aby DNS dokázat poskytnout adresy obou IP protokolů. Proto je nutné, rozšířit záznamy o adresy IPv6 (tzv. záznamy typu AAAA).
- Druhým úkolem je zpřístupnit DNS systém prostřednictvím obou IP protokolů. To závisí na využívané síťové technologii, použitém operačním systému serveru DNS a programovém vybavení.

Aktuální a funkční podobu specifikuje doporučení RFC3596.

3.3 Mechanismy podporující migraci firemního prostředí

Jestliže jsou součástí firemní sítě prvky nepodporující IPv6, nejčastěji to bývají zastaralé operační systémy pracovních stanic, tak je možné využít některý z mechanismů vyvinutých právě pro takovou situaci. Na správném posouzení technických možností každé konkrétní sítě závisí volba některého z možných řešení nebo jejich kombinace. Jedním z důležitých kritérií při volbě správného mechanismu je posouzení technických možností připojení od současného poskytovatele konektivity do Internetu.

3.3.1 Tunneling

Tunelování umožňuje přenášet data jedné verze IP prostřednictvím zapouzdření do druhé a naopak. Slouží hlavně pro podporu uživatelů, kteří nejsou schopni využít vlastnosti Dual-stack a jsou tak odkázáni na pouze na jednu verzi IP protokolu. Tunelování IP paketů je možno realizovat několika způsoby.

Dual-stack Lite

DS Lite(Dual-stack Lite) je jedním z tunelovacích mechanismů. Tohoto tunelovacího mechanismus je vhodné využít v situaci, kdy je konektivita poskytovatele připojení k Internetu na IPv6. Využití DS Lite otevírá koncovým uživatelům možnost využít obou verzí IP protokolu. Hlavní myšlenkou DS Lite je tunelovat IPv4 provoz přes prostředí ISP které je vytvořeno ve verzi IPv6. Je zřejmé, že pokud koncový uživatel disponuje technologií s podporou IPv6, tak se jedná o přímou datovou komunikaci čistě ve verzi

IPv6. Většina firemních a domácích sítí využívá pro vnitřní adresaci privátních rozsahů adres IPv4. V tomto případě je nutné, aby směrovač na hranici privátní sítě (také označován jako B4 – Basic Bridging Broad Band) a sítě poskytovatele dokázal zapouzdřit pakety IPv4 do paketů IPv6. Takto zabalené pakety jsou následně doručeny na směrovač poskytovatele, který disponuje připojením i veřejnými adresami IPv4. Na tomto směrovači pak dochází prostřednictvím NAT k překladu na veřejnou adresu IPv4 a používá se pro něj označení AFTR (Adress Family Transition Router). Právě IPv6 adresu AFTR musí hraniční směrovač zákazníka znát, aby tunelování mohlo proběhnout správně. Adresu AFTR takový směrovač získá z ruční konfigurace od administrátora sítě nebo dynamicky od poskytovatele prostřednictvím DHCPv6. Zprávy DHCPv6 obsahují parametry pro nastavení Dual-Stack Lite.

Jako každý tunelovací mechanismus, i dual-stack lite má problémy s velikostí datagramů a fragmentací. Autoři doporučují, aby MTU páteřní sítě bylo alespoň o 40 B větší než MTU koncových sítí a k fragmentaci pokud možno nedocházelo. Není-li vyhnutí, musí fragmentace proběhnout na úrovni obalujícího IPv6, tunelované IPv4 datagramy musí zůstat v původní podobě. Pro přímou komunikaci AFTR s B4 po IPv4 vyhradila IANA adresní rozsah 192.0.0.0/29, přičemž standardní adresou AFTR je 192.0.0.1 a B4 rozhraní 192.0.0.2. Mají všichni stejnou, protože IPv4 provoz je beztak tunelován, takže k rozlišení jednotlivých B4 poslouží jejich IPv6 adresy.[3]

Z myšlenky DS Lite je zřejmé, že před jeho nasazením musí uživatel vyžadovat ze strany poskytovatele připojení alespoň minimální podporu a spolupráci.

6to4 tunneling

Pakety IPv6 jsou zapouzdřeny do paketů IPv4 na hraničním routeru. V takovém případě je možno přenášet pakety IPv6 po síti, která je původně vybudována na IPv4. V současnosti se tak jedná o nejpoužívanější typ smíšené kombinace sítě.

Alarmující je jeho špatná spolehlivost – podle měření, která prováděl Geoff Huston či RIPE NCC, se kolem 10 až 15 % požadavků přicházejících na servery po 6to4 nedočká odpovědi.[4]

[3] (Satrapa, 2012 str. 273)
[4] (Satrapa, 2012 str. 261)

6over4

Tento způsob umožňuje přenos paketů IPv6 v síti IPv4. Nejvhodnější použití 6over4 je v případě IPv6 klientů izolovaných v síti IPv4. Funguje tak, že se na klientské stanici vytvoří virtuální interface IPv6. Z adres IPv6 jsou pak vytvořeny adresy IPv4, které jsou dále využity standardním způsobem pro přenos v síti IPv4. Dále je třeba, aby daná IPv4 síť podporovala šíření multicastů pro komunikaci 6over4 klientů a 6over4 směrovačů prostřednictvím IPv4. Nevýhodou je, že tento způsob není příliš podporován ze strany vývojářů operačních systémů a před zavedením tohoto způsobu při migraci je nutno zjistit zda je dostupná potřebná technická vybavenost všech zařízení, která 6over4 budou využívat.

6rd

Rapid Deploy (6rd) je odvozena od metody 6to4. Tento mechanismus umožňuje poskytovatelům připojení nabízet zákazníkům IPv6 i přesto, že jejich páteřní síť je nativně IPv4. Adresy IPv6 které používá 6rd v sobě nesou i adresy IPv4 přenášeného paketu (obvykle adresa zákazníkova směrovače). Takto zapouzdřené pakety jsou dále přenášeny na překladový směrovač poskytovatele a ten musí být připojen do Internetu IPv6. Moderními poskytovateli je 6rd často používán pro jeho rychlé a poměrně nenákladné nasazení.

ISATAP

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) slouží pro přenos IPv6 přes strukturu sítě IPv4 a pracuje obdobně jako 6over4. ISATAP je určen především pro privátní sítě. Podle přesného postupu vytváří IPv4 adresy pro možnost směrování v prostředí sítě IPv4. Na rozdíl od 6over4 nevyužívá IPv4 multicast pro zjištění ISATAP směrovačů v síti. Směrovač ISATAP by měl mít nativní připojení do sítí obou verzí IP. Seznam možných směrovačů je nakonfigurován v seznamu PRL (Potential Router List). Průběžně jsou směrovače uvedené v seznamu dotazovány zprávou RDM (Router Discovery Message). Tak je možné zjistit, který směrovač je možné požívat a prostřednictvím zprávy pro automatické nastavení získat prefixy pro sestavení IP adresy. Protože nejsou využívány skupinove adresy (multicasty), tak se konfigurace ISATAP provádí ručně nebo prostřednictvím DNS. V tabulce pro překlad adres DNS serveru je pro

automatickou konfiguraci vytvořit záznam pro jméno *isatap*, který bude odkazovat na IP adresy ISTAP směrovačů.

Teredo tunneling

Další automatický mechanismus tunelování v síti IPv4. Využívá automatického nastavení prostřednictvím Teredo serveru. Je vhodný pro použití v sítích za překladem adres NAT (Network Address Translation). Komunikace je rozdělena do rolí na klienty a server. Klientské stanice v síti IPv4 za NATem se zaregistrují na Teredo server (např. teredo.nic.cz) a ten následně vytvoří následně vazbu mezi adresou IPv6 a příslušnou adresou IPv4 plus portem. Na tuto adresu a port je třeba směrovat další datový provoz. Klientské stanice musí mít nainstalovaný operační systém s podporou teredo tunelů. Na straně teredo klientů je třeba nastavit adresu Teredo serveru, aby mohlo dojít k úspěšnému navazování tunelů. Už z tohoto je zřejmé, že teredo server musí být připojen do Internetu prostřednictvím IPv4 i IPv6. Jeho specifikace je dána doporučením RFC4380.

3.3.2 Překlady IP adres (IP/ICMP Translation Algorithm)

Pro přechod k IPv6 je vedle tunelovacích mechanismů možno využít také několik technik překládání adres. V případě překladu adres je důležité pro všechny techniky překladů zachovat stejný algoritmus mapování IP adres. Stejný algoritmus v tomto případě zajišťuje vzájemnou kompatibilitu mezi jednotlivými technikami. Pravidla pro překlady adres jsou specifikována v doporučení RFC6145 (Stateless IP/ICMP Translation Algorithm - *SIIT*).

Překládání IPv4 je poměrně snadné a spočívá v jednoduchém přidělení IPv6 adresy ke každé překládané IPv4 adrese. Pokud však jde o opačný překlad, je nutno se vypořádat s výrazně větším adresním rozsahem. Tento problém je však vyřešen dynamickým mapováním adres NAT v poměru 1:n, kde na jednu adresy IPv4 připadá několik adres IPv6, nebo v poměru m:n, kde na malé množství adres IPv4 je mapováno větší množství adres IPv6.

NAT64 / 46

Nejedná se o mechanismus tunelování paketů, ale o překlad adres mezi verzemi IP. Tímto mechanismem je možné zpřístupnit zdroje dat v sítích IPv4 pro hosty připojené v sítích IPv6. V případě NAT64 dochází k překládání IPv6 adres na adresy IPv4. Samotný překlad

provádí směrovač na rozhraní sítí obou verzí IP protokolů. NAT64 vytváří překladovou tabulku. Překladová tabulka obsahuje informaci o vazbě mezi adresou IPv6 a adresou IPv4 s příslušným číslem portu. Pro navázání zpětné komunikace je nutné vytvářet statické záznamy v překladové tabulce. Přesný popis NAT64 je předmětem doporučení RFC6146. Stejným způsobem je možné využít opačného překladu NAT46 pro zpřístupnění cílových stanic v internetu na IPv6.

CGNAT

V případě nedostatku adres IPv4 je možno využít mechanismu CGNAT (Crrier-grade Network Address Translation). Tento mechanismus nijak nevyužívá IPv6, ale jen rozšiřuje adresní prostor veřejných adres přidělovaný uživatelům. Výsledkem použití CGNAT je situace, kdy několik uživatelů využívá jednu veřejnou adresu. Pokud je CGNAT nastaven pro poměr 512:1 znamená to, že jednu veřejnou adresu teoreticky využívá 512 uživatelů. Pro vnější prostředí se jednotlivý uživatelé za jednou veřejnou IP adresou odlišují pouze číslem portu transportního protokolu. Čísla portu transportního protokolu jsou obvykle přidělována dynamicky, z čehož vyplývá, že není garantována statická vazba mezi IP adresou a portem. To komplikuje dostupnost uživatelů za CGNAT ze strany Internetu. V souvislosti s migrací na IPv6 je možné CGNAT využít k získání času pro její plánování a přípravu. Samotný přechod na IPv6 mechanismus překladu adres CGNAT nijak přímo neřeší.

3.4 Migrace firemního prostředí

Ke zprovoznění IPv6 v podnikové síti leze přistupovat několika možnými způsoby:

- Je možné celou záležitost s migrací ignorovat a nedělat nic a čekat, co udělají konkurenční podniky.
- Možností jak problém nedostatku adres IPv4 je rozšíření stávajícího adresního prostoru. Je možné využívat překladu adres NAT, nebo přikoupit některý ze zbývajících adresních rozsahů IPv4 dostupných na trhu.
- Zprovoznění IPv6 je v současnosti optimální a zodpovědný přístup k řešení celkové problematiky IPv4. Využitím metody Dual-stack je možné v jedné síti provozovat obě verze IP protokolu zároveň. V podstatě je metoda Dual-stack

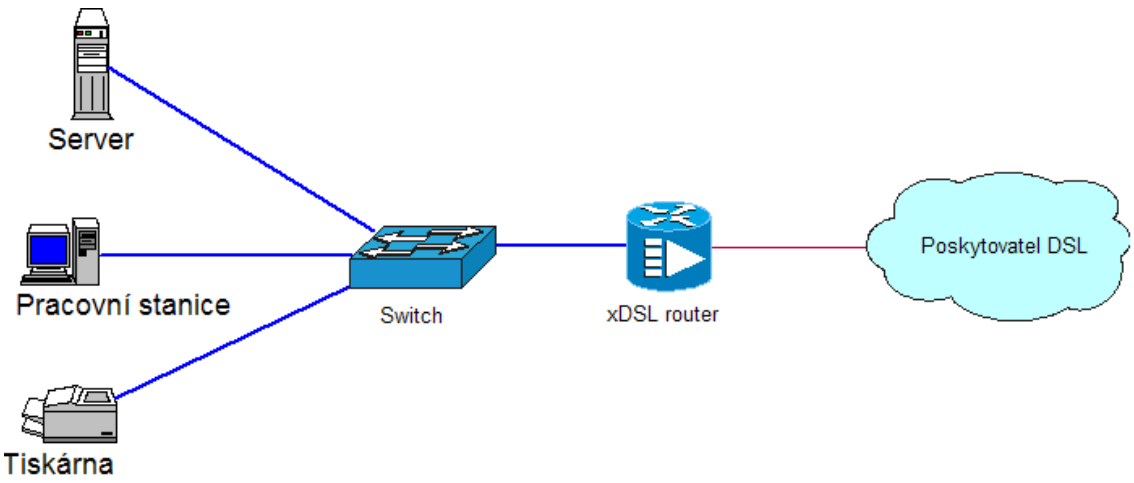
rozšířením stávající sítě do stavu, ve kterém může síť dlouhodobě fungovat nezávisle na podpoře IPv6 ze strany uživatelů.

Velký vliv na migraci firemní sítě má složení a technické možnosti všech prvků, které tvoří příslušnou síť. Skladba využívaných elementů sítě je závislá na tom k jakému účelu má daná počítačová síť sloužit. Podle účelu jsem rozdělil firemní sítě do několika skupin (středně velká firma, poskytovatel připojení, datacentrum a domácí síť).

3.4.1 Definice sítě firemního prostředí

Prostředí počítačové sítě je součástí celkového podnikového informačního systému firmy, který slouží k efektivnímu sdílení informací a vzájemné komunikaci uvnitř i mimo firmu. Typickými službami, které využívají datovou síť, jsou HTTP (Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Potocol), VoIP (Voice over IP), FTP (File Transfer Protocol), databázové služby. Služby běžné firemní sítě jsou realizovány na zařízeních, jako jsou servery, síťové tiskárny, IP telefony nebo scannery. Všechna uvedená zařízení využívají ke komunikaci síťový protokol IP a je tedy důležité je uvažovat jako zařízení, kterých se týká migrace na síťový protokol IPv6. Kromě koncových síťových zařízení se migrace vztahuje i na aktivní síťové prvky (směrovače, firewally). Před započetím migrace je důležité zjistit u všech zařízení a aplikací, zda jsou schopny komunikovat prostřednictvím IPv6. Podpora IPv6 je důležitá především ze strany vývojářů operačních systémů a výrobců aktivních síťových prvků. Běžné firemní sítě využívají pro připojení do Internetu některou z fixních služeb nabízených poskytovateli konektivity.

3.4.2 *Příklad topologie firemní sítě*



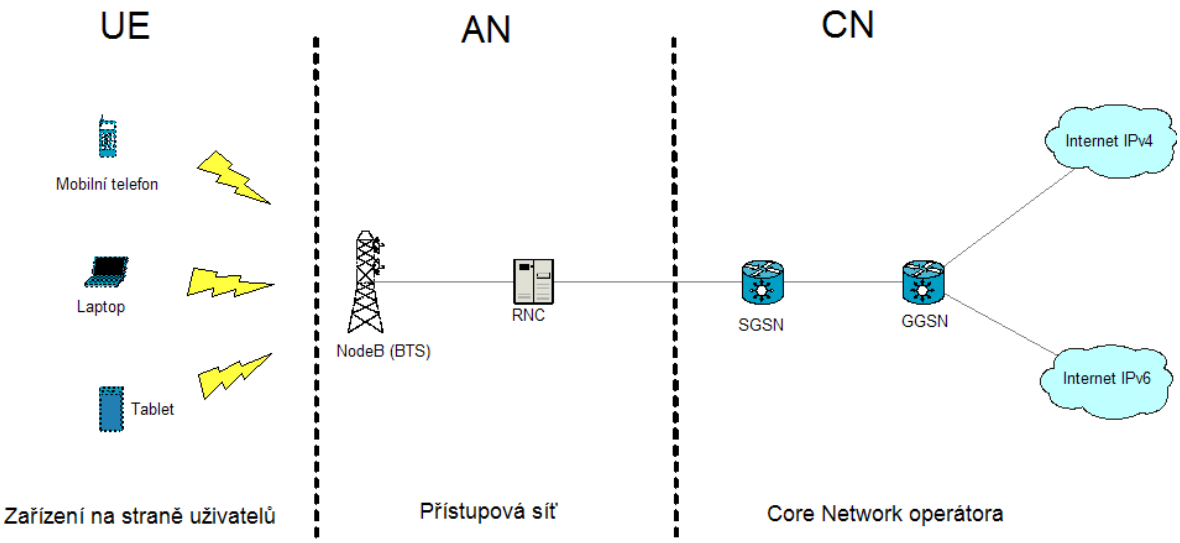
3.5 Migrace ISP

Nedostatek IP adres aktuálně nejvyužívanějšího IPv4 se zásadně dotýká poskytovatelů konektivity do internetu, jejich obchodních partnerů i jejich zákazníků. Většina uživatelů Internetu je závislá na způsobu připojení jejich poskytovatelů. ISP tak tvoří jeden z nejdůležitějších článků podpory globální migrace na IPv6. V současné době je možné využít různých druhů připojení lišících se především mobilitou a přenosovými rychlostmi. Mezi nejčastěji používané služby, kterých se týká migrace protokolu IP, patří mobilní služby (GPRS, UMTS, CDMA, LTE) a fixní služby (DSL, FTTX).

3.5.1 Mobilní internet (GPRS, UMTS, LTE)

Technologie, která tvoří nejčastější typy mobilního připojení, se dá logicky rozdělit do tří částí. První část tvoří mobilní terminály MS (Mobile Station). Zahrnuje uživatelská zařízení, která jsou na straně uživatele (telefony, tablety, mobilní modemy). Druhá část je přístupová síť AN (Access Network). Je to část na straně ISP a zajišťuje kvalitu a geografický rozsah pokrytí službou. Tuto část tvoří obvykle radiové vysílače a přenosová síť. Třetí část CN (Core Network) je také na straně ISP a zprostředkovává uživatelům ověření, přihlášení ke službě, přidělení parametrů služby, účtování, řídí uživateli mobilitu mezi vysílači a zprostředkovává přeposílání dat mezi uživatelem a Internetem. Migrace protokolu IP se týká pouze dvou částí celkové struktury, protože AN nevyužívá protokolu síťové vrstvy pro přenos dat k uživateli. Pro úspěšnou migraci je důležité, aby mobilní terminál dokázal pracovat s IPv6 nebo v režimu Dual-stack. Ve třetí části struktury provozovatele mobilního internetu CN se nacházejí dvě zásadní komponenty, na kterých závisí dostupnost internetových služeb po IPv6. Jednou je SGSN (Serving GPRS Support Node) a druhou je GGSN(Gateway GPRS Support Node). Zjednodušeně lze říci, že SGSN ověřuje uživatele při jeho přihlášení, řídí předávání datových toků do geografických lokalit podle potřeby uživatele a přeposílá uživatelská data do GGSN. Bránu z části mobilní struktury tvoří GGSN, která je připojena přímo do internetu. Pro migraci je nutné, aby právě GGSN byla připojena k internetu prostřednictví IPv4 i IPv6.

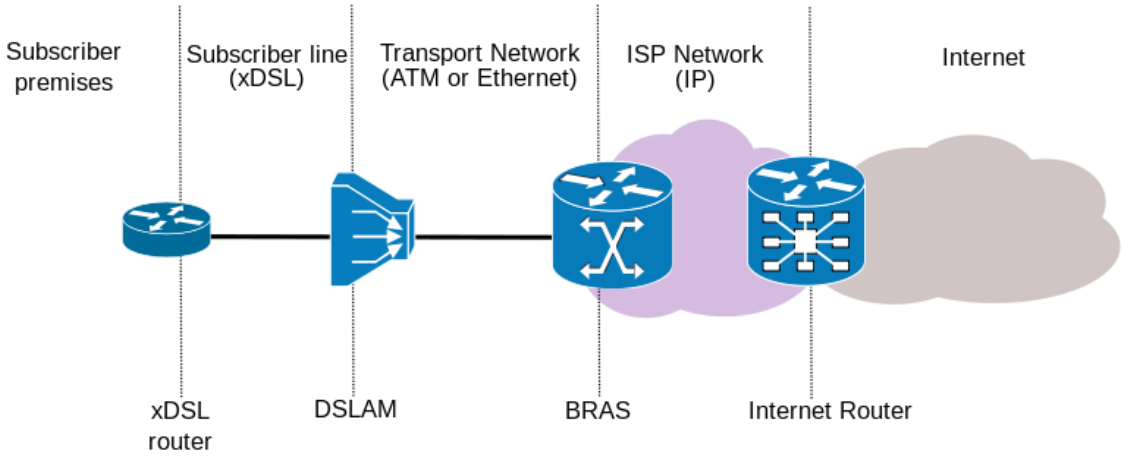
3.5.2 *Stručný přehled struktury mobilního Internetu*



3.5.3 DSL

Služba DSL (Digital Subscriber Line) zpřístupňuje uživatelům připojení k Internetu prostřednictvím metalických spojů. Tyto spoje byly původně využívány pro připojení telefonů k veřejné telefonní síti. Pro své technické parametry (přenosovou rychlost a dostupnost v osídlených lokalitách) je DSL jednou z nejrozšířenějších služeb pro připojení uživatelů k Internetu. Nejčastěji využívaným typem DSL je ADSL (Asymetric Digital Subscriber Line). Pro ADSL je typický rozdíl mezi přenosovou rychlostí směrem k uživateli a směrem od uživatele, který bývá obvykle výrazně nižší. Modulace nosného signálu pro datový přenos ADSL umožňuje jednu metalickou linku využívat současně pro hlas i data, aniž by se vzájemně rušila. Oddělení obou typů komunikací je na koncích linky zajištěno frekvenčními splittery. Konkrétní přenosové parametry DSL linky závisí na kvalitě a délce fyzického média. Protějšek zákaznického zařízení (modemu, xDSL routeru) na straně ISP tvoří DSLAM (Digital Subscriber Line Access Multiplexer).

3.5.4 *Obecné schéma technologie DSL*[5]



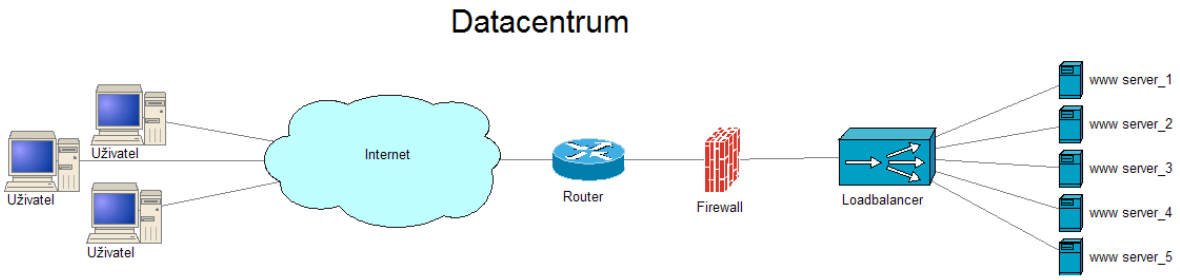
Technologie DSL využívá síťovou vrstvu na koncových zařízeních u zákazníka, na BRAS (Broadband Remote Access Server) na straně ISP. BRAS ve spolupráci se severem RADIUS (*Remote Authentication Dial In User Service*) přiděluje uživatelům IP adresy. Pro využití IPv6 ve službě ADSL je tedy nutná podpora DSL modemu (routeru), BRAS a RADIUS serveru.

3.5.5 Datacentra (Serverhousing, Serverhosting)

Důležitou součástí struktury Internetu jsou servery, na kterých jsou provozovány internetové služby. Servery se obvykle instalují do technologických sálů datacenter. Provozovatelé datacenter mimo jiných služeb svým klientům poskytují především konektivitu do Internetu. Pro nejefektivnější využití IPv6 je důležité, aby servery se službami byly dostupné právě na tomto protokolu. Nedostupnost internetových služeb na IPv6 by mohla bránit migraci jejích uživatelů nebo vést k jejich nedostupnosti. Pro doplnění technických informací zde zmiňuji, že migrace v případě datacentra se týká síťových prvků (směrovčů, firewallů, loadballancerů) a serverů samotných. U severů je nutná podpora operačních systémů, virtuálních serverů a DNS.

[5] (Ludovic.ferre, 2010)

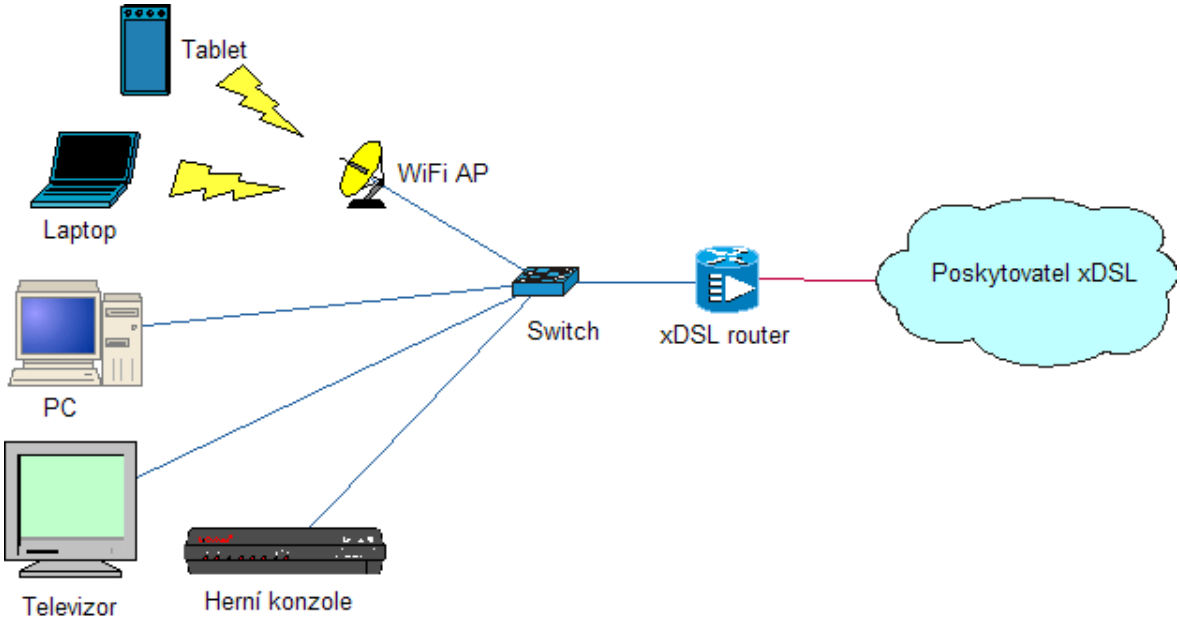
3.5.6 *Příklad sítě pro datacentrum*



3.6 Migrace SOHO (Small Office Home Office)

Prostředí domácí sítě nebo malé kanecláře se často označují jako SOHO. Síť tohoto typu je součástí téměř každé moderní domácnosti. Domácí počítačové sítě nejčastěji slouží k elektronické korespondenci, hraní počítačových her, sdílení souborů v Internetu, telefonování a studiu. Konektivita do Internetu bývá realizována nejčastěji prostřednictvím služby DSL nebo WiFi.

3.6.1 *Přehledové schéma sítě typu SOHO*



4 PRAKTICKÁ ČÁST

4.4 Firemní prostředí

Pokud začneme uvažovat o migraci firemní sítě na IPv6, tak si musíme uvědomit, jakých prvků sítě se migrace bude týkat, jaký bude mít vliv na uživatele a jaké kroky je nutné udělat pro dosažení zprovoznění IPv6 v rámci firemní sítě. Především je třeba se zaměřit na prvky síťové vrstvy OSI modelu (pracovní stanice, servery, směrovače a firewally). A u těchto prvků zjistit do jaké míry podporují IPv6 případně některý z migračních postupů.

4.4.1 Pracovní stanice a servery

Pracovní stanice jsou jednou z nejdůležitějších částí podnikové sítě. Svým pracovním prostředím a síťovou konektivitou vytvářejí nástroj pro tvorbu, úpravu a sdílení dat v rámci podnikového prostředí. Součástí každé běžné funkční pracovní stanice je OS (Operating System), který dokáže zprostředkovat také síťovou komunikaci. Běžnou součástí podnikové síťové struktury jsou i servery poskytující síťové služby. Nejčastěji vyžívané služby podnikových serverů jsou server elektronické pošty, sdílené datové úložiště (SMB, FTP), HTTP server nebo databázový server. Důležitou službou pro podporu síťové komunikace je DNS. Tato služba poskytuje převod jmenných adres na IP adresy. V případě IPv6 hovoříme o záznamech typu AAAA. Rozšíření DNS pro podporu IPv6 je specifikováno standardem RFC3596. Pro využívání IPv6 je tedy nutná podpora ze strany DNS. Schopnost serverů poskytovat síťové služby prostřednictvím IPv6 závisí stejně jako u pracovních stanic na jejich OS. Podpora IPv6 na straně OS je tedy nutným předpokladem k jeho využití. V oblasti operačních systémů tvoří nejdůležitější skupinu uživatelé systémů MS Windows, LINUX, MAC OS. Každý ze zmíněných OS v současnosti plně podporuje IPv6. Některé OS však nutnou podporu IPv6 nabízí až od určité verze.

4.4.2 *Přehled nejběžnějších OS podporujících IPv6:*

Operační systém:	**IPv6 od verze:**
MS Windows	Vista
MAC OS	10.7 (Lion)
Fedora	13
FreeBSD	9.0
Solaris	10

V okamžiku, kdy se na všech pracovních stanicích a serverech nacházejí OS s podporou IPv6 je možné tvrdit, že jedna z nejdůležitějších podmínek migrace je splněna. V současnosti je stále jedním z nejpoužívanějších OS na pracovních stanicích systém Windows XP, který podporuje IPv6 jen částečně. Systém Windows XP se nedokáže dotazovat DNS serveru, který je dostupný pouze na IPv6adrese.

4.4.3 Síť

Na straně sítě je nejprve třeba analyzovat využité aktivní prvky sítě pracujících na síťové vrstvě. Analýzu je třeba provést do té míry, aby z výsledků bylo zřejmé, zda všechny související síťové elementy jsou schopny poskytnout datové přenosy prostřednictvím IPv6. Renomovaní výrobci (Juniper, HP, Cisco Systems) se snaží udržet krok s konkurenčními produkty. To má za následek, že není v současnosti problém jejich technologii nakonfigurovat tak, aby mohl přenášet data obou verzí IP. Součástí analýzy síťových prvků by mělo být i zjištění, jaké tunelovací nebo překladové algoritmy máme k dispozici. Na základě toho můžeme plánovat použití vhodného migračního postupu.

Po analýze na straně vlastní podnikové sítě je třeba zohlednit podmínky vnějšího prostředí sítě. Zvlášť důležitá je podpora od poskytovatele připojení k vnějšímu prostředí a technické požadavky obchodních partnerů, kteří mohou využívat některou naši síťovou službu (FTP, HTTPS).

Příklad 1

Pro představu zde uvádím příklad postupu ruční konfigurace IPv6 na směrovači Cisco 2651XM:

První krok - *Povolení přeposílání paketů IPv6:*

Router(config)#**ipv6 unicast-routing**

Druhý krok - *Povolení IPv6 a nastavení adresy na rozhraní:*

Router(config-if)#**ipv6 enable**

Router(config-if)# **ipv6 address FDF5:3C82:F07F:F005::/64 eui-64**

Třetí krok - *Pro rychlé zpracování paketů ve směrovači Cisco je vhodné aktivovat CEF (Cisco Express Forwarding):*

Router(config)#**ip cef**

Router(config)#**ipv6 cef**

Abychom zajistili, že všechny sítě nakonfigurované na našem směrovači budou dostupné i pro okolní síťové prostředí je třeba povolit jejich směrování prostřednictvím některého z routovacích protokolů (OSPFv3, RIPng).

Čtvrtý krok – *Aktivace routovacího protokolu OSPF jako instance číslo 1:*

Router(config)#**ipv6 router 1**

Router(config-rtr)#**redistribute connected**

Příklad 2

Postup konfigurace IPv6 na směrovači H3C MSR30-40 (Comware Software, Version 5.20)

První krok – aktivace přeposílání paketů IPv6:

[TEST-ACS] **ipv6 nd hop-limit 0**

[TEST-ACS]**ipv6**

Druhý krok - *Povolení IPv6 a nastavení adresy na rozhraní:*

[TEST-ACS-GigabitEthernet0/1] **ipv6 address FDF5:3C82:F07F:F002::/64 eui-64**

Třetí krok – *Nastavení statického směrování prefixu sítě IPv6:*

[TEST-ACS]**ipv6 route-static 2A00:1028:F:: 48 GigabitEthernet0/0**
FE80::219:AAFF:FEFB:36BF

Čtvrtý krok – *Aktivace směrovacích protokolů OSPF a RIPng jako instance číslo 1:*

[TEST-ACS]**ripng 1**

[TEST-ACS] **ospfv3 1**

4.4.4 *Přehled nejběžnějších síťových prvků s podporou IPv6:*

Výrobce:	Podpora IPv6 od verze:
Cisco Systems	IOS 12.2(2)
HP Commware	5.2
Juniper	JUNOS 12.2

Cílem migrace firemního prostředí by mělo být zprovoznění sítě s podporou obou verzí IP. To má nejmenší dopad na samotné uživatele, protože je možné připojovat do sítě pracovní stanice a servery nezávisle na jejich podpoře protokolu IP. Pokud se správci dané sítě podaří docílit tohoto stavu, tak se v budoucnu nebude setkávat s problematikou nedostatku IP adres. Takto připravená síť umožňuje koexistenci obou síťových protokolů zároveň na několik let dopředu.

4.5 Sítě ISP

4.5.1 Mobilní Internet

V České republice podle předběžných údajů na konci roku 2012 bylo 13,5 milionu aktivních SIM karet. Uvedl to ***Český telekomunikační úřad*** *ve své čerstvě vydané výroční zprávě za rok 2012.*[6]

Rozvoj v oblasti mobilních telefonů přinesl mobilní terminály vybavené operačním systémem nazývané smartphony. Největší zastoupení v řadách běžných uživatelů mají vývojáři mobilních operačních systémů společnosti Apple (iOS), Microsoft (Windows Mobile) a Google (Android). V současné době nejčastěji záleží na verzi mobilního operačního systému a službách povolených na zařízení přímo výrobcem. Tato regionální nastavení ze strany výrobců jsou často vyžádány ze strany mobilních operátorů z důvodu optimalizace mobilních terminálů příslušnému prostředí. Většina mobilních terminálů dodávaných na trh v ČR nemá povoleno používání IPv6 i přesto, že samotné zařízení i jeho OS IPv6 je schopno plně využívat. Jde o softwarovou úpravu ze strany výrobce uživatelských terminálů. Pravděpodobně by se mohlo jednat o již zmíněné technické opatření, které zabrání šíření režijních dat souvisejících čistě s IPv6 v mobilních sítích které podporují pouze IPv4. Tímto opatřením dochází k úspoře přenosového pásma. Mobilní terminály s operačním systémem umožňují uživatelům využívat široké spektrum aplikací a internetových služeb. Tato výhoda má za následek narůstající poptávku po terminálech s OS.

[6] (Macich, 2013)

4.5.2 *Prodeje mobilních telefonů podle operačního systému ve čtvrtém čtvrtletí 2013 (v milionech kusů)*[7]

OS	Kusů 4Q12	Kusů 4Q13	Podíl 4Q12	Podíl 4Q13	4Q13/4Q12 Změna
Android	161,1	226,1	70,3 %	78,1 %	40,3 %
iOS	47,8	51	20,9 %	17,6 %	6,7 %
Windows Phone	6	8,8	2,6 %	3 %	46,7 %
BlackBerry	7,4	1,7	3,2 %	0,6 %	-77 %
Ostatní	7,4	2	2,9 %	0,7 %	-70,1 %
Celkem	**229**	**289,6**	**100 %**	**100 %**	**26,5 %**

U mobilních terminálů s operačními systémy je podobně jako u pracovních stanic nutno vědět od jaké verze je IPv6 podporován.

4.5.3 *Přehled nejběžnějších mobilních OS podporujících IPv6:*

Operační systém:	**IPv6 od verze:**
Android	4.2 (Jelly Bean)
Apple iOS	4.1
Windows Phone	6.5
Symbian	7.0

Síťová struktura CN (Core Network) současných ISP v ČR umožňuje migraci na IPv6 pouze na základě provedení konfiguračních změn. V tomto stavu není nutná žádná investice do technologie ze strany ISP pro samotné provedení migrace. V okamžiku migrace je však nutné, aby ISP měl k dispozici dostatek vyškoleného personálu, který dokáže vyřešit případné problémy na straně zákaznického servisu. Operátoři mobilních datových služeb v ČR aktuálně disponují dostatečným množstvím veřejných adres IPv4,

[7] (Buchta, 2014)

aby se nemuseli potýkat s jejich nedostatkem. Výraznou úsporu veřejných adres IPv4 přineslo využití mechanismu pro překládání adres CGNAT.

4.5.4 DSL

Služba DSL je v ČR nečastějším typem fixního připojení k Internetu. S počtem 1,4 milionu uživatelů, tak tvoří významný segment uživatelů, kterého se týká migrace na IPv6. Nejvýznamnějšími poskytovateli služby DSL v ČR jsou v současnosti poskytovatelé Telefónica, T-Mobile, Vodafone, UPC a GTS. Telefónica nabízí zákazníkům připojení IPv6 od června roku 2012. Poskytovatel UPC plánuje nabídku připojení prostřednictvím IPv6 od roku 2017. Pro zavedení IPv6 je třeba na straně zákazníka DSL směrovač s podporou IPv6 a na straně ISP je to BRAS, DNS a konektivita do IPv6 Internetu.

Pro samotnou migraci je nutné na DNS upravit záznamy tak, aby bylo možné získávat překlady adres obou IP protokolů. Dále se na BRAS vytvoří profily služeb s podporou přidělování IPv6 adres. Obvykle se jedná o profily, které přidělují IP adresy koncovým uživatelům v kombinaci IPv6+IPv4 privátní adresa. Privátní adresa se následně překládá využitím CGNAT na veřejnou. Nebo v kombinaci adres IPv6+IPv4 veřejná není nutné používat CGNAT a uživatel, tak může využít přímou konektivitu do Internetu prostřednictvím obou IP protokolů. Zařízení BRAS potom musí mít připojení do Internetu obou verzí IP protokolu. K tomu je nejčastěji využíváno MPLS (Multi Protocol Label Switching) páteře, která zároveň propojuje i ostatní služby s Internetem. Prozatím se pro připojení uživatelů DSL nepoužívá samotné IPv6 konektivity, protože je stále spousta internetových služeb dostupná pouze prostřednictvím IPv4 a pro uživatelé pouze IPv6 by byly tyto služby nedostupné, nebo by bylo nutné mezi sítěmi překládat adresy.

4.5.5 Datacentra

Pokud budeme uvažovat o migraci datacentra a zaměříme se na technologii síťové vrstvy, tak se bude nejčastěji týkat serverů, firewallů a loadbalancerů. Nejprve je třeba upravit dostupnou službu DNS tak, aby dokázala zpracovat dotazy IPv6. V souvislosti s konektivitou je nutná konektivita datacentra prostřednictvím IPv6. Jinak samotná migrace nemá smysl. Na straně serverů je důležitá podpora OS případně virtuálních serverů (vmware, Hyper-V).

4.5.6 *Přehled nejběžnějších OS a jejich podpora IPv6:*

Operační systém:	**IPv6 od verze:**
Windows Server	Server 2003
HP-UX	11i
SUN Solaris	10
LINUX	Linux kernel 2.6

Na směrovačích je třeba zapnout podporu IPv6 pro autokonfiguraci koncových stanic (ICMPv6, DHCPv6). V případě datacenter je možné také využít ruční nastavení IP adres na segmentech sítě, kde jsou připojeny servery. V síťové struktuře datacenter se běžně využívá zařízení (loadbalanceru) pro rozdělování datových toků směrem k serverům. Rozdělením datových toků na více samostatných serverů má za následek jejich rovnoměrné zatížení. Loadbalanceru je také možné využít pro překládání mezi adresami IPv4 a IPv6. Pro migraci je možné vytvořit takový profil, který internetovou službu zpřístupní prostřednictvím IPv4 i IPv6. Servery jednotlivých služeb je potom možné migrovat na IPv6 postupně nebo je provozovat současně na dobu nezbytně nutnou. Podporu IPv6 je možné využít například u zařízení Cisco ACE 4710. Vlastní datacentra velkých podniků bývají rozdělena na několik bezpečnostně oddělených zón. Pro kontrolu datového provozu mezi zónami se využívají firewally. Podpora IPv6 na firewallu nám umožní vytvářet pravidla (access listy), která umožní řízenou datovou komunikaci mezi zónami v datacentru. Například zařízení typu Cisco ASA je možné využít jako firewall s podporou IPv6. V rámci ČR všichni významní provozovatelé datacenter v této době nabízejí konektivitu prostřednictvím obou verzí IP protokolu.

4.6 Malé sítě SOHO

V drtivé většině domácích sítí je v současnosti využíváno privátních adresních rozsahů IPv4. Tak časté použití IPv4 je dáno typem konektivity do Internetu a technickými možnostmi síťových zařízení. Pokud poskytovatel připojení do Internetu neumožňuje připojení prostřednictvím IPv6, tak je vhodné zvážit důvody, proč nasazovat IPv6 v tak malé síti jako je domácnost nebo malá kancelář. Přesto však může být užitečné zpřístupnění některých domácích síťových zařízení z Internetu (např. sdílení souborů, systém elektronického zabezpečení, vzdálená plocha). Jestliže se uživatel domácí sítě

rozhodne pro používání IPv6 měl by kontaktovat poskytovatele konektivity, aby zjistil potřebné informace o možnostech jeho připojení. Potom je třeba zjistit, která zařízení domácí sítě IPv6 podporují. Tyto informace lze zjistit z technických specifikací a příruček jednotlivých výrobců nebo vývojářů.

Pro domácí směrovače je typické to, že v sobě integrují několik typů aktivních síťových prvků (xDSL modem, router, firewall, switch, WiFi access point). V našem případě nás zajímá podpora IPv6 a možných tunelovacích mechanismů (např. Teredo) na směrovači.

4.6.1 *Přehled nejběžnějších xDSL koncových zařízení podporujících IPv6:*

Výrobce:	**IPv6 podpora:**
Technicolor TC 7200	ANO
Motorola 5101	NE
Huawei EchoLife HG622u	ANO
ZyXEL Prestige 660HN-T3A	ANO

Vzhledem k tomu, že se pohybujeme v oblasti domácích sítí, přibývá zde specifický typ využití počítačové sítě, který nemá mezi podnikovými sítěmi příliš časté zastoupení. Jedná se využití sítě za účelem odpočinku, které poskytuje hraní počítačových her. Současná úroveň počítačových her většinou vyžaduje přístup k Internetu. Počítačové hry jsou nejčastěji nainstalovány na běžný počítač nebo herní konzoli. Herní konzole jsou často součástí domácího síťového prostředí. Pokud je herní konzole součástí domácí počítačové sítě, tak je třeba její možnost provozu na IPv6 zahrnout do analýzy síťového prostředí. Nejčastěji se vyskytují konzole výrobců Microsoft, SONY nebo Nintendo.

4.6.2 *Přehled nejběžnějších herních konzolí podporujících IPv6:*

Výrobce:	**IPv6 podpora:**
Microsoft Xbox One	NE
Microsoft Xbox 360	ANO
SONY PS4	ANO
Nintendo Wii	NE

5 VÝSLEDKY A DISKUSE

Rozhodnutí zda a kdy přistoupit k migraci firemního prostředí na IPv6 závisí kromě vlastního technického vybavení také na technologických možnostech vnějšího prostředí tvořeného ISP nebo jinými obchodními partnery. Ze strany vnějšího prostředí je zásadním aspektem dostupnost internetových služeb prostřednictvím IPv6, která v současnosti není stoprocentní. Z tohoto faktu vyplývá, že použití IPv4 jako síťového protokolu je stále ještě nezbytnou součástí moderních počítačových sítí. Dostupnost internetových služeb prostřednictvím IPv6 tak závisí kromě jiného na migraci provozovatelů hostingových center a jejich služeb.

Dalším důležitým aspektem, který je nutné uvážit, je připojení firemní sítě k vnějšímu prostředí. Pokud poskytovatel konektivity neumožňuje připojení prostřednictvím IPv6 je nutné zvažovat některý z uvedených mechanismů tunelování IP nebo překladu adres. Situace pro migraci firemní sítě je optimální v okamžiku, kdy ISP umožňuje připojení prostřednictvím obou IP protokolů a případné nutné překlady mezi IPv4 a IPv6 realizuje automaticky na své straně.

V okamžiku kdy jsou splněny všechny důležité podmínky vnějšího prostředí, tak je možné začít uvažovat o migraci vlastní firemní sítě. Nejprve je nutné analyzovat podporu IPv6 u všech souvisejících prvků sítě a na základě zjištěných přesných informací rozhodnout o způsobu provedení migrace a naplánování jejích jednotlivých kroků. Pokud firemní síť využívá některou ze služeb DSL, tak je vysoká pravděpodobnost, že poskytovatel umožňuje využívat IPv6 okamžitě nebo tuto možnost na vyžádání uskuteční.

Z pohledu poskytovatele konektivity je důležité vycházet z aktuálně používaných koncových zařízení na straně zákazníků, z dostupnosti internetových služeb prostřednictvím IPv6 a s technickými dispozicemi vlastní technologie. V současné době je technická vybavenost největších poskytovatelů v ČR na dostatečné úrovni, aby dokázala většině svých zákazníků poskytnout síťové připojení prostřednictvím obou verzí IP protokolu. V oblasti mobilního připojení je důležité zmínit, že je aktuálně využíváno tak velké množství mobilních terminálů, které nepodporují IPv6, a proto operátoři v ČR prozatím mobilní připojení s podporou IPv6 nenabízejí. I přesto však jsem toho názoru, že nabízet možnost připojení zákazníkům prostřednictvím IPv6 je důležitou podmínkou udržení konkurenceschopnosti a významným krokem k přechodu na IPv6 v globálním měřítku.

Neméně důležitými účastníky celkové migrace jsou hostingová centra a dostupnost jejich služeb v datacentrech prostřednictvím IPv6. Zpřístupnění internetových služeb prostřednictvím IPv6 ovlivňuje celkový průběh migrace. Moderní hostingová centra provozovaná v ČR umožňují v současnosti přístup k internetovým službám prostřednictvím obou verzí IP protokolu.

6 Závěr

Současný stav migrace firemních sítí je teprve na začátku. Pokud budeme uvažovat sítě středně velkých firem, tak je aktuálně v ČR téměř každá síť v provozu na původním protokolu IPv4. Důvodem je nejčastěji masívní využívání zastaralých operačních systémů na pracovních stanicích i serverech. Dalším důvodem je dostupnost připojení s podporou IPv6 ze strany poskytovatelů konektivity do Internetu. Dokud nebudou splněny všechny technické požadavky nutné pro migraci, tak se na straně sítě středně velkých společností nejspíše k migraci přistupovat nebude.

Největší poskytovatelé mobilního připojení na území ČR jsou v současnosti schopni poskytnout konektivitu využívající IPv6, ale protože na současném trhu mobilních terminálu není dostatek zařízení s podporou IPv6 nebo Dual-stack, je nejlepším postupem s migrací počkat, dokud se situace nezmění. Nedostatek veřejných IPv4 adres je tak v mobilních sítích ošetřen pomocí CG-NAT.

V souvislosti s poskytováním fixního připojení do Internetu je situace výrazně pokročilejší. Poskytovatelé fixního připojení již v současnosti umožňují konektivitu prostřednictvím IPv6. Zákazníci pevných služeb, tak aktuálně tvoří skupinu několika set tisíc připojení. Migrace fixních přípojek na IPv6 tak pozvolna probíhá. Pro připojení prostřednictvím IPv6 zákazníci využívají zároveň i stávajícího IPv4 k zajištění dostupnosti Internetových zdrojů, které nejsou na adresách IPv6 ještě přístupné. V případě fixního připojení k Internetu je také vyžíváno překladu veřejných adres IPv4 prostřednictvím CG-NAT.

Počítačové sítě používané v domácnostech obvykle, nepotřebují připojení do Internetu prostřednictvím staticky nastavených nebo přidělených IP adres. Pokud jsou v domácí síti zařízení podporující IPv6 nebo Dual-stack, tak je možné požádat poskytovatele připojení prostřednictvím IPv6. Správnou konfigurací na směrovači je pak možné IPv6 plně začít používat.

Vzhledem k rozrůstajícímu se použití IPv6 lze předpokládat, že se z trhu postupně začne snižovat poptávka po veřejných adresách IPv4. Celkový postup migrace na IPv6 bude i nadále záviset na podpoře výrobců, vývojářů, poskytovatelů síťových služeb a v neposlední řadě všech uživatelů Internetu.

Za migrací na IPv6 stojí především celosvětový technický a sociální rozvoj současné moderní společnosti. Jsem toho názoru, že problematika migrace na IPv6 je po

technické stránce téměř vyřešena. Vzhledem k reálnému technickému vybavení všech subjektů využívajících Internet předpokládám, že během několika málo let se IPv4 svým rozsahem stane v Internetu tím minoritním, až nakonec zanikne úplně.

7 Seznam použitých zdrojů

Buchta, Martin. 2014. IDC: Více než 90 % smartphonů prodaných ve 4. čtvrtletí 2013 má Android či iOS. *Channelworld.* [Online] 20. 2 2014. http://channelworld.cz/analyzy/idc-vice-nez-90-smartphonu-prodanych-ve-4-ctvrtleti-2013-ma-android-ci-ios-10825.

2014. Comparison of IPv6 support in operating systems. *Wikipedia The Free Encyclopedia.* [Online] Wikipedia, 1. 3 2014. [Citace: 15. 3 2014.] http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems.

Graziani, Rick. 2012. *IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6.* Indianapolis : Cisco Press, 2012. ISBN-10: 1-58714-313-5.

http://en.wikipedia.org/wiki/Regional_Internet_registry. Wikipedia. *Wikipedia.* [Online]

Jirovský, Václav. 2001. Vademecum správce sítě. *Vademecum správce sítě.* Praha : Graga Publishing spol. s r. o., 2001, ISBN 80-7169-745-1, 2001, str. 333.

Ludovic.ferre. 2010. XDSL Connectivity Diagram en.svg. *Wikipedia.org.* [Online] 14. 4 2010. http://commons.wikimedia.org/wiki/File:XDSL_Connectivity_Diagram_en.svg.

Macich, Jiří ml. 2013. channelworld.cz. *channelworld.cz.* [Online] 14. 5 2013. http://channelworld.cz/analyzy/ctu-aktivnich-sim-karet-je-v-cr-vice-nez-obyvatel-ale-pocet-jiz-neroste-8756.

McFarland , Shannon, a další. 2011. *IPv6 for Enterprise Networks.* Indianapolis : Cisco Press, 2011. ISBN-10: 1587142279.

NIX.CZ. 2014. NIX.CZ. *NIX.CZ.* [Online] 12. 2 2014. http://nix.cz/cs/technical#ip.

Satrapa, Pavel. 2012. Internetový protokol verze 6 IPv6. *Internetový protokol verze 6 IPv6.* Praha : CZ.NIC, z. s. p. o., Americká 23, 120 00 Praha 2, ISBN 978-80-904248-4-5, 2012, str. 273.

Shinder, Debra Littlejohn. 2003. *Počítačové sítě.* Praha : SoftPress s.r.o., 2003. ISBN-80-86497-55-0.