TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky a mezioborových inženýrských studií

RNDr. Pavel Satrapa, Ph.D.

IPv6 a jeho uplatnění v univerzitní počítačové síti

Habilitační práce

Liberec 2006

Poděkování

Chtěl bych poděkovat všem, kteří přispěli ke vzniku této práce. Návrh, realizace a provoz rozsáhlé sítě je týmovou záležitostí. Proto si poděkování v první řadě zaslouží mí kolegové, kteří se se mnou podílejí na tomto úkolu. V první řadě bych chtěl jmenovat Petra Adamce, Petra Koláře, Jiřího A. Randuse a Davida Kmocha, kteří v historii sítě liberecké univerzity zanechali významnou stopu. Rád bych poděkoval také kolegům ze sdružení CESNET, s nimiž jsem měl tu čest spolupracovat.

Rozvoj sítě by byl nemožný bez podpory vedení univerzity. Velmi oceňuji mimořádně vstřícný přístup k této problematice, s nímž jsem se setkal u všech rektorů Technické univerzity v Liberci, profesorů Zdeňka Kováře, Davida Lukáše a Vojtěcha Konopy.

V neposlední řadě si zaslouží poděkování má rodina, která mne v mé práci soustavně podporuje, třebaže to často znamená, že se tím krátí můj čas strávený s ní.

Pavel Satrapa

Anotace:

Práce podává stručný přehled aktuálního stavu protokolu IP verze 6, jeho implementace a rošíření. Dále popisuje historii a současný stav počítačové sítě Technické univerzity v Liberci a služeb jí poskytovaných. Hlavní pozornost je pak věnována implementaci protokolu IPv6 v prostředí této sítě.

Abstract:

This report provides a short overview of contemporary status of the IP version 6 protocol, its implementation and deployment. Further it describes the history and present status of the computer network of Technical university of Liberec and provided services. Main focus is given to the implementation of IPv6 protocol in this network.

Anotation:

Dieser Bericht bietet kurze Übersicht des aktuellen Zustandes des Protokolls IP Version 6, seines Implementazion and Erweiterung. Ferner er beschreibt die Historie und zeitgenössischen Zustand des Computernetzwerkes der Technischen Universität in Liberec und siene Dienste. Der Schwerpunkt des Berichtes ist dann die Implementazion des IPv6 Protokolls in diesem Netzwerk.

Obsah

1 Úvod

Internet Protocol verze 6 (IPv6) vznikl v první polovině devadesátých let 20. století s cílem vyřešit problém s krátícím se adresním prostorem Internetu a přinést některé nové vlastnosti proti stávajícímu IPv4. Přestože byl definován v již roce 1995 a všeobecně je považován za jedinou perspektivu Internetu, jeho prosazování do reálných sítí je velmi zdlouhavé a v současnosti je stále objem provozu IPv6 v porovnání s IPv4 marginální.

Podílí se na tom řada faktorů, z valné většiny netechnických – pomalý vývoj techniky a programů využívajících nový protokol, náklady spojené s jeho nasazením (pořízení nové techniky, školení personálu, změny konfigurací) i vlažný zájem uživatelů. Akademické sítě – lokální i rozlehlé – se snaží přispět ke zrychlení postupného přechodu k IPv6 a zavádějí jej jako alternativu k IPv4. Cílem je učinit jej dostupným uživatelům a otevřít prostor pro vývoj aplikací a služeb postavených nad novým protokolem či adaptaci těch stávajících.

Problematice IPv6 se věnuji okrajově od roku 1994, soustavně pak od roku 1999. Tato práce shrnuje dosažené výsledky mého úsilí v oblasti osvětové i implementační. Publikoval jsem jedinou existující českou monografii na toto téma a přibližně 30 článků v médiích elektronických i tištěných, vystoupil na několika seminářích a konferencích. Vedl jsem tým implementující první pokusnou páteřní IPv6 infrastrukturu v síti TEN-155 CZ a jako osoba zodpovědná za vytvoření a rozvoj univerzitní sítě TU v Liberci jsem vedl i implementaci IPv6 do jejího prostředí. Následující stránky přinášejí podrobnější informace o těchto mých aktivitách.

Kapitola 2 shrnuje historický vývoj a současný stav specifikací IPv6 a souvisejících protokolů. Jedná se spíše o doplněk a aktualizaci monografie [44], v níž naleznete podrobný výklad problematiky. Kapitola 3 poskytuje přehled současného reálného stavu IPv6, jeho implementace a rozšíření v počítačových sítích. Zvláštní pozornost věnuji historii a stavu podpory IPv6 v národní akademické síti ČR. V obou těchto kapitolách se často odkazuji na své články publikované v on-line časopisu Lupa (ISSN 1213-0702), zabývajícím se problematikou Internetu.

V kapitole 4 najdete stručný přehled historie a současného stavu počítačové sítě Technické univerzity v Liberci – její postupný vývoj i současné řešení podstatných složek, jako je adresace, směrování, DNS, správa uživatelů či služby. Navazující kapitola 5 pak poskytuje informace o implementaci IPv6 v prostředí této sítě a jejích služeb.

Jako přílohy přikládám k práci monografii [44] a relevantní články publikované ve výše zmiňovaném časopise Lupa, které ji rozšiřují a popisují změny, k nimž

došlo od jejího vydání. Tyto texty obsahují podrobnější popisy a vysvětlení protokolů, mechanismů a dějů stručně představených ve vlastní práci, která se díky tomu výrazně zjednodušila a zkrátila.

2 IPv6 – vývoj a současný stav protokolu

2.1 Vznik a vývoj IPv6

Internet Protocol verze 6 (IPv6) je vyvíjen jako nový základní protokol celosvětové sítě Internet. Má nahradit současnou verzi 4 (IPv4), vyvinutou během 70. let dvacátého století a používanou jako jednotný protokol síťové vrstvy sítě Internet od roku 1981.

Motivací pro vznik nového protokolu byl krátící se adresní prostor IPv4, který nedostačuje pro rychlý rozvoj Internetu a exponenciální nárůst počtu připojených počítačů – viz [35]. Tento problém se stal aktuálním na přelomu 80. a 90. let. Prognózy spotřeby adres ukazovaly, že během přibližně deseti let dojde k vyčerpání dostupných adres pro IPv4. Čas pro vývoj řešení byl dostatečný, proto bylo v rámci IETF rozhodnuto neřešit pouze otázku nedostatku adres, ale vyvinout zcela nový protokol s vlastnostmi, které IPv4 chybí.

Zachován měl být základní koncept – nespojovaný protokol bez záruk, dostatečně pružný a reagující na změny v síti. Požadované nové vlastnosti měly zahrnovat:

- přepracované adresování – rozsáhlý adresní prostor, jehož omezení by již nikdy nemělo vynutit změnu protokolu, nové typy adres, jednotnou adresaci Internetu i vnitřních sítí
- hierarchické směrování v souladu s hierarchickou adresací, podpora služeb s definovanou kvalitou, optimalizace pro vysokorychlostní směrování
- zahrnutí bezpečnostních mechanismů – ověření autenticity dat a jejich šifrování
- podpora mobilních zařízení (přenosné počítače, osobní sítě apod.)
- automatická konfigurace

Kromě toho měl být umožněn plynulý přechod z IPv4 na novou verzi protokolu. Vzhledem k rozsahu Internetu není možné stanovit pevné datum, kdy se páteřní protokol změní z jednoho na druhý. Musí se jednat o plynulý proces, kdy jednotlivé sítě a zařízení postupně přejdou z IPv4 na IPv6, aniž by byla funkčnost celku zásadně narušena.

U zrodu IPv6 stáli především Steven Deering a Robert Hinden, autoři *RFC 1883: Internet Protocol, Version 6 (IPv6) Specification* publikovaného v prosinci 1995.

V něm je definován formát rámce a základy jeho zpracování. Společně s několika dalšími RFC popisujícími doprovodné prvky a mechanismy (adresní architekturu, ICMPv6, ukládání do DNS, autokonfigurační mechanismy a podobně) tvoří první generaci definice IPv6.

Na jejím základě začaly vznikat, byť velmi pomalu, první experimentální implementace. Získané zkušenosti se odrazily ve druhé generaci definičních dokumentů, soustředěné kolem *RFC 2460: Internet Protocol, Version 6 (IPv6) Specification* z prosince 1998. Změny nebyly radikální, nicméně nová definice protokolu nebyla kompatibilní s původní, protože došlo k drobné úpravě formátu datagramu (čtyřbitová položka Priorita byla nahrazena osmibitovou Třídou provozu a následující Značka toku byla o čtyři bity zkrácena) a změnila se i adresní architektura.

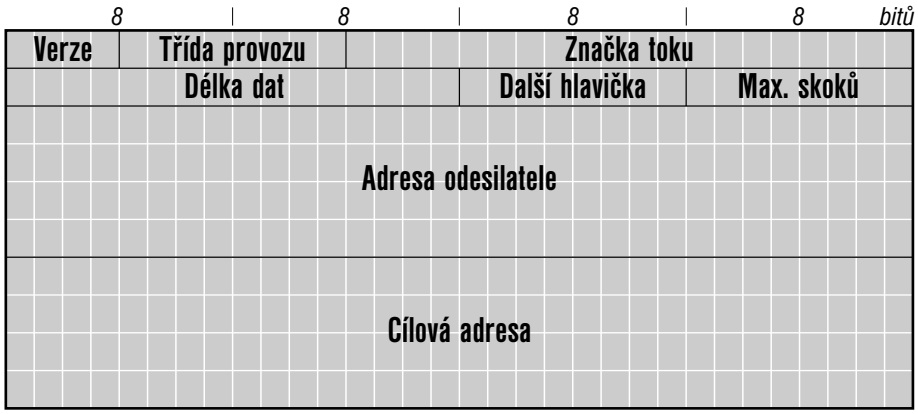
RFC 2460 zůstává v platnosti dodnes, to však neznamená, že by se vývoj IPv6 zastavil. Soustředí se na doprovodné mechanismy, například adresace dospěla v RFC 4291 již do své čtvrté generace. Doplňují se také některé prvky, které v původních dokumentech chyběly. Například definice mobility dospěla do fáze RFC teprve v červnu 2004, přestože je oficiálně deklarována jako povinná součást IPv6.

Ve zbývajících částech této kapitoly ve stručnosti popíši základy IPv6. Podrobný popis lze najít v monografii [44] přiložené k práci. Přestože i v kontextu světových publikací patří mezi nejaktuálnější výklady této problematiky (literatura věnovaná IPv6 je až překvapivě chudá), od jejího vydání došlo k několika podstatným změnám a zveřejnění významných specifikací. Kapitola je proto koncipována spíše jako aktualizace této publikace. Informace o většině změn jsem publikoval v samostatných článcích, které přikládám k práci a na něž se v textu odkazuji.

2.2 Formát datagramu

Základním východiskem při návrhu formátu IPv6 datagramu byla snaha o maximální jednoduchost, která by vyšla vstříc vysokorychlostnímu směrování. Výsledkem je konstantní velikost hlavičky datagramu s minimem položek. Případné doplňkové informace, které IPv4 datagram obsahuje v části Volby s proměnnou délkou, byly v IPv6 přesunuty do rozšiřujících hlaviček. Jejich pořadí je navíc předepsáno tak, aby zpracovávající směrovač mohl co nejrychleji ukončit průchod rozšiřujícími hlavičkami (v ideálním případě hned z hodnoty položky Další hlavička pozná, že datagram nenese žádnou doplňkovou informaci podstatnou pro směrování) a datagram zpracovat.

V důsledku snahy o maximální zjednodušení narostla velikost IPv6 hlavičky proti IPv4 na dvojnásobek (40 B proti 20 B), přestože obsahuje adresy čtyřnásobné délky. Ze čtyřicetibajtové hlavičky zabírají 32 B adresy příjemce a odesilatele a pouhých 8 B další doprovodné informace. Do rozšiřujících hlaviček, připojovaných jen v případě potřeby, byly přesunuty veškeré informace,



Obrázek 2.1: Formát datagramu

které nemusí nést každý datagram, jako jsou explicitní směrování (definující body, jimiž datagram musí projít), fragmentace, bezpečnostní mechanismy, informace pro podporu mobility a další.

Z hlediska směrování se IPv6 nachází v komplikované situaci. Na jedné straně má základní koncepcí navázat na svého předchůdce, a tedy poskytnout nespojovanou službu bez záruk. Na druhé straně je zde ovšem požadavek na podporu služeb s definovanou kvalitou či podporu datových toků, jejichž implementace je výrazně snazší ve spojovaném prostředí.

Tento rozpor se odráží i ve skutečnosti, že související položky hlavičky (Třída provozu a Značka toku) jsou sice v RFC 2460 zavedeny, jejich obsah však víceméně není definován a ponechán k dispozici dalším dokumentům. V případě Třídy provozu se staví na poměrně známé půdě – koncept diferencovaných služeb (differentiated services, diffserv) je rozpracován i pro IPv4, kde se pro uložení informace o třídě požívá položka TOS (Type of Service). Naproti tomu koncept datových toků je zcela nový. Měl by umožnit směrovačům optimalizovat konzistentní přenos dat mezi dvěma počítači – například přenos jednoho datového souboru či IP telefonní hovor. První pokus o jeho vyjasnění přineslo *RFC 3697: IPv6 Flow Label Specification* v roce 2004 (viz přílohu A na straně 59), ovšem stále se jedná o první kroky v dané problematice a je dosud nejasné, k jakým konkrétním mechanismům povede a zda vůbec vyústí v cokoli implementovatelného.

K výraznému posunu proti IPv4 došlo v oblasti fragmentace. Datagramy, jejichž velikost přesahuje pakety přenášené použitou technologií druhé vrstvy, smí v IPv6 fragmentovat pouze odesilatel (v IPv4 fragmentuje směrovač, u nějž k této situaci došlo). Celkově IPv6 zjevně inklinuje k odstranění fragmentace a zasílání datagramů, jež sítí projdou v nezměněné podobě. V souladu s tímto trendem je i důrazně doporučeno používání objevování MTU cesty. Linky podporující IPv6 musí mít MTU alespoň 1280 B, doporučuje se 1500 B. Vzhledem k mohutnému rozmachu Ethernetu s MTU 1500 B, který obsadil drtivou většinu

lokálních sítí a prosazuje se i na dálkových trasách, lze očekávat, že MTU se ustálí na víceméně jednotné hodnotě 1500 B a fragmentace nebude potřebná.

2.3 Adresace

Vzhledem k tomu, že nedostatek adres byl iniciátorem vzniku IPv6, věnuje se otázkám adresace značná pozornost. Dochází zde také asi k největšímu počtu změn. Od samých začátků panuje shoda na délce adresy, jež činí 128 bitů, tedy čtyřnásobek proti IPv4. Také zápis v podobě šestnáctkových číslic, pro přehlednost rozdělených dvojtečkami do skupin po dvou bajtech zůstává neměnný.

Vývoj však prodělává struktura adresy. Její zatím poslední definici obsahuje *RFC 4291: IP Version 6 Addressing Architecture* z února 2006 – viz příloha B na straně 61. Definuje tři typy adres:

Individuální (unicast) označují jedno síťové rozhraní, jemuž je datagram dopraven.

Skupinové (multicast) identifikují skupinu síťových rozhraní. Datagram je doručen všem jejím členům.

Výběrové (anycast) identifikují také skupinu síťových rozhraní, data se ale doručují jen jednomu jejímu členovi (nejbližšímu).

Proti IPv4 zmizely adresy všesměrové (broadcast), které představují speciální případ skupinových. Pro tyto účely jsou v IPv6 definovány speciální skupinové adresy obsahující například všechny počítače či všechny směrovače v dané části sítě.

Největší význam mají pochopitelně adresy individuální, přesněji globální individuální adresy, jež jsou jednoznačné v celém Internetu a zajišťují běžnou přepravu dat. Hierarchické uspořádání navržené v RFC 2374 se nikdy neprosadilo do praxe. Jejich aktuální definice v *RFC 3587: IPv6 Global Unicast Address Format* je maximálně jednoduchá:

- počáteční tři bity obsahují hodnotu 001 (binárně) identifikující danou část adresního prostoru
- následuje 45bitový globální směrovací prefix (odpovídající adrese sítě v terminologii IPv4, zde s důrazem na agregaci)
- dalších 16 b obsahuje adresu podsítě
- závěrečných 64 b nese identifikátor rozhraní

Podrobnější komentář k RFC 3587 najdete v příloze C na straně 65. Od doby vydání článku došlo k přidělení několika dalších prefixů jednotlivým reionálním registrátorům. Prvních 16 bitů adresy proto může obsahovat i jinou hodnotu než 2001 (nicméně drtivá většina v současnosti používaných adres pochází z

rozsahu 2001::/16, nově přidělené prefixy zatím nejsou využívány). Vzhledem k současné praxi v přidělování adres je počátečních 48 b rozděleno na tři části:

- prefix identifikující RIR (centrálně přidělovaný IANA)
- hodnota přidělená regionálním registrátorem (pro Evropu RIPE NCC)
- hodnota přidělená lokálním registrátorem (typicky poskytovatel Internetu, v případě univerzit roli LIR vykonává sdružení CESNET)

Stanovení velikosti jednotlivých částí adresy je však stále předmětem diskusí. Jejich cílem je, aby se zabránilo nadměrnému plýtvání hned při uvádění protokolu do života, jako se stalo s IPv4. Za všeobecně nedotknutelnou je považována hranice vymezující 64 bitů pro adresu rozhraní v rámci podsítě. Sice zjevně představuje největší rozmařilost v přidělování adres (poloviční hodnota by stačila s obrovskou rezervou), ale vycházejí z ní některé mechanismy a zkrácení identifikátoru rozhraní nelze očekávat.

Největší pozornost se soustředí na šestnáctibitovou adresu podsítě požadovanou *RFC 3177: IAB/IESG Recommendations on IPv6 Address Allocations to Sites* pro všechny sítě, u nichž připadá v úvahu dělení na podsítě. V internetové komunitě dnes existují silné tlaky na rozdělení koncových sítí podle velikosti a v závislosti na ní poskytovat pro adresu podsítě 16 b (65 536 podsítí) nebo 8 b (256 podsítí) – viz přílohu D na straně 67.

Zajímavou inovací, kterou IPv6 obohacuje adresní prostor, jsou dosahy adres. Pro každou adresu je definována určitá část sítě (od jediného rozhraní až po celý Internet), v níž je jednoznačná. Určuje dosah dané adresy. Dosahy jsou užitečné především pro skupinové adresování, kde umožňují efektivně omezovat dosah distribuce dat. V IPv4 se k podobnému účelu požívaly nesystémové triky s životností datagramů (položka TTL, Time to Live). Koncept dosahů představuje další z postupně se vyvíjejících oblastí IPv6. Teprve v březnu 2005 vyšlo *RFC 4007: IPv6 Scoped Address Architecture* podávající podrobnější výklad jejich významu a práce s nimi – viz příloha E na straně 71. Opět se ale jedná jen o první krok na cestě k podrobné definici zacházení s dosahy.

2.4 Domain Name System

Vzhledem k uživatelsky nepříliš přítulnému zápisu IPv6 adres má velmi důležitou úlohu DNS, bez nějž by IPv6 Internet byl jen obtížně použitelný. Jeho vývoj bohužel představuje nepříliš vydařenou kapitolu z historie DNS.

Součástí první generace specifikací z roku 1995 bylo i *RFC 1886: DNS Extensions to support IP version 6* s dost přímočarou definicí záznamů pro ukládání IPv6 adres. Zavedlo záznam AAAA, jehož obsahem měla být kompletní IPv6 adresa dotyčného uzlu:

```
pc1 IN AAAA 2001:718:1c01:1:0214:22ff:fec9:072c
```

Pro reverzní záznamy měly sloužit standardní záznamy PTR, domény pro jejich uspořádání měly být vytvořeny z jednotlivých šestnáctkových číslic kompletního zápisu adresy v obráceném pořadí. Zařazeny měly být do domény *ip6.int*. Pro výše uvedený uzel by tedy zónový soubor pro doménu odpovídající prefixu TU Liberec *1.0.c.1.8.1.7.0.1.0.0.2.ip6.int* obsahoval záznam:

```
c.2.7.0.9.c.e.f.f.f.2.2.4.1.2.0.1.0.0.0 IN PTR pc1.kai.tul.cz.
```

V roce 2000 vyšlo *RFC 2874: DNS Extensions to Support IPv6 Address Aggregation and Renumbering* s návrhem záznamů A6 pro dopředné a DNAME pro reverzní záznamy, jež nahradily předchozí specifikaci. Nový návrh byl elegantnější, umožňoval přebírat část adresy z jiného záznamu, reverzní data bylo možné zapisovat bez obracení pořadí číslic a ukládat je do běžných zónových souborů. Nově navržený mechanismus byl však choulostivější, což vyvolalo vášnivé diskuse o jeho vhodnosti.

Několikaleté rozepře zastánců obou přístupů ukončilo až *RFC 3596: DNS Extensions to Support IP Version 6* z října 2003, jež jednoznačně rozhodlo ve prospěch robustnosti, tedy původního návrhu. Jedinou změnou, která zůstala po RFC 2874 bylo přesídlení reverzních záznamů z domény *ip6.int* do *ip6.arpa* – viz příloha F na straně 75.

2.5 Objevování sousedů a automatická konfigurace

Mechanismus objevování sousedů (Neighbor Discovery, ND) zajišťuje v IPv6 řadu úkolů souvisejících s automatickým vyhledáváním adres a konfigurací. Konkrétně má na starosti:

- zjišťování linkových adres uzlů ve stejné lokální síti, testování jejich dosažitelnosti a aktualizaci těchto informací
- automatickou konfiguraci – zjišťování prefixů a parametrů sítě, hledání směrovačů
- přesměrování – opravu směrování, pokud je pro odesilatele k dispozici vhodnější cesta
- detekci duplicitních adres

Jeho definici obsahuje *RFC 2461: Neighbor Discovery for IP Version 6*. S pouhými pěti typy zpráv nahrazuje objevování sousedů původní protokol ARP, zastává jednu z úloh ICMP a přidává automatickou konfiguraci.

Automatická konfigurace s ideálem připojování k síti typu plug&play představuje jeden z požadavků na nové vlastnosti IPv6. Protokol pro ni nabízí dvě varianty: konfiguraci stavovou a bezstavovou. Stavová automatická konfigurace se opírá o protokol DHCPv6 a nepřináší proti IPv4 mnoho nového – konfigurace je řízena z DHCP serveru, kde správce sítě definuje parametry připojení jednotlivých počítačů. Snad jedinou překvapující skutečností je, že

adaptace DHCP pro prostředí IPv6 trvala velmi dlouho. *RFC 3315: Dynamic Host Configuration Protocol for IPv6* vyšlo po řadě let vývoje až v červenci 2003. Již před jeho publikací byly k dispozici první experimentální implementace, ovšem problematické kvality – viz příloha G na straně 77.

Zajímavější je bezstavová automatická konfigurace zajišťovaná objevováním sousedů. Při ní si připojený počítač sám přidělí lokální linkovou adresu (algoritmem vycházející z fyzické linkové adresy), ověří její unikátnost a na základě zprávy Ohlášení směrovače získá prefix(y) zdejší podsítě, ze kterých si sestaví globální IPv6 adresy. Na základě Ohlášení směrovačů si také vytvoří základní směrovací tabulku. Stanice si tedy sama nastaví potřebné síťové parametry, aniž by pro ni správce sítě či uživatel museli něco nastavovat.

Otázkou je, zda je takovýto plug&play způsob žádoucí (snižuje bezpečnost a problematizuje zodpovědnost uživatelů za chování v síti), proto je možné jej stanicím povolit či zakázat. Lze však očekávat, že se díky své pohodlnosti prosadí a kontrola přístupu k síti bude probíhat nikoli na základě fyzických adres, ale autentizací uživatele mechanismy, jako je 802.1X.

Vážným problémem bezstavové konfigurace je, že nechává stranou DNS. I zde se však hledají cesty, jak jeho nastavení zajistit – viz příloha H na straně 81.

2.6 Směrování

Z hlediska elementárního směrování se v IPv6 mnoho nezměnilo. Vychází ze směrovací tabulky, jejíž položky se porovnávají s cílovou adresou datagramu. Položka s nejdelším vyhovujícím prefixem je použita k doručení datagramu. Jediným rozdílem je velikost adres – délka prefixů je zde čtyřnásobná. Existence dosahů adres a jim odpovídajících zón pak může vyvolat existenci několika nezávislých směrovacích tabulek odpovídajících jednotlivým zónám v jednom zařízení.

Významný je důraz na hierarchické přidělování a agregaci adres, bez níž by velikost směrovacích tabulek v páteřních směrovačích rostla nad únosné meze. Jedná se však spíše o organizační opatření, nikoli vlastnost protokolu samotného. Jak bylo uvedeno výše, původně striktně hierarchická definice částí IPv6 adresy byla postupně zobecněna a její hierarchizace se přesunula do praktických pravidel přidělování uplatňovaných regionálními registrátory (RIR).

Pokud se týče směrovacích protokolů, nedošlo v souvislosti s IPv6 k vývoji žádného zcela nového protokolu. Namísto toho jsou adaptovány existující protokoly, do jejichž modifikovaných verzí je doplňována podpora IPv6. Konkrétně byly definovány:

- RIPng v *RFC 2080: RIPng for IPv6*
- OSPFv3 v *RFC 2740: OSPF for IPv6*
- IS-IS v *draft-ietf-isis-ipv6*

- BGP4+ v *RFC 2283: Multiprotocol Extensions for BGP-4*

2.7 Bezpečnostní prvky

Absence bezpečnostních mechanismů – šifrování dat či ověření jejich původu a autentičnosti – je jedním z kritizovaných nedostatků IPv4. Řeší se jejich implementací na aplikační úrovni či vytvářením vložených bezpečnostních vrstev typu SSL. Jedním z požadavků na IPv6 proto bylo poskytnout tyto mechanismy přímo v síťové vrstvě a poskytnout tak univerzální zabezpečenou platformu pro všechny aplikace.

Výsledkem tohoto úsilí byla definice bezpečnostních prvků IP pod názvem IPsec, společná pro IPv4 a IPv6. Základní myšlenky jsou společné pro oba protokoly, v dílčích detailech se pochopitelně odlišují. Jako hlavní deviza IPv6 se uvádí, že v jeho případě je IPsec nedílnou součástí protokolu a jeho implementace je povinná, zatímco v případě IPv4 se jedná o rozšíření. Realita tomu zatím bohužel neodpovídá, jak bude zmíněno v další kapitole.

Definice IPsec existuje již ve třetí generaci. Základem první generace bylo RFC 1825 z roku 1995. O tři roky později je nahradila druhá generace kolem RFC 2401, jež zůstala v platnosti až do konce roku 2005, kdy byla publikována třetí generace. Jejím základem je popis bezpečnostní architektury v *RFC 4301: Security Architecture for the Internet Protocol*.

IPsec staví na dvou bezpečnostních protokolech: Authentication Header (AH) poskytuje ověření integrity a zdroje dat a ochranu proti opakování. Je definováno v *RFC 4302: IP Authentication Header*. Encapsulating Security Payload (ESP) nabízí tytéž služby a navíc utajení prostřednictvím šifrování obsahu datagramu. Jeho definici obsahuje *RFC 4303: IP Encapsulating Security Payload (ESP)*. Několik dalších RFC pak doplňuje pravidla pro použití jednotlivých kryptografických algoritmů v těchto protokolech.

Parametry komunikace mezi konkrétní dvojicí uzlů pak definuje tzv. bezpečnostní asociace, jež obsahuje informace o použitých protokolech, algoritmech, klíčích a podobně. Právě správa klíčů se ukazuje jako kritické místo IPsec a největší překážka jeho nasazení. Nedaří se uvést do života infrastrukturu veřejných klíčů (PKI), což v praxi omezuje použitelnost IPsec na uzavřené komunity. *RFC 4306: Internet Key Exchange (IKEv2) Protocol* definuje protokol pro jejich výměnu, jeho použitelnost bez potřebné infrastruktury však zůstane omezená.

Společné aktivity národních akademických sítí v oblasti autentizace a autorizace dávají naději na obrat k lepšímu alespoň v akademické komunitě. Projekty jako je *eduroam* či společné zajištění serverových certifikátů SureServerEDU garantovaných firmou GlobalSign poskytují dobré vyhlídky pro budoucnost.

Zajímavou otázku představuje vliv bezpečnostních prvků na přenosový výkon. Výsledky experimentů, které jsem společně s kolegy ze sdružení CESNET

prováděl v roce 2000 (viz [31]) ukázaly, že jejich nasazení sice způsobí znatelný pokles propustnosti komunikace[1], ta však zůstává rozumně použitelnou. Experiment navíc probíhal na technice, jejíž výpočetní výkon hluboce zaostává za současnými standardy, v současnosti by výkonnostní rozdíl mezi otevřenou a chráněnou komunikací byl nepochybně znatelně nižší. Za pozoruhodné považuji zanedbatelné rozdíly v přenosovém výkonu mezi IPv4 a IPv6 na dané platformě, které testování ukázalo.

2.8 Mobilita

Podpora mobilních zařízení představuje jednu ze základních předností IPv6. Vzhledem k jejich rychle rostoucímu počtu je považována za možný argument pro definitivní prosazení IPv6, společně s obrovským adresním prostorem.

Vzhledem k důležitosti podpory mobility je krajně nešťastné, že se dlouho nedařilo dokončit její definici. Když se v roce 2001 pracovní návrh již zdál být stabilizovaný, došlo k odmítnutí navržených bezpečnostních mechanismů, jež vyvolalo zásadní přepracování celé definice. Konečnou podobu tak získala až v roce 2004 v *RFC 3775: Mobility Support in IPv6*.

Staví na myšlence, že mobilní zařízení má svou určitou domácí síť, v níž je registrováno a zavedeno do DNS. Pokud se právě nachází mimo svou domácí síť, zastupuje je v ní domácí agent, s nímž je propojeno ze svého aktuálního působiště šifrovaným tunelem (viz [1]). Domácí agent přebírá veškeré datagramy určené na domácí adresu mobilního uzlu a přeposílá mu je daným tunelem.

Přeprava datagramů tímto způsobem by byla neefektivní (podobně pracuje podpora mobility v IPv4), proto IPv6 obsahuje mechanismus optimalizace směrování. V něm mobilní uzel oznámí svému komunikačnímu partnerovi svou aktuální adresu, aby data mohla být posílána přímo. Optimalizace však představuje určité bezpečnostní riziko, proto je doplněna patřičnými bezpečnostními prvky (nikoli však na bázi IPsec, které je vzhledem k chybějící PKI efektivně nepoužitelné pro komunikaci mezi náhodnou dvojicí uzlů).

Podpora mobility si vyžádala zavedení několika rozšiřujících hlaviček. Konkrétně se jedná o hlavičku Mobilita pro správu vazeb mezi domácí a dočasnou adresou uzlu, hlavičku Domácí adresa, již mobilní uzel přidává ke svým datagramům, a speciální tvar hlavičky Směrování, kterou používá protější uzel komunikace k doručení dat na dočasnou adresu mobilního uzlu. Celý systém je koncipován tak, aby mobilita zůstala skryta před vyššími vrstvami síťové architektury, vůči nimž se IP vrstva chová, jako by mobilní uzel vždy komunikoval ze své domácí adresy. Podrobnější komentář obsahuje příloha I na straně 85.

[1] Při použití AH přibližně na třetinu, při šifrování s použitím ESP na čtvrtinu. Hodnoty se výrazně liší v závislosti na použitém kryptografickém algoritmu.

2.9 Přechod z IPv4 na IPv6

Značnou péči věnuje IETF metodám a technologiím, které by měly umožnit plynulý přechod Internetu z IPv4 na IPv6. Dostupné návrhy lze rozdělit do dvou základních skupin: tunelující, které propojují uzly komunikující stejným protokolem po sítí, jež daný protokol nepodporuje (viz příloha J na straně 91), a překladové snažící se o vzájemný překlad protokolů a umožnění komunikace mezi uzly hovořícími různými verzemi IP (viz příloha K na straně 95).

Tunelující přístupy vyžadují, aby alespoň některé uzly v síti využívaly tzv. dual-stack, tedy podporovaly obě verze protokolu. Ty pak mohou přepravovat datagramy jedné verze IP jako data v datagramech verze druhé a zprostředkovat tak například vzájemnou komunikaci dvou koncových IPv6 sítí po Internetu podporujícím pouze IPv4. Jejich základem je *RFC 2473: Generic Packet Tunneling in IPv6 Specification* popisující základní principy tunelování.

Doprovodné mechanismy se zabývají otázkou vytváření a správy tunelů. Z hlediska počátečního získávání zkušeností s novým protokolem jsou důležité tunel servery a tunel brokery (*RFC 3053: IPv6 Tunnel Broker*) umožňující komukoli s připojením k Internetu vytvořit si tunel přenášející IPv6 a experimentovat s protokolem. Pro reálné nasazení IPv6 do produkční sítě je přínosný především mechanismus 6to4 (*RFC 3056: Connection of IPv6 Domains via IPv4 Clouds*), který z jedné IPv4 adresy přístupového směrovače vytvoří IPv6 prefix standardní délky 48 bitů pro adresaci celé koncové sítě. 6to4 adresy používají prefix 2002::/16, podle nějž je podporující směrovače poznají a datagramy automaticky tunelují na IPv4 adresu přístupového směrovače obsaženou v prefixu dané sítě.

Základem skupiny překladových mechanismů je SIIT (*RFC 2765: Stateless IP/ICMP Translation Algorithm (SIIT)*) definující překlad datagramů mezi IPv6 a IPv4. Ke své činnosti však vyžaduje doprovodné prvky, jejichž specifikaci ponechává na dalších dokumentech. Největší pozornost je přikládána mechanismu NAT-PT (*RFC 2766: Network Address Translation – Protocol Translation (NAT-PT)*), který se zaměřuje na vzájemné mapování adres mezi IPv4 a IPv6 sítí. Právě správa adres je nejvýznamnější chybějící komponentou SIIT, který společně s NAT-PT tvoří funkční celek. Schopnosti překladu jsou samozřejmě omezené, pokročilejší vlastnosti protokolů leží mimo jeho dosah. Zajišťuje však alespoň základní interoperabilitu mezi oběma světy.

3 Implementace a rozšíření IPv6

V současné době již existují implementace IPv6 pro všechny významnější operační systémy i hardwarové směrovače. Přesto reálné nasazení protokolu dlouhodobě nenaplňuje očekávání.

S cílem podpořit rozvoj a praktické uplatnění nového protokolu založili v roce 1999 výrobci síťových zařízení, poskytovatelé Internetu a výzkumné a vzdělávací instituce konsorcium nazvané *IPv6 Forum*. Významnou složkou jeho činnosti je osvěta – organizace vydává informační materiály a pořádá konference po celém světě.

Pro konsolidaci stavu implementací IPv6 je však ještě významnější jeho program *IPv6 Ready*. Jedná se o certifikáty dosvědčující kompatibilitu zařízení a programového vybavení se specifikacemi protokolu. K získání statutu IPv6 Ready a práva používat odpovídající logo musí produkt splnit předepsanou sérii testů. Existují dvě certifikované úrovně (tzv. fáze) podpory: fáze 1 pokrývá pouze základní prvky protokolu, zatímco fáze 2 zahrnuje i implementačně náročnější komponenty, jako je IPsec či mobilita.

Obrázek 3.1: Logo IPv6 Ready, fáze 1

Program IPv6 Ready začíná přinášet velmi pozitivní výsledky. Logo stvrzující kompatibilitu se pro výrobce a autory stává prestižní záležitostí a vynakládají patřičné úsilí o jeho získání. Díky tomu se kvalita implementací v poslední době znatelně zlepšila. IPv6 Forum zde převzalo osvědčený koncept – podobnou

roli sehrálo jako logo Wi-Fi pro výrobky z oblasti bezdrátových sítí podle standardu IEEE 802.11.

Ve zbývající části této kapitoly popíši aktuální stav IPv6 a jaké jsou jeho příčiny a důsledky.

3.1 Implementace

Jak byl uvedeno výše, o implementace IPv6 v současnosti není nouze. Dlouhodobě však pokulhávala jejich kvalita. V případě mnohých systémů či komerčních produktů se nelze vyhnout dojmu, že hlavním cílem autorů bylo zaškrtnout kladně kolonku „máme implementováno IPv6“, nikoli poskytnout uživatelům reálně použitelnou platformu poskytující dříve zmiňované výhody, díky nimž se má IPv6 prosadit. Situace se začíná zlepšovat až v poslední době, do značné míry díky programu IPv6 Ready. Pokročilé vlastnosti, jako je například podpora IPsec či mobility, však dosud často chybí, přestože jsou de iure nedílnou součástí protokolu.

Typickým představitelem této kategorie je implementace IPv6 v **Microsoft Windows XP**, nejrozšířenějším operačním systému současnosti. MS Windows XP podporují IPv6, ovšem tato podpora je určena pro výzkum, vývoj a testování a samotný výrobce zapovídá v instalační příručce její použití v produkčním prostředí. V praxi to znamená, že IPv6 není přítomno v grafických nástrojích pro správu a užívání systému. Je třeba je explicitně aktivovat řádkovým příkazem

```
ipv6 install
```

a také veškeré jeho ovládání se odehrává prostřednictvím řádkových příkazů. IPsec je podporován pouze v tom smyslu, že systém zná rozšiřující hlavičky AH a ESP, neumí však žádné kryptografické algoritmy (pouze nešifrující prázdný algoritmus, určený dle RFC pro testování). V oblasti mobility dovedou MS Windows XP komunikovat s mobilním uzlem, samy jím však nemohou být. Je zjevné, že v prostředí tohoto operačního systému sice lze používat IPv6, řada jeho jeho významných výhod však zůstává nedostupná.

O málo lepší podporu IPv6 nabízí serverový systém Microsoft Windows Server 2003, který disponuje certifikací IPv6 Ready fáze 1. Tu má i systém Windows CE 4.2 pro kapesní počítače.

Podle [7] se má situace výrazně zlepšit v nové generaci MS Windows Vista/Longhorn. Podpora protokolů IPv4 a IPv6 zde bude integrována do jedné knihovny a jejich vlastnosti by se proto měly výrazně přiblížit. IPv6 bude implicitně instalováno a aktivováno, konfigurace a správa bude srovnatelná s IPv4. V případě dostupnosti obou protokolů budou Windows Vista/Longhorn dávat přednost IPv6. IPsec se dočká skutečné implementace, včetně kryptografických algoritmů a protokolu IKE pro výměnu klíčů. Celkově lze očekávat, že přicházející generace MS Windows bude pro rozšíření IPv6 představovat

velmi zásadní impuls a podstatným způsobem rozšíří uživatelský zájem o nový protokol.

Dlouhodobě nejlepší podporou IPv6 disponuje **BSD Unix**, kde významnou úlohu sehrálo soutěžení tří alternativních implementací. Nakonec se z nich jako nejkvalitnější prosadila japonská implementace KAME, jež v současné době tvoří standardní součást distribucí BSD. Vyniká širokým pokrytím vlastností IPv6 (včetně pokročilých, jako je IPsec[1] či mobilita) a zároveň velkou úspěšností v testech kompatibility.

KAME kód je pochopitelně certifikován jako IPv6 Ready fáze 2. Projekt KAME, jehož cílem bylo vyvinout kvalitní a standardy naplňující implementaci IPv6, byl v březnu 2006 ukončen jako úspěšný.

Implementace IPv6 pro **Linux** byla zahájena velmi brzy – již v roce 1996. Její kvalita však nebyla valná a vývoj se navíc na několik let v podstatě zastavil. Jako reakce na nepříliš potěšující stav vznikl v Japonsku v roce 2000 projekt USAGI (UniverSAl playGround for Ipv6) usilující o zvýšení kvality podpory IPv6 v Linuxu. Původně existoval kód USAGI v podobě samostatné změny (patch) standardního jádra, postupně ale byly jejich výsledky přebírány do standardní distribuce.

Současná podpora IPv6 v jádře systému je proto postavena na USAGI kódu. Ten nadále existuje i samostatně pro vývoj a testování nových vlastností (viz *http://www.linux-ipv6.org/*). Po ověření jsou nové prvky přebírány do standardního jádra – tento model je pro Linux obvyklý. V současnosti je implementace IPv6 poměrně kvalitní, včetně řady pokročilých prvků. Významnějším nedostatkem je chybějící podpora mobility, které se věnuje samostatný projekt (viz *http://www.mobile-ipv6.org/*).

Výrazné zlepšení podpory IPv6 se odrazilo i v získání certifikátu IPv6 Ready fáze 2 pro jádro verze 2.6.15 v květnu 2006.

Linux je velmi heterogenní systém s řadou alternativních distribucí, jejichž vlastnosti se významně liší. Nejvýznamnější distribuce již v současné době standardně obsahují podporu IPv6, jež typicky bývá implicitně zapnuta. Využívat nový protokol v prostředí Linuxu je tedy poměrně snadné (až na výše zmiňovanou mobilitu).

Jen málo informací o podpoře IPv6 je dostupných pro operační systém **Mac-OS X**. Jeho aktuální verze protokol podporuje a implicitně je aktivován, takže počítače firmy Apple mohou pracovat v IPv6 sítích. Kvalita implementace bude pravděpodobně velmi dobrá, protože vychází z kódu BSD. Podrobné informace o jejím stavu však výrobce nepublikuje a nenechal svůj operační systém ani certifikovat.

[1] Měření výkonu IPv6 zmiňované v předchozí kapitole probíhalo v prostředí BSD s KAME, které již v roce 2000 poskytovalo kvalitní podporu IPsec, tehdy jako jediná dostupná platforma.

Firma **Cisco Systems** implementovala IPv6 poměrně pozdě. Její IPv6 software zůstával několik let ve stádiu beta-verze a termín jeho převzetí do verze oficiální byl opakovaně odkládán. Teprve IOS verze 12.2T v roce 2001 poskytl nový protokol i v produkční verzi systému. Vzhledem k tomu, že Cisco Systems je největším výrobcem aktivních prvků pro počítačové sítě, považuji toto zpoždění společně s chabou podporou v systému MS Windows za jedny z nejvýznamnějších příčin pomalého prosazování IPv6.

IOS verze 12.2 získal certifikaci IPv6 Ready fáze 1. Podpora IPv6 v IOS se však postupně zlepšuje, takže verze 12.4(9)T již byla certifikována jako IPv6 Ready fáze 2 a je pro nasazení IPv6 velmi dobře použitelná.

Jedním z významných konkurentů Cisco Systems je firma **Juniper Networks**, jejíž výrobky používá i řada NREN (včetně evropské páteře GÉANT). IPv6 implementovala dříve, pravděpodobně jako jeden z nástrojů konkurenčního boje. Další vývoj však byl pomalejší, takže v současnosti disponuje pouze certifikací IPv6 Ready fáze 1 pro JUNOS verze 6.0R2.

3.2 Dostupnost v komerčním Internetu

Z hlediska praktické dostupnosti IPv6 v nabídce komerčních poskytovatelů Internetu panují velké rozdíly mezi jednotlivými regiony. Obecně platí, že zájem o nový protokol je největší v zemích, které se zapojily pozdě do rozvoje Internetu a v důsledku toho trpí nedostatkem IPv4 adres (podmínky pro jejich přidělování se postupem času zpřísňovaly). Je zřetelné, že nedostatek adres stále představuje velmi významný faktor v prosazování nového protokolu.

Asi nejpalčivější je problém nedostatku IPv4 adres v Asii, kde především rozvoj Internetu v Číně výrazně přesahuje dostupné adresní možnosti. Nejkřiklavější případy nedostatku adres pocházejí právě z této země (například přidělení jedné sítě třídy B, tedy 65 536 adres pro síť více než 60 tisíc čínských středních škol; stejný adresní rozsah má k dispozici jen samotná TU v Liberci).

Speciálním případem je Japonsko, známé velmi silným příklonem k IPv6. Předseda vlády jej označil za kritickou část iniciativy eJapan 2005 a firmy implementující IPv6 jsou podporovány daňovými úlevami. Japonsko vstoupilo do Internetu včas a jeho velké sítě mají adres dostatek, nedaří se mu ale výrazněji prosadit mezi výrobci síťových zařízení. IPv6 je zde vnímáno jako ekonomická příležitost a šance zvýšit podíl na trhu síťových technologií na úkor amerických výrobců, jejichž přístup k IPv6 je poměrně vlažný.

Není překvapující, že řada asijských (a v první řadě japonských) poskytovatelů Internetu nabízí IPv6 buď jako přídavnou službu k IPv4, nebo přímo jako základní připojovací protokol. Celosvětově pravděpodobně prvním poskytovatelem nabízejícím regulérní IPv6 služby bylo japonské NTT Communications. Jako další příklady lze jmenovat IIJ či Japan Telecom.

Na druhém pólu zájmu o IPv6 stojí paradoxně kolébka Internetu, Severní Ame-

rika. Zdejší sítě získávaly své adresní rozsahy v dobách, kdy podmínky jejich přidělování byly poměrně volné, a tudíž mají zpravidla dostatek prostoru. IPv4 přináší značné komerční úspěchy a motivace zdejších subjektů pro příklon k novému protokolu není vysoká, což se projevuje i na objemu přidělovaných IPv6 adres. Stále zůstává v platnosti výrok jednoho ze správců tamější univerzitní počítačové sítě „IPv6 je jako atomové zbraně. Všichni je chtějí mít, ale nikdo je nechce používat."

Administrativa USA se snaží tuto situaci změnit. Proto v srpnu 2006 Úřad pro správu a rozpočet Bílého domu vydal memorandum požadující, aby veškerá páteřní infrastruktura federálních úřadů do června 2008 podporovala IPv6 a jednotlivé úřady byly schopny tímto protokolem komunikovat. Součástí memoranda je i časový plán realizace a požadavek, aby veškeré nové vybavení úřadů podporovalo IPv6 nebo měl alespoň plán zavedení podpory IPv6 do června 2008. Toto memorandum znamená pochopitelně výrazný impuls pro dodavatele[2].

Evropa se nachází kdesi mezi těmito extrémy. Určitý zájem o IPv6 zde je, což dokládají počty prefixů přidělených koncovým sítím. Motivace je podobná Japonsku – snaha o podchycení perspektivní technologie, která může v budoucnu přinést zajímavé zisky. Přístup k IPv6 proto mezi evropskými poskytovateli Internetu není zcela vzácný, na druhé straně jej však nelze považovat ani za běžný jev.

Zajímavá je samozřejmě nabídka IPv6 mezi domácími poskytovateli Internetu, kterou jsem pro časopis *Lupa* mapoval v březnu 2005 – viz příloha L na straně 99. Osmnáct oslovených společností tvořili nejvýznamnější klasičtí poskytovatelé Internetu, celostátní distributoři kabelové televize a mobilní operátoři. Z nich dvě společnosti poskytovaly IPv6 již v době průzkumu a další tři byly připraveny je nabídnout či chystaly plošné nasazení této služby. Téměř 30 % nejvýznamnějších poskytovatelů datových služeb v ČR tedy na jaře roku 2005 poskytovalo IPv6 nebo k tomu alespoň podnikalo aktivní kroky. Průzkum však také ukázal mizivý zájem ze strany zákazníků o tuto službu, což je nepochybně hlavní příčinou popsaného stavu.

3.3 Akademické a experimentální sítě

Mezi propagátory a první implementátory IPv6 dlouhodobě patří národní sítě pro vědu, výzkum a vzdělávání (National Research and Education Networks, NRENs). V jejich případě není motivací nedostatek adres ani komerční úspěch, ale úsilí ověřovat nové technologie, protokoly a služby a nabízet svým uživatelům co nejmodernější a nejkomplexnější síťové prostředí.

Jak dokládá přiložený článek (příloha M na straně 103), již v první polovině roku 2003 bylo IPv6 k dispozici ve většině evropských NREN. Páteřní síť by

[2] Ovšem nelze přehlížet, že podobným způsobem americká administrativa ohlásila počátkem devadesátých let postupný přechod na protokoly OSI, k němuž nikdy nedošlo.

pokud možno měla být neutrální, proto bylo ve většině případů zvoleno řešení typu dual-stack s víceméně rovnocennou podporou obou protokolů. Vymykalo se pouze řešení přijaté německou sítí WiN, využívající pro IPv6 vyhrazené směrovače (navzdory mé předpovědi z roku 2003 toto uspořádání používají dosud).

Ze studie [41] vyplývá, že v zemích Evropské unie přibližně 10 % ze všech institucí připojených k národním akademickým sítím je zároveň připojeno i protokolem IPv6. Mezi univerzitami je podíl ještě vyšší – přibližně 15 %. Objem IPv6 provozu vůči IPv4 je i v těchto sítích malý, řádově jednotky procent. Pouze v ojedinělých případech překračuje hranici 10 %.

O rozšíření podpory IPv6 v akademických sítích svědčí i údaje o jejich napojení na páteřní evropskou infrastrukturu poskytovanou sítí **GÉANT**. S výjimkou Lotyšska mají všechny připojené NREN i připojení protokolem IPv6. Ve valné většině nativní, pouze Litva a Rakousko jsou zatím připojeny tunely.

Samotná páteřní síť GÉANT zavedla IPv6 poměrně pozdě. Oficiálně byl jeho provoz zahájen 19. ledna 2004, k praktické realizaci došlo během roku 2003. Skutečnost, že valná většina národních sítí uvádí jako dobu svého IPv6 připojení k páteři GÉANT rok 2003, svědčí o tom, že tyto sítě měly již v té době protokol implementován a byly na připojení připraveny. GÉANT, stejně jako většina národních sítí, se rozhodl pro dual-stack řešení s víceméně rovnocennou podporou IPv4 i IPv6.

Mezi experimentálními sítěmi má zcela unikátní postavení síť **6bone**. Vznikla v roce 1996, krátce po vydání první generace RFC definujících protokol a jeho základní mechanismy. Jejím cílem bylo především ověřovat jeho vlastnosti a implementace a získávat praktické zkušenosti s provozem IPv6 sítě. Síť 6bone byla koncipována jako virtuální. Neměla vlastní infrastrukturu, jednotlivé spoje byly typicky realizovány pomocí tunelů procházejících běžným IPv4 Internetem. Pro její účely byl vyhrazen speciální prefix 3ffe::/16 (původně 5f00::/8), podle nějž bylo možné adresy náležející síti 6bone na první pohled identifikovat.

Síť byla již při svém ustavení deklarována jako dočasná, jež bude po naplnění své úlohy zrušena. Když se po roce 2000 začalo IPv6 objevovat v páteřních sítích a regionální registrátoři začali přidělovat globální adresy s prefixem 2001::/16, začal postupný odklon koncových sítí od 6bone. Svého maxima síť dosáhla kolem roku 2003, kdy se počet připojených koncových sítí odhaduje na 1000 (vzhledem ke svému značně distribuovanému charakteru síť 6bone nikdy nevydávala oficiální statistiky).

Vzhledem ke zřetelnému poklesu zájmu a poklesu počtu připojených sítí vyšlo v březnu 2004 *RFC 3701: 6bone (IPv6 Testing Address Allocation) Phaseout* ohlašující konec používání jeho adres a tedy i ukončení činnosti celé sítě. K tomu došlo 6. června 2006 – po tomto datu již nejsou šířeny směrovací informace o prefixech začínajících 3ffe::/16 (viz příloha O na straně 111). Během deseti let

své existence síť 6bone, do níž byla naše univerzita také několik let zapojena, podstatným způsobem přispěla k poznání a rozvoji nového protokolu.

V jádru podobné cíle jako 6bone měla i síť **6NET**, realizovaná v rámci 6. rámcového programu EU. Tentokrát se však mělo jednat o „seriózní“ síť, tedy síť nativní, nikoli tunelovanou. Projekt se zaměřil na ověřování IPv6 a získávání praktických zkušeností s ním v prostředí podobném rutinnímu nasazení. Na řešení se podílely komerční firmy (v čele s Cisco Systems jako koordinátorem), většina účastníků však pocházela z akademického prostředí. Díky zapojení sdružení CESNET do projektu došlo počátkem roku 2003 ke zprovoznění prvního mezinárodního nativního IPv6 spoje v ČR. Jednalo se o spoj s rychlostí 155 Mb/s do uzlu sítě 6NET ve Frankfurtu nad Mohanem, využívaný výlučně pro nativní přenos IPv6.

Významným výstupem projektu 6NET byla kniha [26] poskytující informace o protokolu a jeho praktickém nasazení. Na jejím vzniku jsem se podílel autorstvím kapitol „IPv6 Basics“ a „Addressing“.

3.4 IPv6 v síti TEN-155 CZ a CESNET2

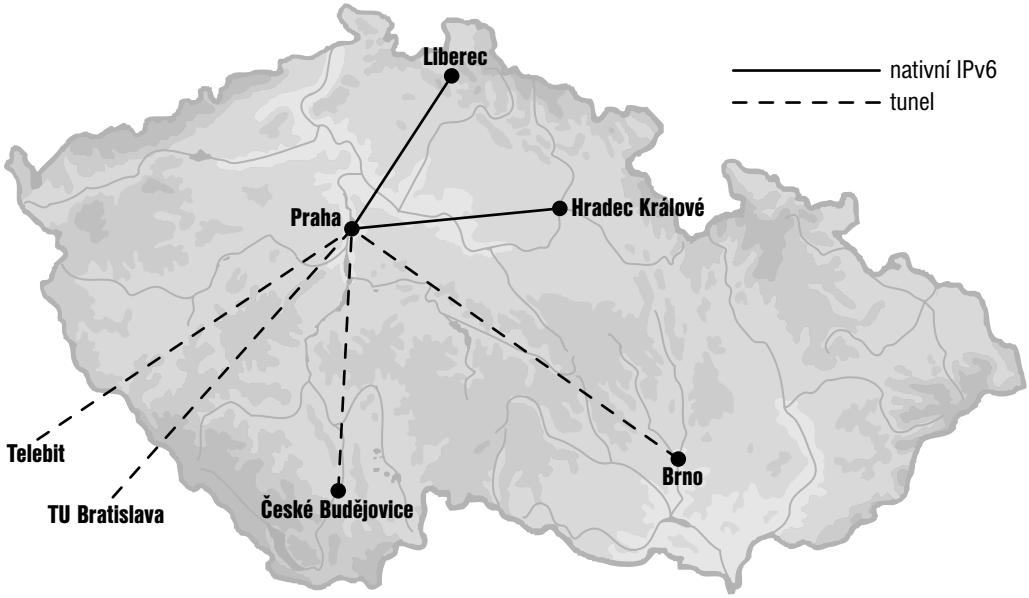
V letech 1999–2001 jsem vedl projekt sdružení CESNET, jehož cílem bylo zavedení pilotní podpory IPv6 do páteřní akademické sítě České republiky TEN-155 CZ a později CESNET2.

Jak dokládá zpráva [30], podpora IPv6 v dostupných produktech byla v té době velmi slabá. Cílem projektu bylo především získat praktické zkušenosti s novou verzí protokolu a jejími konkrétními implementacemi a na jejich základě vytvořit co nejpoužitelnější prostředí. Proto jsme v počáteční fázi zvolili různorodé platformy pro implementaci přístupových IPv6 směrovačů v jednotlivých koncových sítích.

Výraznou výhodou bylo použití technologie ATM v páteřní síti TEN-155 CZ. Jeho prostřednictvím bylo možné vytvořit virtuální okruhy vyhrazené pro IPv6 a realizovat tak některé spoje nativně, což bylo ve své době velmi unikátní řešení. Celá experimentální IPv6 síť byla napojena na síť 6bone prostřednictvím dvojice tunelů a adresována v rámci jejího adresního prostoru.

K významné změně došlo v roce 2001, kdy byla páteřní síť TEN-155 CZ nahrazena novou generací pod názvem CESNET2 (viz [32]). Ta přinesla výrazně vyšší přenosové rychlosti a řadu zajímavých vlastností, ovšem odklonila se od technologie ATM. Vzhledem k tomu, že technika použitá v jádru nové sítě nepodporovala IPv6, bylo jedinou možností jeho nasazení použití tunelů. Koncové IPv6 sítě byly proto s centrálním směrovačem propojeny tunely.

V roce 2001 došlo také k významné změně v adresování IPv6 sítě. Podařilo se nám získat produkční prefix 2001:718::/35 (později zkrácený na 32 bitů v souladu s pravidly RIPE NCC). Tou dobou se začal otázkou IPv6 intenzívněji



Obrázek 3.2: Topologie pilotní IPv6 sítě v roce 1999

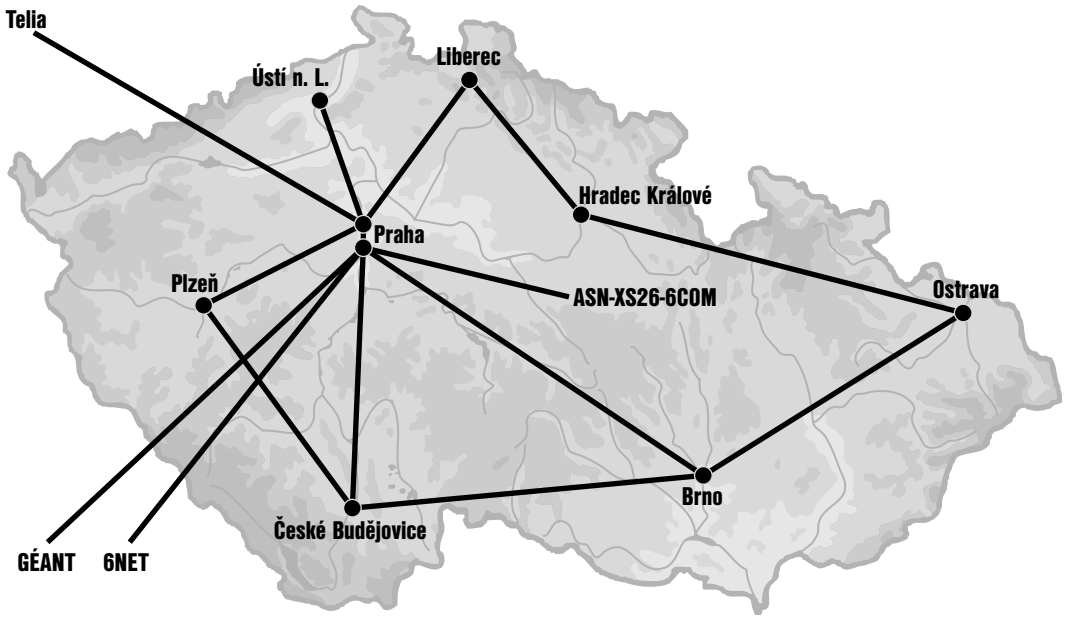
zabývat i tým rozvíjející evropskou síť GÉANT, od nějž jsme získali nový prefix pro 6bone adresy, konkrétně 3ffe:803d::/34.

Vypracovali jsme dokument definující adresní architekturu v síti provozované sdružením CESNET a pravidla pro přidělování adres koncovým sítím – viz [54]. Podle něj byl všem potenciálním sítím připojeným k libereckému uzlu sítě CESNET2 přidělen společný prefix 2001:0718:0500::/42. Síť TU v Liberci jako první reálně připojená pak získala prefix 2001:718:1c01::/48. Adresní architektura zmiňuje i prefixy pro 6bone, které však byly poměrně záhy opuštěny.

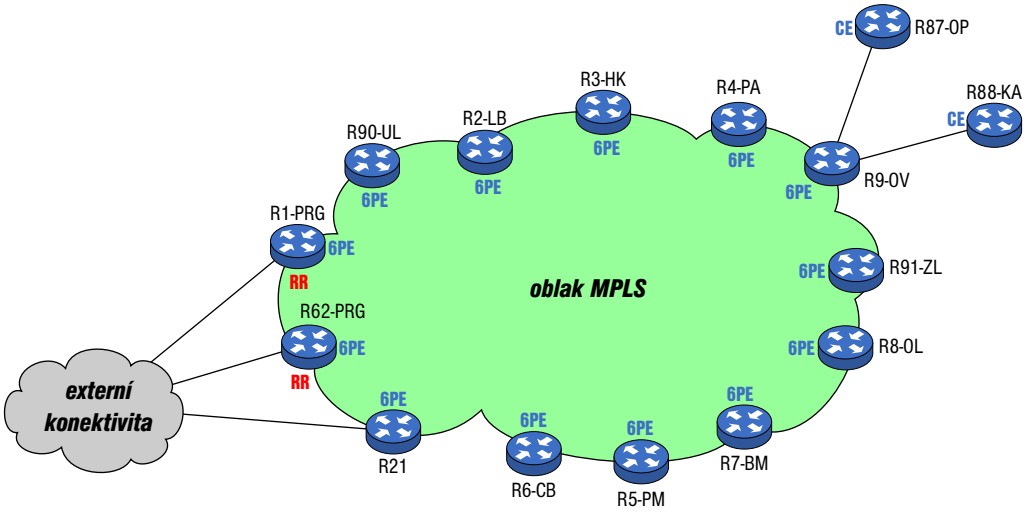
V roce 2002 byl změněna topologie tunelů tak, aby odpovídala fyzické topologii sítě a co nejvěrněji kopírovala IPv4 infrastrukturu – viz obrázek 3.3 a zprávu [33]. Stále však nebylo možné podporovat IPv6 v páteři nativně, jeho směrování doposud zabezpečovaly samostatné směrovače.

Nativní podpory a prakticky rovnocenného postavení IPv6 a IPv4 v páteřní síti se podařilo dosáhnout až o rok později nasazením technologie 6PE (viz [34]). Ta používá pro přenos IPv6 datagramů MPLS, stejně jako pro IPv4. Hraniční směrovače MPLS oblasti se navzájem informují o dostupných sítích prostřednictvím interního protokolu BGP (iBGP). Vzhledem k tomu, že celý přenos jádrem MPLS sítě se z pohledu IP jeví jako atomický, chová se síť, jako by všechny hraniční směrovače byly svými přímými sousedy. Z pohledu IPv6 je topologie páteře triviální – viz obrázek 3.4.

Výhodou 6PE je, že vyžaduje podporu pouze v hraničních směrovačích MPLS sítě, jejíž jádro může zůstat beze změny. Nabízí rovnocennou přepravu obou protokolů a lze je do sítě aplikovat postupně. Podrobněji je tento přístup popsán v příloze N na straně 107, úspěšně jsme jej prezentovali na konferenci *IPv6 Global Summit* v Barceloně [55].



Obrázek 3.3: Topologie páteřní IPv6 sítě v roce 2002



Obrázek 3.4: Topologie páteřní IPv6 sítě od roku 2003 po nasazení 6PE

Vzhledem k tomu, že řešení založené na 6PE má všechny potřebné vlastnosti, je v páteřní síti CESNET2 používáno dodnes a v nejbližší době se o jeho změně neuvažuje. Jeho nevýhodou je, že nepodporuje skupinově adresované datagramy (multicast), které jsou v současnosti stále směrovány dedikovanými směrovači. Provozní skupina CESNETu pracuje na vhodnějším řešení.

4 Univerzitní síť TU v Liberci

4.1 Vznik sítě

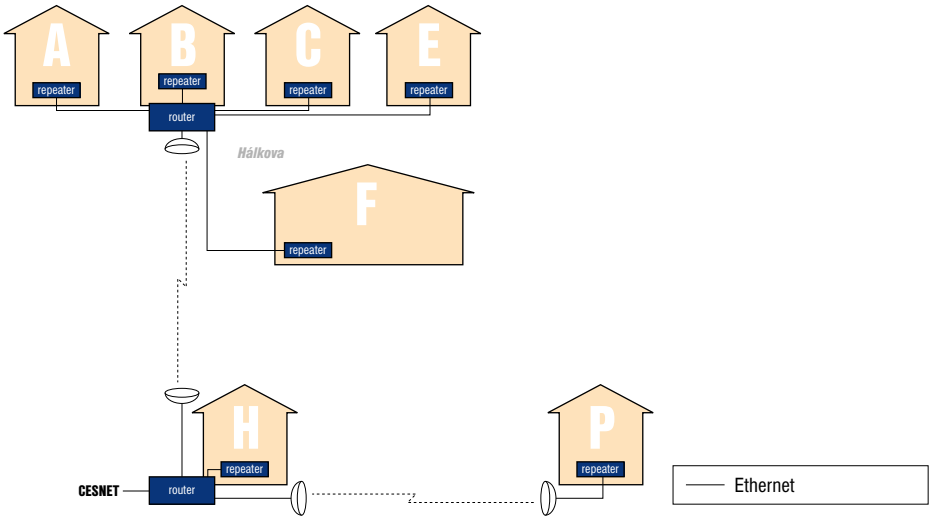
Zavedení počítačové sítě v prostředí Technické univerzity v Liberci (resp. tehdejší Vysoké školy strojní a textilní) se začalo připravovat počátkem devadesátých let 20. století. Její koncepční návrh jsem připravil ve spolupráci s RNDr. Petrem Kolářem ve druhé polovině roku 1991 a předložil jej společně s rámcovou cenovou kalkulací nákladů na realizaci vedení univerzity.

Návrh sítě s názvem LIANE (LIberec Academic NEtwork) byl postaven na technologii Ethernet a počítal s jejím zavedením do všech kanceláří a vybraných učeben nejvýznamnějších univerzitních budov. Ethernet byl v době návrhu k dispozici ve třech kabelážních variantách: silný a tenký koaxiální kabel a kroucená dvojlinka. Silný koaxiální kabel jsme zavrhli jako neperspektivní. Kroucená dvojlinka dosud nebyla ještě oficiálně standardizována a dostupná zařízení byla velmi drahá. Proto jsme pro realizaci jako nejvhodnější zvolili tenký koaxiální kabel. Vzhledem k jeho choulostivosti (možnost rozpojení segmentu u každé stanice) jsme se rozhodli pro rozvod použít EAD zásuvky a přípojné EDA kabely.

Síť byla navržena jako stromová. V každé budově byl umístěn jeden víceportový opakovač, do nějž se koncentrovaly segmenty tenkého koaxiálního kabelu procházející jednotlivými patry. Spoje z těchto opakovačů byly svedeny do centrálního multiprotokolového směrovače, mezi budovami byly spoje vedeny optickými vlákny. Pro zajištění centrálních síťových služeb se počítalo s operačním systémem Novell NetWare. V síťové vrstvě proto síť podporovala protokoly IP a IPX. Každá budova představovala z jejich pohledu jednu podsíť.

Jelikož předpokládané náklady na realizaci (více než 3 mil. Kč) přesahovaly možnosti univerzity, doporučilo vedení obrátit se na čerstvě vzniklý Fond dynamického rozvoje vysokých škol při MŠMT. Pro rok 1992 jsme připravili, získali a úspěšně realizovali projekt *Počítačová síť VŠST v Liberci*, na nějž v roce 1993 navázal projekt *Rošíření počítačové sítě VŠST v Liberci*. Řešitelem projektů byl prof. Vojtěch Konopa, tehdejší prorektor pro rozvoj, já jsem působil jako spoluřešitel a projekty jsem garantoval a realizoval po odborné stránce.

Výsledkem byla funkční síť výše popsané koncepce, jejíž topologii znázorňuje obrázek 4.1. Významný problém představovalo rozložení univerzity do několika lokalit. Kabelová infrastruktura tehdy v Liberci prakticky neexistovala a jednání s potenciálními dodavateli ukázala, že vhodné datové trasy propojující jednotlivé areály nelze pronajmout. Rozhodli jsme se proto pro bezdrátové řešení.



Obrázek 4.1: Topologie univerzitní počítačové sítě, 1993

Po průzkumu dostupných zařízení jsme vybrali a nasadili pojítko MR 23VXD kanadské firmy Microwave Radio Corporation. Jednalo se o unikátní zařízení, jež svou přenosovou rychlostí 10 Mb/s předčilo všechny běžně dostupné výrobky. Bezdrátovým spojem jsme realizovali páteřní trasu propojující hlavní areál univerzity Hálkova s budovou H, kde se nacházelo centrum datových komunikací. Vzhledem k velmi pozitivním zkušenostem jsme pak stejnou technologií realizovali i trasu mezi budovami H a P (jež byla z neznámých důvodů naopak zdrojem řady problémů a trpěla značnou nespolehlivostí).

Po připojení budov ve středu města (v roce 1994 přibyla budova S) se topologie mírně změnila. Byla nyní postavena na dvou směrovačích – směrovač v budově B propojoval podsítě v budovách hlavního areálu školy, směrovač v budově H pak podsítě budov v centru města. Z tohoto uspořádání vychází jádro sítě dodnes.

V době svého vzniku, na konci roku 1992, měla univerzitní síť problematické připojení k Internetu – akademická národní páteř teprve vznikala. Díky zapojení do projektu *Datennetz Dreiländereck* iniciovanému TH Zittau jsme získali připojení k německé univerzitní síti WiN. Bylo realizováno protokolem X.25, ten se však typicky využíval jen jako transportní pro IP datagramy, k intenzívnějšímu využívání služeb postavených přímo nad X.25 nikdy nedošlo. Náš přístup byl omezen na síť WiN, nejednalo se o plnohodnotné připojení k Internetu.

Velkým přínosem pro univerzitní síť bylo připojení k síti CESNET, jež bylo uvedeno do provozu na jaře 1993. Vedle dvojnásobné kapacity (19,2 kb/s, brzy povýšena na 64 kb/s) přineslo možnost komunikace s ostatními domácími univerzitami a také neomezený přístup do sítě Internet. Naše datová komunikace pochopitelně z valné většiny přešla do sítě CESNET a připojení k WiN bylo proto na podzim roku 1993 zrušeno.

Na konci roku 1993 byla valná většina hlavních prostor univerzity pokryta

kvalitní počítačovou sítí s připojením k Internetu. Za unikátní považuji, že se podařilo dosáhnout jednotné přenosové rychlosti 10 Mb/s v celé síti, včetně spojů mezi jednotlivými areály. Tím se uzavřela první etapa vývoje sítě LIANE, etapa vzniku sítě.

4.2 ATM – nenaplněné očekávání

Další rozvoj sítě byl motivován především snahou o zvýšení jejího výkonu – s rychle rostoucí mírou využití se postupně stávaly páteřní trasy úzkým místem. Proto jsme hledali vhodný způsob, jak zvýšit jejich přenosovou kapacitu. Na náš postup měly klíčový vliv dva faktory poloviny 90. let: vznikající infrastruktura optických kabelů a příchod nových síťových technologií, především ATM.

Hlavní překážkou zvýšení rychlosti páteřní sítě byly mikrovlnné trasy propojující jednotlivé areály. Bezdrátový přenos je z principu zatížen řadou problémů a rychlosti dosahované bezdrátovými pojítky vždy zaostávají za řešeními používajícími metalické či optické spoje, nemluvě o velmi vysoké ceně špičkových bezdrátových zařízení. Proto jsme se snažili najít vhodné propojení univerzitních areálů optickými vlákny. Standardním řešením je pronájem odpovídajících tras od vhodného poskytovatele.

Našim záměrům vyšel vstříc Český Telecom, který nabídl pronájem dvou vláken na klíčové trase mezi budovami B (Hálkova) a H (Voroněžská) za velmi přijatelných podmínek. Trasa měla být pronajata v podobě temných vláken, tedy jako pasivní optický spoj, jehož osazení přenosovou technikou si zajistí univerzita. Požadovaná cena představovala přibližně polovinu poplatku za pronájem kmitočtů pro bezdrátové pojítko. Nabídka představovala klíčový krok k vyšší kapacitě páteře a univerzita ji pochopitelně akceptovala.

Mezi síťovými odborníky panovala v polovině 90. let všeobecná shoda, že budoucnost patří technologii ATM. Ta nabídla přenosovou rychlost 155 Mb/s a krátce po ní i 622 Mb/s, příchod gigabitových rychlostí se očekával v horizontu dvou až tří let. Svými atraktivními vlastnostmi, jako je integrace datových a hlasových služeb či poskytování přenosových služeb se zaručenou kvalitou (Quality of Service, QoS) představovalo ATM jednoznačnou volbu.

V roce 1996 vyhlásilo MŠMT program TEN-34 CZ. Jednalo se o program navazující na evropský projekt TEN-34 usilující o vybudování evropské akademické páteřní sítě s rychlostí 34 Mb/s a pozvednutí evropských datových komunikací na úroveň srovnatelnou s USA. Na tento projekt navazovaly národní programy s podobnými cíli pro akademickou infrastrukturu evropských států. V rámci programu TEN-34 CZ vznikla stejnojmenná páteřní síť provozovaná sdružením CESNET, bylo však možné získat prostředky i pro adekvátní rozvoj univerzitních sítí.

Kolega Mgr. Jiří Randus připravil do programu projekt na zavedení ATM do páteře univerzitní sítě TU v Liberci. Předpokládal nahrazení stávajících směrovačů dvojicí ATM přepínačů. V jednotlivých budovách měly být ethernetové

rozbočovače postupně nahrazovány LAN přepínači napojujícími Ethernet na ATM páteř. Jejím základem měl být optický spoj B–H, pro nějž bylo počítáno s přenosovou rychlostí 622 Mb/s. Mělo se jednat o jenu z prvních instalací ATM trasy této rychlosti v ČR. Projekt byl přijat a v roce 1996 úspěšně realizován v tom smyslu, že byla pořízena potřebná technika (ATM přepínače Cisco LightStream 1010, směrovač Cisco 4700 a LAN přepínače Cisco Catalyst 5000 a 3000), nakonfigurována a připravena k nasazení.

To bohužel uvázlo na pronájmu optické trasy. Telecom ji sice technicky připravil, následně však radikálně změnil podmínky pronájmu. Jeho zástupci prohlásili původní nabídku za zmatečnou a odporující vnitřním pravidlům firmy. Kategoricky odmítli pronájem temných vláken a místo toho nabídli pronájem datové služby – nikoli pasivní optický spoj, ale „nasvícená“ vlákna napojená na ATM infrastrukturu poskytovatele. Praktickým důsledkem bylo snížení přenosové rychlosti na 155 Mb/s a navýšení ceny pronájmu na padesátinásobek původní nabídky, což bylo pochopitelně zcela nepřijatelné.

Následovala mnohaměsíční jednání, během nichž univerzita nabízela i odkoupení celé trasy. Telecom však jakýkoli jiný vztah než pronájem datové služby odmítal. Univerzita se nakonec rozhodla položit vlastní optický kabel – vzhledem k extrémně vysoké ceně datové služby činila návratnost této investice méně než rok. V roce 1998 došlo k položení optického kabelu, který propojil budovy H a B na vzdálenost cca 1 km osmi jednovidovými vlákny.

Ve druhé polovině roku 1998 tedy bylo možné instalovat připravenou ATM infrastrukturu v původní podobě. Standardizace v oblasti ATM ovšem mezitím pokročila, byly definovány nové signalizační protokoly a nadstavbové mechanismy. Zjistili jsme, že pokud bychom chtěli svou technologii doplnit o podporu těchto nových prvků, vyžadovalo by to investice v řádu stovek tisíc. Navíc se ukazovalo, že vývoj ATM zdaleka nepokračuje předpokládanou rychlostí a nad jeho budoucností se začaly objevovat první otazníky.

Nakonec jsme se rozhodli ATM zcela opustit a místo něj osadit páteřní trasy gigabitovým Ethernetem. Z dnešního hlediska se tento krok jeví jako jednoznačně správný, ovšem v roce 1998 se jednalo o velmi těžké rozhodnutí. V té době nebylo zdaleka jisté, zda zpomalení nástupu ATM je jen dočasným zaváháním, nebo zda se jedná o první příznak dlouhodobého vývoje. Pečlivým studiem dostupných informací jsme dospěli k závěru, že pravděpodobnější je druhá varianta a že bude výhodnější ATM co nejrychleji opustit. Pozdější léta nám pak dala za pravdu – např. páteřní síť CESNET2 opustila ATM v roce 2001.

Pokus o nasazení ATM představuje v historii sítě LIANE jediný významnější omyl, tato cesta se ukázala jako slepá. Snažili jsme se alespoň minimalizovat finanční ztráty – směrovač a LAN přepínače jsme využili v síťové infrastruktuře, ATM přepínače se nám podařilo odprodat. Domnívám se, že dvouletá přestávka vynucená změnou postoje Českého Telecomu a následným hledáním řešení pro vybudování optického spoje paradoxně přispěla k minimalizaci našich ztrát. Kdybychom ATM v roce 1996 nasadili do reálného provozu a

následně rozvíjeli, investovali bychom do něj s největší pravděpodobností podstatně větší prostředky a následně jej opouštěli později a bolestněji.

4.3 Třetí generace: kroucená dvojlinka a gigabitová páteř

Ve druhé polovině 90. let se spěla ke konci morální životnost koaxiálních rozvodů. Jimi poskytovaná rychlost 10 Mb/s stále dostačovala potřebám většiny uživatelů, servery a náročnější aplikace však požadovaly rychlejší připojení, jež se stávající kabeláží nebylo možné poskytnout. Standardním metalickým médiem pro Ethernet se stala kroucená dvojlinka. Pokud jsme chtěli síti nabídnout perspektivu dalšího rozvoje, bylo nutné přejít na tuto kabeláž.

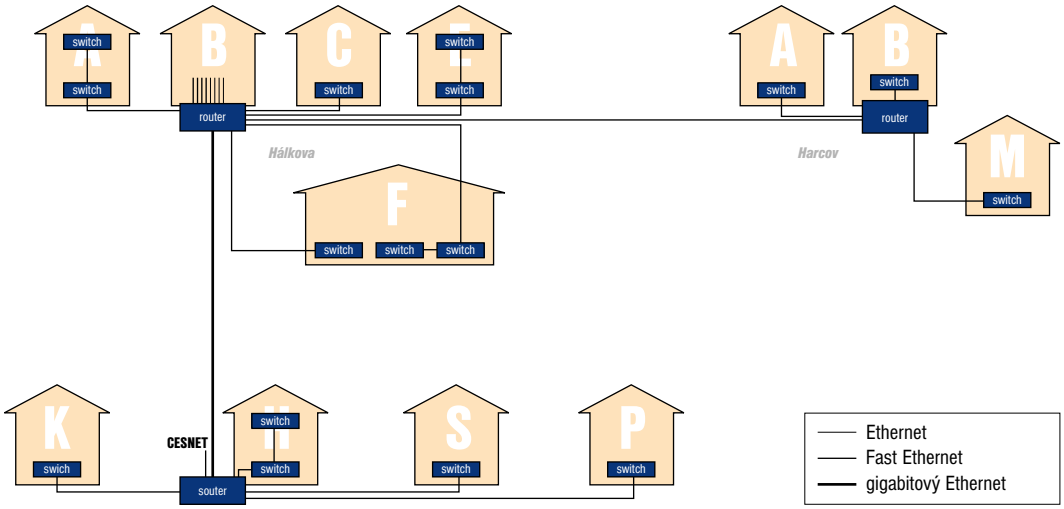
Proto jsem do programu Rozvoj informační infrastruktury výzkumu a vývoje podal projekt nazvaný Rozšíření rychlé páteře počítačové sítě TU v Liberci. Jeho cílem bylo změnit kabeláž v univerzitních budovách na kroucenou dvojlinku a připojit jednotlivé budovy vyšší rychlostí k páteřní síti. Projekt byl úspěšně realizován v letech 1998–2000.

Hned v prvním roce jeho řešení došlo k výše uvedené změně koncepce páteřní sítě, opuštění ATM a jeho nahrazení rychlými variantami Ethernetu. Konkrétně jsme centrální směrovače nahradili dvojicí L3 přepínačů Extreme Networks Summit 48. Na klíčovou trasu B–H jsme nasadili gigabitový Ethernet, jednotlivé budovy byly připojeny Fast Ethernetem s přenosovou rychlostí 100 Mb/s. Centrem rozvodů sítě v každé budově byl Fast Ethernet přepínač Cisco Catalyst 2924, na nějž byly napojeny jednoduché aktivní prvky připojující koncové počítače uživatelů. V počátečních fázích jsme používali ethernetové rozbočovače, po poklesu cen na přijatelnou úroveň jsme jako koncové prvky nasazovali Fast Ethernet přepínače. Uvnitř budov byl tedy zpočátku poskytován Fast Ethernet pouze omezeně serverům a náročným aplikacím, později však bylo jeho nasazení rozšiřováno, až po plošné pokrytí všech přípojných míst touto technologií.

Výsledný stav sítě po realizaci celého projektu vidíte na obrázku 4.2. Hlavní výhoda celého řešení spočívala v nasazení jednotné technologie Ethernet. Jednotlivé části sítě sice používaly jeho různé varianty s odlišnou rychlostí, formát rámce však zůstával jednotný, díky čemuž odpadly problémy s fragmentací a podobnými jevy. Také připojení k národní akademické síti bylo realizováno Fast Ethernetem, později gigabitovým Ethernetem.

Vzhledem k velmi ranému opuštění ATM se nám podařilo být jednou z prvních instalací gigabitového Ethernetu v ČR a tedy jednou z prvních sítí s gigabitovou páteří.

Paralelně s popsanou změnou koncepce páteřní sítě probíhalo i její postupné rozšiřování. Nejvýznamnější bylo nepochybně zavedení sítě v areálu studentských kolejí Harcov, které představují hlavní ubytovací kapacitu TU v Liberci. Síť zde byla budována postupně v letech 2000–2005, kdy jsme postupně rozšíře-



Obrázek 4.2: Topologie univerzitní počítačové sítě, 2000

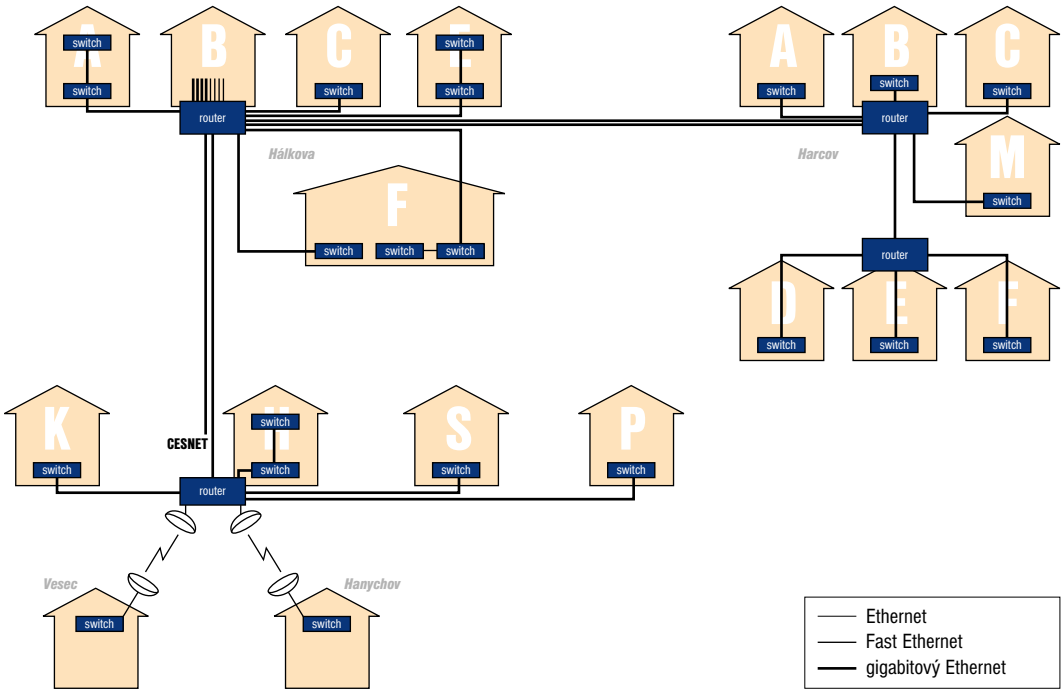
vali pokrytí jednotlivých budov a posilovali jejich páteřní propojení i připojení celého areálu k síti LIANE.

Rozvoj sítě harcovských kolejí byl podpořen několika úspěšně řešenými projekty FRVŠ: Zpřístupnění sítě TUL v objektu kolejí Harcov (rozvod sítě v budovách A a B, 2000), Rozšíření optické páteře počítačové sítě TU v Liberci (položení optické trasy propojující areál kolejí s areálem Hálkova, 2001), Rozšíření počítačové sítě na kolejích TU v Liberci (rozvod sítě v budově C, 2002), Internet v bloku D kolejí Technické univerzity v Liberci (rozvod sítě v budově D, 2003) a Dobudování počítačové sítě kolejí TU v Liberci (rozvod sítě ve zbývajících budovách E a F, gigabitové propojení budov, 2005).

4.4 Aktuální stav sítě

V roce 2004 uvolnilo vedení univerzity prostředky na náhradu centrálních aktivních prvků sítě. Dvojice L3 přepínačů Summit 48 byla nahrazena modulárním L3 přepínačem Cisco Catalyst 6500 v pozici centrálního směrovače sítě v areálu Hálkova a L3 přepínačem Cisco Catalyst 3750 v pozici centrálního prvku pro budovy ve středu města. Jejich nasazení umožnilo rozšířit gigabitové přenosové rychlosti plošně v celé páteři – všechny univerzitní budovy jsou v současnosti připojeny gigabitovým Ethernetem. Ten je v omezené míře dostupný i uvnitř budov pro uspokojení nejnáročnějších přenosových požadavků. Stejně jako v případě Fast Ethernetu před pěti lety postupně rozšiřujeme jeho pokrytí, všechny nově instalované aktivní prvky již podporují rychlosti 10, 100 i 1000 Mb/s.

Z hlediska kvantitativního se síť rozšířila i do nově získaných budov (budova K) a menších ubytovacích kapacit ve Vesci a Hanychově, takže v současnosti pokrývá kompletně celou univerzitu. Aktuální topologii najdete na obrázku 4.3.



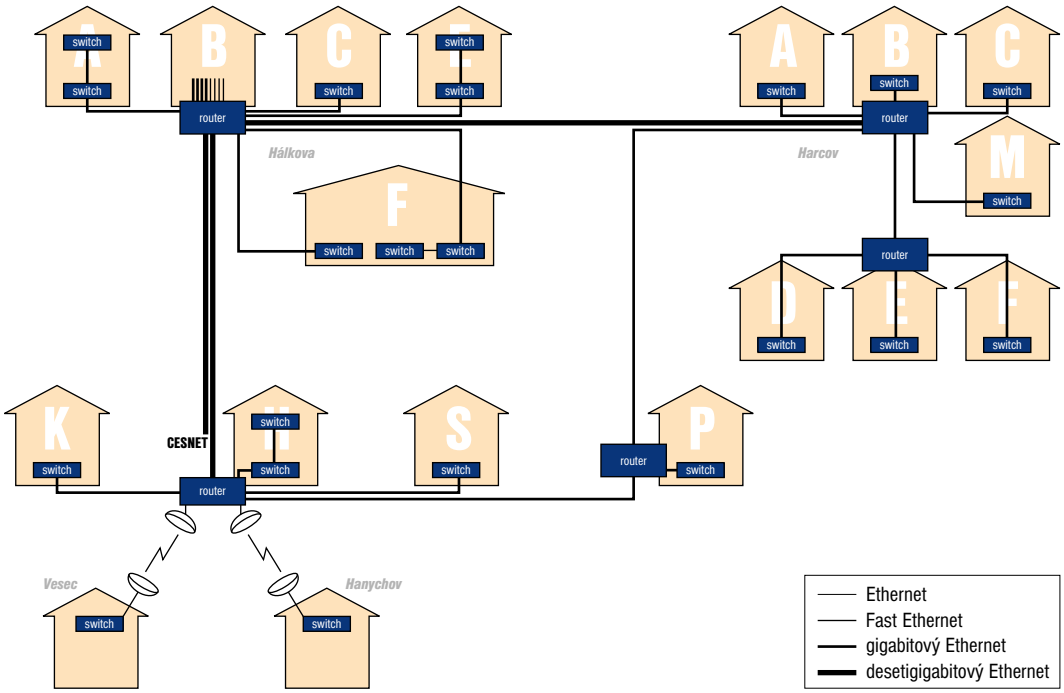
Obrázek 4.3: Současná topologie univerzitní počítačové sítě

K zajištění externí konektivity je LIANE napojena na síť CESNET2. Spojení je realizováno zálohovaným gigabitovým Ethernetem, uzel sítě CESNET2 se nachází v budově H. Na jeho správě se pochopitelně podílejí zaměstnanci TU.

Na její čistě ethernetové koncepci nemáme co měnit – Ethernet je dnes jednoznačně dominantní technologií lokálních sítí, jež zcela ovládl a vytlačil veškeré konkurenční platformy. Jedinou výjimku představují bezdrátové sítě, které však (alespoň v jejich současné podobě) mohou sloužit spíše jako doplněk než náhrada Ethernetu. Bezdrátová infrastruktura TU v Liberci je popsána v části 4.8 na straně 44.

Z hlediska infrastrukturního plánujeme pro blízkou budoucnost dvě významnější změny: První je nasazení desetigigabitového Ethernetu na nejexponovanější úseky sítě (trasy B–H a B–Harcov) pro zvýšení propustnosti těchto kritických úseků (a postupné šíření desetigigabitového Ethernetu pro připojení budov, až se tato technologie stane cenově dostupnější a datové objemy si tento krok vyžádají). Druhá změna představuje významný zásah do topologie – položením optického kabelu mezi koleje Harcov a budovu P chceme narušit stávající stromovou topologii a v centru sítě vytvořit okruh B–Harcov–P–H–B. Důvodem je především zvýšení robustnosti sítě, která se postupně stala podstatným prvkem vnitřního života TU a její rozpad na nepropojené části při případném přerušení některé z dálkových optických tras by byl velmi bolestivý. Proto plánujeme vytvoření redundantní trasy, jež by takové případy řešila.

Předpokládáme realizaci těchto dvou kroků do roku 2008. Plánovanou topologii sítě po jejich provedení zobrazuje obrázek 4.4.



Obrázek 4.4: Předpokládaná topologie univerzitní počítačové sítě v roce 2008

Jako síťový protokol převládá IPv4, jež je klíčovými prvky infrastruktury směrováno hardwarově, tedy ve vysokých rychlostech. Podporováno je i IPv6, což je hlavním tématem této práce a bude podrobně popsáno v následující kapitole. Z historických důvodů v jádru sítě zůstává podpora protokolu IPX, přestože centrální NetWare server sítě preferuje IP. Původně jsme předpokládali zrušení jeho podpory již během roku 2005, řada uživatelů však odmítá tento překonaný protokol opustit. Postupně se jej snažíme vyřazovat.

4.5 Adresace, směrování a registrace počítačů

Technická univerzita v Liberci má od roku 1992 přidělenu IPv4 adresu sítě třídy B, prefix 147.230.0.0/16. Její adresní prostor je rozhodně dostatečný. Pro jeho členění do podsítí jsme původně používali klasické schéma pro adresy třídy B na hranici mezi 3. a 4. bajtem (maska podsítě 255.255.255.0). S rostoucí velikostí sítě a počtem připojených počítačů však tento přístup přestával vyhovovat. Proto v současnosti používáme adresy podsítí nestejné délky. Podsítě v rámci LIANE lze rozdělit do tří skupin:

- podsítě budov mají prefix délky 21 bitů, v rámci budovy lze tedy adresovat přibližně 2000 zařízení

- koncové lokální podsítě (např. počítačové učebny kateder) mají prefix délky 24 bitů
- provozní podsítě používané na páteřních spojích sítě typicky propojují jen malý počet zařízení, proto jim přidělujeme zpravidla prefixy délky 29 bitů; všechny provozní sítě sdílejí společný 24bitový prefix, podle nějž lze jejich adresy snadno rozpoznat

Síť LIANE v současnosti zahrnuje přibližně 60 podsítí s veřejnými IP adresami. Tyto sítě jsou páteřními prvky směrovány. Typická konfigurace podsítě pro IPv4 v budově obsahuje

```
interface Vlan72
 ip address 147.230.72.250 255.255.248.0
 ip access-group budova_a_in in
 ip verify unicast source reachable-via rx allow-default
                                          allow-self-ping
 ip helper-address 147.230.16.1
 no ip redirects
 no ip unreachables
 ip pim sparse-mode
 ip route-cache flow
 ip igmp version 3
 load-interval 30
 service-policy input shape-dcc-pmap
```

Vedle konfigurace adres pro trojici podporovaných síťových protokolů (IPv4, IPv6, IPX) obsahuje i bezpečnostní prvky – přístupový seznam definující povolené/zakázané adresy pro danou podsíť (`ip access-group`) a kontrolu, zda adresa odesilatele přicházejících datagramů skutečně leží v dané podsíti (`ip verify`). DHCP požadavky se předávají centrálnímu serveru (`ip helper-address`).

Kromě podsítí adresovaných veřejnými IP adresami se v LIANE nacházejí dvě logicky zcela izolované podsítě, z bezpečnostních důvodů nedostupné z veřejných adres – síť účtáren a menzovní síť. Pro jejich adresaci používáme neveřejné adresy z rozsahů podle RFC 1918.

Zatímco síť účtáren používá vlastní, fyzicky oddělenou kabeláž, menzovní síť bylo třeba implementovat v rámci společné infrastruktury – jsou do ní zahrnuty vybrané části sítě v budovách F, H a na kolejích Harcov. Vzájemná komunikace těchto částí musí procházet společnými páteřními spoji. Pro její logické oddělení používáme virtuální sítě na bázi 802.1Q. Typická konfigurace páteřního rozhraní, jímž prochází menzovní síť, zahrnuje příkazy

```
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,12,254,260-262,533
```

```
switchport mode trunk
switchport nonegotiate
```

Páteřní prvky datagramy z této podsítě nesměrují (nemají ani přiděleny odpovídající adresy), chovají se k nim jako ethernetové přepínače. Celá menzovní síť se tedy vůči připojeným počítačům chová jako běžná lokální ethernetová síť, přestože je fyzicky rozložena v několika lokalitách a propojena netriviální infrastrukturou.

Pro výměnu směrovacích informací mezi páteřními prvky používáme protokol RIP verze 2. Vzhledem k jednoduché topologii bez alternativních cest jeho schopnosti dostačují potřebám sítě. Součástí plánovaného vytvoření redundantní topologie bude i přechod na sofistikovanější protokol, konkrétně OSPF.

Konfigurační parametry jsou připojeným počítačům poskytovány dynamicky protokolem DHCP. Pro jejich správu jsme vyvinuli vlastní registrační systém, který data o připojených počítačích ukládá do centrálního registru ve formátu XML. Na jeho základě pak generuje konfigurační soubory pro DHCP i DNS servery. Typická registrační data pro koncový počítač vypadají následovně:

```
<pocitac>
   <jmeno>onyx.kmp.tul.cz</jmeno>
   <interface>
      <ethernet>0020B4AA1948</ethernet>
      <podsit>p</podsit>
      <ip>147.230.32.92</ip>
      <ip6>0213:d3ff:fe5f:fe35</ip6>
   </interface>
   <kontakt>Kleopatra Tuha</kontakt>
   <umisteni>212A</umisteni>
</pocitac>
```

Na základě tohoto údaje pak systém generuje následující konfiguraci DHCP:

```
subnet 147.230.32.0 netmask 255.255.248.0 {
  option subnet-mask 255.255.248.0;
  option broadcast-address 147.230.39.255;
  option routers 147.230.32.250;
  option domain-name-servers 147.230.16.140, 147.230.16.1;
  option domain-name "tul.cz";
  default-lease-time 43200;
...
  host onyx.kmp.vslib.cz.p {
    hardware ethernet 00:13:D3:5F:FE:35;
    fixed-address 147.230.32.92;
  }
...
}
```

Vzhledem ke nikoli ojedinělé nekázni uživatelů (svévolné přidělování adres vedoucí ke konfliktům s registrovanými počítači) jsme se rozhodli ověřovat DHCP komunikaci (DHCP snooping) a až na explicitně uvedené výjimky povolovat datovou komunikaci jen počítačům, jež obdržely svou síťovou konfiguraci prostřednictvím DHCP a jsou tedy registrovány (ARP inspection). Díky těmto opatřením počet incidentů s „vypůjčenými“ adresami klesl na minimum. Celkově je v síti registrováno přibližně 5500 počítačů.

Stávající systém založený na registraci počítačů a přidělování pevné adresy a doménového jména na základě MAC adresy poskytuje dobrý přehled o počítačích v síti a jejich příslušnosti k jednotlivým univerzitním útvarům. Na druhé straně je však poněkud rigidní a rostoucí míra využívání notebooků a dalších mobilních zařízení pravděpodobně časem vynutí jeho změnu.

Jako perspektivní vidíme zachovat registrace a pevné adresy pouze pro servery, zatímco uživatelským počítačům budou adresy poskytovány náhodně z vyhrazených rozsahů. Přístup k síti bude řízen ověřením uživatele na bázi protokolu 802.1X, podobně jako v bezdrátové síti (viz část 4.8 na straně 44). Nasazení této metody zatím brání vysoká cena ethernetových přepínačů podporujících 802.1X. Pokrytí celé sítě tímto autentizačním protokolem by vyžadovalo investici v řádu několika milionů Kč, proto tento krok zatím odkládáme, dokud nebude 802.1X dostupné i v přepínačích nižších cenových kategorií.

4.6 DNS

Z hlediska DNS se univerzitní síť nachází v nepříjemné situaci. Dlouhodobě univerzita používala doménu druhé úrovně *vslib.cz*. V roce 2004 rozhodlo vedení školy na základě podnětu akademického senátu o strategické změně domény na *tul.cz*, jež odpovídá zavedené zkratce univerzity.

Změnu domény nelze provést skokově – doména figuruje v konfiguraci řady serverů a služeb a následky by byly příliš dramatické. Proto jsme vypracovali a postupně implementujeme plán plynulé změny domény. V jeho první fázi jsme zavedli doménu *tul.cz* jako alternativní k *vslib.cz* – doménová jména s koncovkou *tul.cz* byla zavedena jako přezdívky pro jména z domény *vslib.cz* a centrální služby byly konfigurovány tak, aby doménu *tul.cz* akceptovaly, standardně však používaly *vslib.cz*.

V současné době se nacházíme ve fázi druhé, kdy je pozice domén opačná: jako primární slouží *tul.cz*, zatímco *vslib.cz* představuje akceptovanou alternativu. Pro každou IP adresu jsou tedy v DNS zavedeny dva záznamy – záznam A v doméně *tul.cz* a záznam CNAME v doméně *vslib.cz*. Například

```
bubo.tul.cz.    A       147.230.16.1
bubo.vslib.cz.  CNAME   bubo.tul.cz.
```

Reverzní záznam PTR pochopitelně obsahuje kanonickou adresu

```
1.16.230.147.in-addr.arpa.  PTR  bubo.tul.cz.
```

Již od počátku jsme se rozhodli strukturovat DNS podle kateder a útvarů. Každému z nich je přidělena samostatná doména třetí úrovně, do níž jsou zařazovány registrované počítače. Toto schéma se velmi osvědčilo a podstatným způsobem usnadňuje orientaci v připojených počítačích. Celkem existuje v současnosti přibližně 80 těchto útvarových poddomén.

Primární DNS server se nachází v univerzitní síti, sekundární server nám poskytuje sdružení CESNET a je fyzicky umístěn v Praze. Kromě toho jsme v síti instalovali pomocný DNS server, na nějž se místní klienti obrací se svými dotazy. Cílem tohoto uspořádání bylo především odlehčit primárnímu serveru.

4.7 Správa uživatelů

Původní koncepce uživatelských služeb byla postavena na operačním systému Novell NetWare, který počátkem 90. let představoval de facto jedinou použitelnou platformu pro poskytování služeb systémům na bázi MS DOS. Všichni uživatelé byli registrováni na centrálním serveru TYTO, kde měli k dispozici určitý diskový prostor, omezenou nabídku aplikací a elektronickou poštu zajišťovanou programy Pegasus Mail a Mercury.

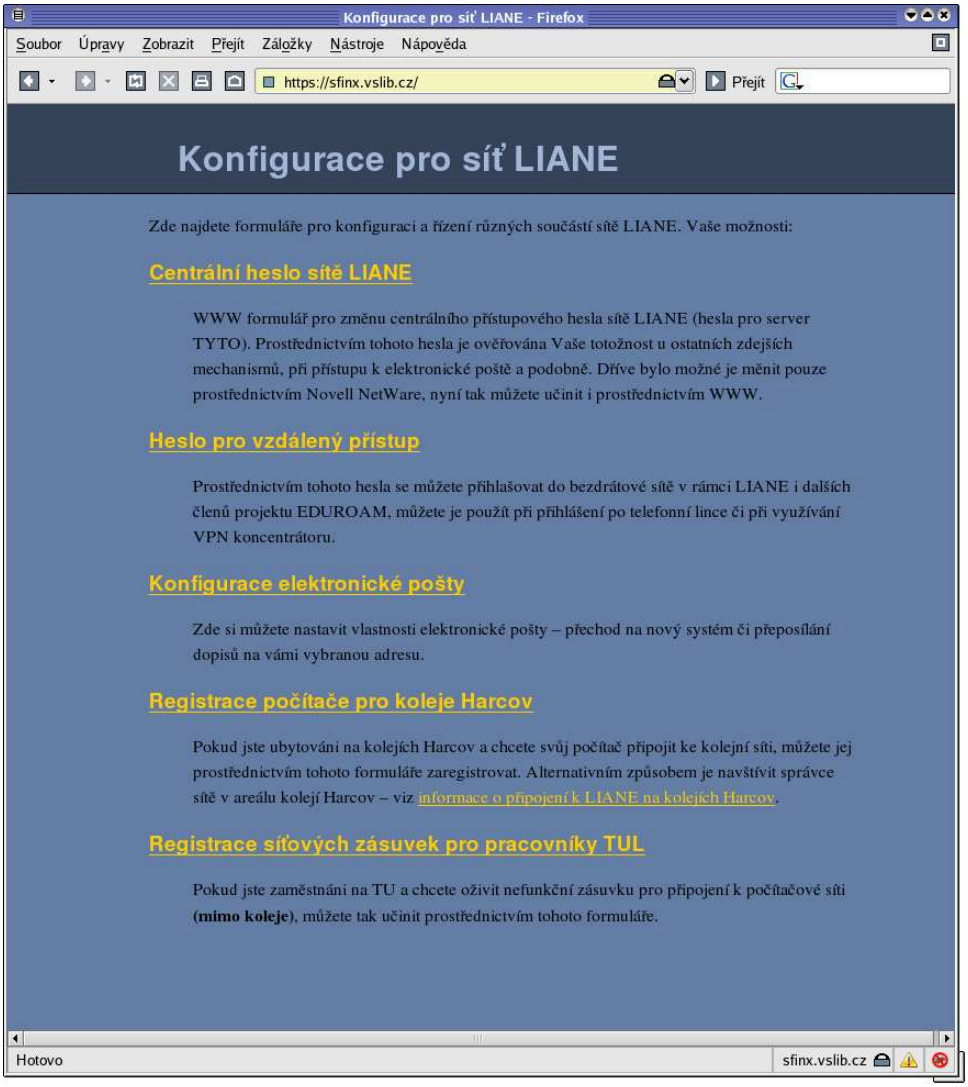
Určité prvky z této koncepce zůstaly zachovány do dnešních dnů. Uživatelé jsou stále registrováni na centrálním NetWare serveru. Jeho hlavní úlohou však v současnosti je poskytovat autentizační služby protokolem LDAP a umožnit tak centrální správu uživatelů, jejich hesel a přístupových práv. Tato služba je postavena na bázi Novell eDirectory. Stejnou platformu používáme i pro replikaci LDAP informací.

Každý uživatel LIANE, jimiž se automaticky stávají všichni zaměstnanci a studenti TU v Liberci, tedy dostane uživatelské jméno a přístupové heslo pro centrální adresářovou službu. V současné době centrální LDAP server obsahuje přibližně 8 000 aktivních uživatelů. Základem údajů uložených v LDAP je specifikace EduPerson (viz [28]) rozšířená o několik atributů pro specifické potřeby TUL. Odvození údajů od základu EduPerson usnadní naše zapojení do autentizačních federací, jež se v současnosti formují v rámci CESNETu i mezinárodních projektů.

Nikterak ojedinělým problémem naší univerzity je, že zde existuje řada dalších informačních systémů (například studentská matrika STAG, menzovní objednávkový systém a další), pocházejících z různých zdrojů, procházejících vlastním vývojem a budujících si vlastní databáze uživatelů a jejich hesel. Tyto systémy byly často nasazovány ještě před zprovozněním LDAP serveru, nebo se jejich autoři o problematiku správy uživatelů a heterogenního prostředí uživatelských služeb příliš nestarali. V současné době usilujeme o sjednocení správy uživatelů v těchto systémech a jejich postupné navázání na centrálně poskytovaný LDAP adresář. Přestože se nám podařilo dosáhnout dílčích úspě-

chů, potrvá nepochybně několik let, než se podaří navázat všechny systémy na centrálně poskytované uživatelské informace.

Prostřednictvím svého centrálního uživatelského jména a hesla má každý uživatel přístup k sadě konfiguračních formulářů, jimiž může nastavovat parametry síťových služeb, registrovat počítač a podobně (viz obrázek 4.5). Jejich nabídku a možnosti postupně rozšiřujeme, aby uživatelé byli pokud možno co nejnezávislejší na správě sítě a mohli si vše potřebné nastavit sami.



Obrázek 4.5: Konfigurační formuláře sítě LIANE

Centrální LDAP server je napojen na autentizační infrastrukturu projektu eduroam, jež umožňuje roaming akademických uživatelů mezi zapojenými institucemi. Naši uživatelé se tedy mohou připojovat k Internetu i v sítích jiných institucí, aniž by pro ně místní správci museli cokoli definovat či konfigurovat. Podrobnější popis projektu najdete v příloze Q na straně 115.

Především s ohledem na infrastrukturu eduroam, jejíž některé části, které se

nacházejí mimo naši kontrolu, přenášejí uživatelská jména a hesla v otevřené či slabě šifrované podobě, jsme se rozhodli založit pro uživatele oddělená hesla pro externí přístup k síti. Těchto hesel se používá pro připojení bezdrátovou sítí, telefonické připojení či připojení k VPN koncentrátoru. Heslo pro externí přístup k síti není uživatelům zakládáno centrálně, vytváří si je každý samostatně v případě potřeby. Slouží k tomu jeden z výše uvedených konfiguračních formulářů.

4.8 Bezdrátová síť

Infrastrukturu pro bezdrátové připojení na bázi protokolu IEEE 802.11a/b/g jsme začali vytvářet poměrně pozdě, v roce 2004. Dříve však nebyl ze strany uživatelů patrný výraznější zájem. Vznik bezdrátové sítě byl podpořen projektem *Podpora mobility na TU v Liberci* z Fondu rozvoje sdružení CESNET z. s. p. o., jehož řešitelem byl Petr Adamec.

Na bezdrátovém připojení se podílejí dva významné funkční celky: vlastní bezdrátová síť tvořená přístupovými body a autentizační infrastruktura řídící přístup k ní. Bezdrátovým signálem jsme se snažili v první fázi pokrýt především ty lokality, kde dochází k významnější koncentraci studentů vybavených přenosnou výpočetní technikou a kde mají možnost tuto techniku používat. Proto jsme přístupové body instalovali přednostně do univerzitní knihovny, menz a přilehlých kaváren a do velkých poslucháren. Později jsme postupně signál šířili i do méně exponovaných prostor. Do sítě bylo zapojeno i několik přístupových bodů pořízených katedrami, jež chtěly pokrýt své učebny.

Přístupové body jsou napojeny na standardní infrastrukturu sítě LIANE, kde je pro ně vytvořena samostatná virtuální síť, oddělená od ostatních.

V současné době je instalováno již více než 25 přístupových bodů. Vzhledem k tomu, že jejich řízení a správa bezdrátové sítě tohoto rozsahu již přestává být jednoduchou záležitostí, podali jsme do Fondu rozvoje sdružení CESNET z. s. p. o. další projekt *Rozvoj bezdrátové sítě Technické univerzity v Liberci* (řešitelem je opět Petr Adamec). Jeho cílem je vedle rozšíření počtu přístupových bodů především instalace centrálního řízení bezdrátové infrastruktury založeného na zařízení Cisco 4400 WLAN Controller a programu Cisco Wireless Control System. Projekt je momentálně posuzován. Bude-li přijat, dojde k jeho realizaci do poloviny roku 2007.

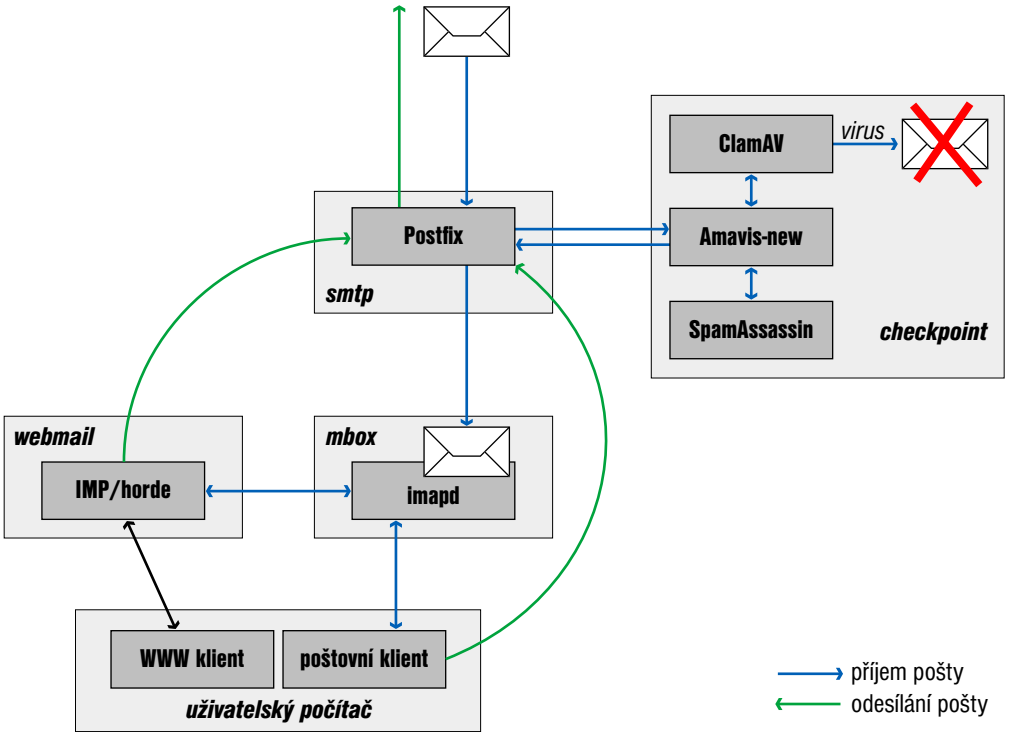
Autentizační mechanismy bezdrátové sítě jsou postaveny na protokolu IEEE 802.1X a využívají protokol RADIUS. Univerzitní autentizační server bezdrátové sítě je postaven na programu FreeRADIUS a napojen na infrastrukturu eduroam. V podstatě slouží jako směrovač autentizačních požadavků, kdy podle uživatelského realmu předává autentizační požadavky buď lokálnímu LDAP serveru zmíněnému v předchozí části, nebo národnímu RADIUS serveru, pokud se jedná o hostujícího uživatele z jiné instituce. Konfiguraci bezdrátové sítě, včetně implementace všech tří typů autentizace podporovaných projek-

tem eduroam jsme podrobně popsali v technické zprávě [53], která tvořila jeden z výstupů projektu.

Pro ověření uživatele se využívá výše zmíněné heslo pro externí přístup do sítě LIANE. Toto heslo si vytvořilo (a bezdrátovou síť využívá) již více než 300 uživatelů. Jejich počet soustavně roste.

4.9 Služby

Nejvyužívanější centrální službou univerzitní sítě je elektronická pošta. Její uspořádání znázorňuje schéma 4.6. Příjem a odesílání dopisů zajišťuje program Postfix na centrálním serveru *smtp.tul.cz*. Při příchodu jsou dopisy kontrolovány programem Clam AntiVirus, zda neobsahují některý ze známých virů. V případě pozitivního nálezu je dopis zlikvidován.



Obrázek 4.6: Poštovní systém TU v Liberci

Následuje kontrola programem SpamAssassin, který na základě heuristických analýz označuje dopisy, jež pravděpodobně obsahují nevyžádané reklamní materiály (spam). Na rozdíl od virů není detekce spamu zcela spolehlivá. Proto jsou dopisy považované za spam pouze označeny (vložením řetězce ***SPAM*** na začátek hlavičky Subject a připojením rozšiřujících hlaviček X-Spam-... poskytujících podrobnější informace) a doručeny uživatelům. Ti si mohou na základě informací v hlavičkách sami rozhodnout, jak s dopisy naložit – například nastavit automatický přesun do určité složky či vymazání.

Finálně jsou dopisy uloženy do poštovních schránek na serveru *mbox.tul.cz*. Uživatelé k nim mohou přistupovat buď přímo poštovními klienty protokolem IMAP, nebo s využitím WWW rozhraní poskytovaného serverem *webmail.tul.cz*. Toto rozhraní interně pro práci se schránkou také využívá protokol IMAP. V obou případech je komunikace šifrována (IMAPS, HTTPS).

K odesílání pošty slouží server *smtp.tul.cz*, na nějž se obracejí poštovní klienti či WWW rozhraní. V otevřeném režimu akceptuje dopisy k odeslání pouze ze sítě TU, při použití šifrování a autentizace uživatele lze jeho prostřednictvím odeslat dopis odkudkoli z Internetu.

Další centrálně poskytovanou službou je pracovní prostor na serverových discích. Ten byl využíván především studenty díky své dosažitelnosti ze všech počítačů zapojených do LIANE. Některé katedry také tuto službu využívaly pro distribuci výukových materiálů studentům. Ovšem s rostoucí dostupností USB pamětí, používáním notebooků studenty a všeobecným přechodem poskytování informací na platformu WWW postupně pozbývá na významu a její využívání klesá. Služba je z historických důvodů poskytována serverem Novell NetWare a nepočítáme s jejím přenosem na jinou platformu. Spíše bude ve více či méně vzdálené budoucnosti ukončena jako nepotřebná.

Centrální servery sítě LIANE pochopitelně poskytují obvyklé všeobecné informační služby, jako je WWW (*www.tul.cz*), FTP (*ftp.tul.cz*) či hosting fakultních a katedrálních WWW serverů. Další poskytované služby (např. on-line přístup ke studentské matrice, menzovní objednávkový systém, diskusní fóra a podobně) jsou provozovány útvary mimo správu LIANE.

5 IPv6 v síti LIANE

Motivace pro zavedení IPv6 do univerzitní sítě je podobná jako v případě NREN – snaha poskytnout uživatelům co nejmodernější služby a přispět k rozvoji a prosazení nového protokolu, jehož všeobecné přijetí by pro Internet znamenalo významný přínos. Proto jsme se snažili již ve velmi raných fázích nabídnout našim uživatelům možnost využívat IPv6.

5.1 Infrastruktura a adresace

Liberecký uzel patřil do první vlny sítí připojených na experimentální IPv6 páteř sdružení CESNET, díky čemuž byl protokol pro naše uživatele dostupný již od roku 1999 – viz mapka 3.2 na straně 28. Prvky Extreme Networks Summit 48, které tehdy tvořily páteř sítě, bohužel IPv6 nepodporovaly a nedokázaly jej směrovat. Měly ovšem jinou vlastnost, jež umožňovala zavést IPv6 do sítě LIANE v nativní podobě – protokolové virtuální sítě.

Pokud se na jednom rozhraní nachází více virtuálních sítí, je obvyklou metodou jejich rozlišení použití značek podle IEEE 802.1Q. Summit 48 kromě toho umožňoval definovat podsíť, do níž zařazoval přicházející pakety, které sice neměly žádnou 802.1Q značku, ale patřily určitému protokolu síťové vrstvy. Vzhledem k tomu, že IPv6 má v Ethernetu přiřazen odlišný identifikátor protokolu (86dd hexadecimálně) než IPv4 (identifikátor 0800), bylo možné tímto způsobem definovat virtuální síť zahrnující pouze IPv6 pakety. Vzhledem k tomu, že centrální prvky nedovedly IPv6 směrovat a provoz byl minimální, rozhodli jsme se dočasně pokrýt celou LIANE jednou podsítí, takže prostřednictvím IPv6 spolu mohly všechny počítače komunikovat přímo.

Síť LIANE tak v roce 1999 disponovala nativní podporou protokolu IPv6 – nativní bylo její připojení k národní páteři i distribuce protokolu uvnitř sítě. To bylo velmi ojedinělé v době, kdy drtivá většina IPv6 komunikace probíhala tunelovaně.

Po pořízení nové generace centrálních směrovačů podporujících směrování IPv6, k němuž došlo v roce 2004, jsme mohli přepracovat strukturu adresování a přepravy IPv6 do aktuální podoby, již považujeme za definitivní. V ní struktura IPv6 podsítí odpovídá podsítím IPv4 – oba protokoly jsou tedy topologicky homogenní. Každá univerzitní budova tedy obsahuje jednu základní podsíť pro IPv4 i IPv6.

Pro adresaci používáme prefix 2001:718:1c01::/48, který jsme získali od sdružení CESNET v roce 2001 v rámci adresní politiky deklarované v [54]. Jedná se

o produkční prefix z rozsahu spravovaného RIR. Abychom usnadnili orientaci v IP podsítích, používáme pro IPv6 podsítě identifikátory se stejným zápisem jako pro IPv4. Například podsíť budovy A má identifikátor 72. Její IPv4 prefix tedy je 147.230.72.0/21 a IPv6 prefix 2001:718:1c01:72::/64. Identifikátory mají odlišnou hodnotu, protože pro zápis IPv4 adres se používá soustava desítková, zatímco pro IPv6 šestnáctková, vnější podobnost však považujeme pro přehlednost za důležitější.

Typická základní konfigurace rozhraní páteřního směrovače Cisco Catalyst 6500 (resp. 3750), zahrnující obě podsítě, pak vypadá následovně:

```
interface Vlan72
! IPv4
 ip address 147.230.72.250 255.255.248.0
 ip access-group budova_a_in in
 ip verify unicast source reachable-via rx allow-default
                                          allow-self-ping
 ip helper-address 147.230.16.1
 no ip redirects
 ip pim sparse-mode
 ip route-cache flow
 ip igmp version 3
 load-interval 30
 service-policy input shape-dcc-pmap
! IPv6
 ipv6 address 2001:718:1C01:72::beef/64
 ipv6 access-class budova_a_ip6_in in
 ipv6 verify unicast source reachable-via rx allow-default
                                          allow-self-ping
 no ipv6 redirects
```

Pro identifikátory rozhraní používáme většinou standardní modifikované EUI-64 identifikátory odvozené z linkových (MAC) adres síťových rozhraní. Výjimku představují rozhraní, na nichž jsou poskytovány síťové služby – například adresy DNS serverů či rozhraní centrálních směrovačů vedoucí do sítí jednotlivých budov, jež slouží jako implicitní brány pro všechny zapojené počítače. Závislost těchto adres na hardwarovém zařízení považujeme za nežádoucí, protože případná výměna zařízení (k níž nutně během několika let dochází) by znamenala netriviální zásahy do konfigurací řady prvků[1], riziko nekonzistence a značnou pravděpodobnost narušení konektivity některých zařízení. V případě servisní výměny zařízení při poruše by pak došlo k nežádoucímu prodloužení výpadku služby. Proto pro takováto rozhraní „veřejné služby“ používáme explicitně stanovené adresy, neodvozované od fyzických. Například centrální DNS servery mají adresy 2001:718:1c01:16::aa

[1] Valná většina počítačů a zařízení zapojených do sítě je sice konfigurována automaticky, existují však výjimky.

a 2001:718:1c01:16::bb, zmiňovaná významná rozhraní centrálních směrovačů používají identifikátor beef.

5.2 Konfigurace uživatelských počítačů

Pro konfiguraci síťových parametrů uživatelských počítačů jsme se rozhodli použít bezstavovou automatickou konfiguraci v kombinaci s bezstavovým DHCP pro doplnění informací o DNS, které vlastní bezstavová konfigurace nedokáže poskytnout (viz příloha H na straně 81). V pozadí tohoto našeho rozhodnutí dát přednost bezstavové konfiguraci před stavovou prostřednictvím DHCPv6 stála jednak snaha maximálně usnadnit uživatelům použití IPv6, jednak výše zmiňovaná vize perspektivního řízení přístupu k síti na základě autentizace uživatelů, nikoli jejich hardwaru.

Na konfiguraci centrálních směrovačů pro aktivaci bezstavové automatické konfigurace není třeba prakticky nic měnit – implicitně posílají do připojených sítí ohlášení směrovače obsahující prefixy zdejších sítí (podle adres přidělených rozhraní) i představení sebe sama jako možného implicitního směrovače pro IPv6. Jedinými změnami proti implicitnímu nastavení bylo zvýšení priority směrovače v ohlášení příkazem

```
ipv6 nd router-preference high
```

a doplnění bezstavového DHCP. Roli bezstavového DHCP serveru mohou hrát přímo centrální směrovače, jejich operační systém nabízí potřebné funkce. Aktivace vyžaduje několik kroků. Jednak je třeba definovat parametry, jež budou tímto mechanismem počítačům předávány (adresy lokálních DNS serverů a implicitní doménu):

```
ipv6 dhcp pool tuldhcp
  dns-server 2001:718:1c01:16::bb
  dns-server 2001:718:1c01:16::aa
  domain-name ip6.tul.cz
```

Pro příslušné rozhraní je následně třeba zapnout používání tohoto mechanismu. Jednak odkazem na něj (teoreticky může existovat několik různých sad parametrů předávaných do různých rozhraní) a jednak zahrnutím příznaku pro použití DHCPv6 ke konfiguraci jiných síťových parametrů než adresy. Nastavení rozhraní pro automatickou konfiguraci proto zahrnuje následující příkazy:

```
interface Vlan72
 ipv6 nd router-preference high
 ipv6 nd other-config-flag
 ipv6 dhcp server tuldhcp
```

Na základě poskytnutých informací si koncové počítače jsou schopny nastavit adresu – například

```
inet6-adr: 2001:718:1c01:16:214:22ff:fec9:72c/64 Rozsah:Globál
inet6-adr: fe80::214:22ff:fec9:72c/64 Rozsah:Linka
```

i základ směrovací tabulky (fe80::211:5dff:feb7:f400 je lokální linková adresa rozhraní centrálního směrovače):

```
2001:718:1c01:16::/64                    dev eth0
fe80::/64                                dev eth0
ff00::/8                                 dev eth0
default via fe80::211:5dff:feb7:f400     dev eth0
unreachable default                      dev lo
```

Inicializují si také parametry DNS, pokud podporují bezstavové DHCPv6:

```
search ip6.tul.cz
nameserver 2001:718:1c01:16::bb
nameserver 2001:718:1c01:16::aa
```

Bohužel podpora bezstavového DHCPv6 je zatím na dost špatné úrovni. Jeho použití zatím většinou vyžaduje instalaci vhodného DHCP klienta, jakým je například program Dibbler.

5.3 Směrování

Vzhledem k tomu, že strategicky plánujeme v sítí přejít na výměnu směrovacích informací protokolem OSPF, rozhodli jsme se pro směrování IPv6 použít OSPFv3. Pro stávající síť se stromovou topologií by sice stačil i jednodušší RIPng, zvolili jsme však sofistikovanější OSPF s výhledem na připravovanou redundantní topologii. Jednoduchá topologie sítě nevyžaduje hierarchické směrování a členění na oblasti. Celá síť je navržena jako jedna OSPF oblast s identifikátorem 0.

Konfigurace centrálních směrovačů je poměrně jednoduchá. Na globální úrovni obsahuje pouze aktivaci směrování a nastavení základních vlastností OSPF procesu:

```
ipv6 unicast-routing

ipv6 router ospf 20
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan516
 no passive-interface Vlan533
 no passive-interface Vlan565
```

OSPF nešíříme do všech rozhraní. Proto je distribuce OSPF zpráv implicitně potlačena (`passive-interface default`) a aktivována jen pro vybraná rozhraní (zde páteřní linky).

Jednotlivá rozhraní, jejichž podsítě mají být OSPF šířeny, pak jsou zahrnuta do OSPF oblasti 0 příkazy `ipv6 ospf` v konfiguraci rozhraní:

```
interface Vlan72
 ipv6 ospf 20 area 0
```

Páteřních spoje, jež propojují vždy jen dva sousední směrovače, pak explicitně deklarujeme jako dvoubodové, abychom poněkud snížili režii OSPF (odpadá volba směrovače „zodpovědného“ za podsíť). Zároveň zde snižujeme interval mezi zprávami HELLO, aby byla konvergence co nejrychlejší:

```
interface Vlan516
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf 20 area 0
```

Koncové počítače jsou zpravidla směrovány staticky pouze na základě implicitní směrovací tabulky získané automatickou konfigurací (viz výše).

5.4 DNS

Program BIND verze 9, který používáme pro realizaci univerzitních DNS serverů, podporuje IPv6. Aby poskytoval informace i protokolem IPv6, stačí aktivovat protokol v hostitelském počítači a do konfiguračního souboru */etc/named.conf* zařadit příkaz

```
listen-on-v6 { any; };
```

Pro poskytování informací o IPv6 adresách univerzitních strojů stačí do zónových souborů zařadit odpovídající AAAA záznamy. Nejdůležitějším rozhodnutím souvisejícím s DNS bylo, jak tyto AAAA záznamy strukturovat a kterým jménům je přidělovat. Existují dvě základní strategie: používat pro IPv4 (A) i IPv6 (AAAA) stejné jméno, nebo záznamy pojmenovat odlišně.

Výhodou přiřazení dvou typů záznamů pod stejné jméno je, že se zachovává integrita počítače z hlediska DNS a komunikující počítače si mohou podle svých schopností vybrat protokol pro vzájemnou komunikaci. Problém nastává, pokud je takto v DNS zaveden počítač nepodporující IPv6. V takovém případě studie praktického nasazení IPv6 ukazují, že při navazování komunikace může dojít k významnému zpoždění (pokud protějšek zvolí IPv6, čeká se desítky sekund na vypršení časové lhůty, než se pokusí použít IPv4)

Použití tohoto přístupu vyžaduje, aby DNS přesně korespondovalo se stavem uživatelských počítačů a zavádělo AAAA záznamy jen pro jména těch z nich, jež IPv6 skutečně podporují. Toho by se dalo s dostatečnou mírou pružnosti dosáhnout jedině vytvořením programu pro automatickou detekci IPv6 na uživatelských počítačích (např. prostřednictvím ICMPv6 ping) nebo možností

samostatné konfigurace této vlastnosti ze strany uživatelů. Ani jedna z těchto metod by nebyla příliš spolehlivá.

Proto jsme se rozhodli jít druhou cestou a používat pro záznamy typu A a typu AAAA odlišná jména. Konkrétně jsme v doméně *tul.cz* zavedli poddoménu *ip6* obsahující veškeré AAAA záznamy pro univerzitní počítače ve struktuře totožné se strukturou záznamů typu A v doméně *tul.cz*. Pro *vslib.cz* uplatňujeme stejnou strategii. AAAA záznamy jsou připraveny pro všechny registrované počítače, bez ohledu na skutečný stav jejich podpory IPv6.

Například pro dříve uvedený počítač registrovaný s údaji:

```
<pocitac>
   <jmeno>onyx.kmp.tul.cz</jmeno>
   <interface>
      <ethernet>0020B4AA1948</ethernet>
      <podsit>p</podsit>
      <ip>147.230.32.92</ip>
      <ip6>0213:d3ff:fe5f:fe35</ip6>
   </interface>
   <kontakt>Kleopatra Tuha</kontakt>
   <umisteni>212A</umisteni>
</pocitac>
```

budou generovány celkem čtyři DNS záznamy ve čtyřech odlišných doménách:

onyx.kmp.tul.cz.	A	147.230.32.92
onyx.kmp.vslib.cz.	CNAME	onyx.kmp.tul.cz.
onyx.kmp.ip6.tul.cz.	AAAA	2001:718:1c01:32:213:d3ff:fe5f:fe35
onyx.kmp.ip6.vslib.cz.	CNAME	onyx.kmp.ip6.tul.cz.

Tento přístup vyžaduje při navazování komunikace prostřednictvím jména explicitně vyjádřit, který protokol má být použit. Je tedy méně elegantní, zato robustnější a předvídatelnější než použití dvou záznamů se stejným jménem. V dané situaci, kdy podpora IPv6 na uživatelských počítačích je mizivá, jej považujeme za praktičtější. Až bude naopak používání IPv6 víceméně standardem, počítáme se změnou na první variantu. Tu lze navíc realizovat přechodnou fází podobnou stávajícímu přechodu z domény *vslib.cz* do *tul.cz* prostou změnou generovaných záznamů na:

onyx.kmp.tul.cz.	A	147.230.32.92
	AAAA	2001:718:1c01:32:213:d3ff:fe5f:fe35
onyx.kmp.vslib.cz.	CNAME	onyx.kmp.tul.cz.
onyx.kmp.ip6.tul.cz.	CNAME	onyx.kmp.tul.cz.
onyx.kmp.ip6.vslib.cz.	CNAME	onyx.kmp.tul.cz.

Následně pak budou domény *ip6* zcela odstraněny.

Dvojí záznamy (A i AAAA pro stejné jméno) používáme již v současnosti pro některé servery poskytující centrální služby. U těchto serverů je podpora IPv6 zaručena (typicky jsou provozovány správou sítě LIANE) a z hlediska plynulého používání protokolů IPv4 i IPv6 na straně klientů je naopak žádoucí, aby poskytovaly služby oběma protokoly pod stejným jménem. Spadá sem například primární DNS server domény *tul.cz/vslib.cz*, centrální poštovní server a podobně.

Do registrační databáze jsou počítače implicitně vkládány se standardním identifikátorem rozhraní EUI-64 vytvořeným z MAC adresy (viz položka `<ip6>` v příkladu XML kódu výše). Adresu je však možné změnit a registrovat počítač s explicitně danou adresou. Přestože IPv6 umožňuje přidělit rozhraní několik různých IPv6 adres, námi vyvinutý registrační software tuto schopnost nemá – nepovažujeme v našem prostředí za potřebné zavádět do DNS koncové počítače s více adresami.

5.5 Podpora mobilních počítačů

Směrovače Cisco teoreticky mohou vykonávat funkci domácího agenta pro mobilní počítače pocházející ze sítí k nim připojených. Jejich operační systém disponuje příkazy pro zapnutí této schopnosti a konfiguraci základních parametrů (omezení počtu klientů, nastavení časových konstant). Chybí však vazba na bezpečnostní mechanismy, potřebné k ověření totožnosti mobilního uzlu při žádosti o vytvoření vazby s domácím agentem.

Skutečnost, že konfigurace domácího agenta není popsána v dokumentaci [29] naznačuje, že dotyčné prvky zatím nejsou zralé pro produkční nasazení.

Vzhledem k tomu, že zatím žádný z uživatelů neprojevil o podobnou službu zájem, rozhodli jsme se tuto problematiku zatím neřešit. Pokud by takový požadavek vyvstal, jsme připraveni použít náhradní řešení se softwarovým směrovačem na bázi operačního systému BSD, který potřebné schopnosti nabízí. Jestliže se požadavek na podporu mobilních zařízení neobjeví, vyčkáme do dokončení jeho implementace v IOS a použijeme jako domácí agenty centrální směrovače sítě.

5.6 Služby

Poskytování služeb protokolem IPv6 závisí především na míře jeho podpory v programech používaných v roli serverů. Naštěstí je v současné době již řada programů portována a dokáže komunikovat oběma protokoly, implementace různých síťových služeb proto nepředstavuje vážnější problém.

Elektronická pošta je realizována prostřednictvím programu Postfix, jenž IPv6 podporuje. Stačí v konfiguračním souboru *main.cf* použít parametr

```
inet_protocols = all
```

Přítomnost IPv6 se projeví i v konfiguraci lokálních sítí, z nichž má server přijímat poštu bez ověřování totožnosti odesilatele (parametr `mynetworks`), kde je třeba uvést odpovídající IPv6 adresy. V našem případě

```
mynetworks = 127.0.0.0/8
             147.230.0.0/16
             [::1]/128
             [fe80::]/10
             [2001:718:1c01::]/48
```

Program Dovecot používaný v roli IMAP serveru IPv6 podporuje. Jeho konfigurace má však připouští jen jedinou definici rozhraní, jímž komunikuje. Jako hodnotu parametru `listen` lze použít hvězdičku pro libovolné IPv4 rozhraní, nebo `[::]` pro libovolné IPv6 rozhraní, nikoli však obě. Hodnota `[::]` podle dokumentace v závislosti na platformě může způsobit napojení serveru i na všechna IPv4 rozhraní, žádné podrobnější informace však nejsou k dispozici. Proto jsme se rozhodli pro konzervativní přístup a na serveru provozujeme dvě nezávislé verze Dovecotu – jednu konfigurovanou pro IPv4, druhou pro IPv6 s direktivou

```
listen = [::]
```

v souboru *dovecot.conf*.

WWW server Apache verze 2 podporuje IPv6 bez problémů. Dokonce ani nevyžaduje žádný explicitní zásah do konfigurace[2]. Pokud je na dotyčném serveru aktivováno IPv6, automaticky jím komunikuje i Apache server. Tímto způsobem je IPv6 poskytováno centrálními WWW servery, jako je *www.tul.cz* či *webmail.tul.cz* poskytující WWW rozhraní k elektronické poště.

Pro **autentizaci** zatím IPv6 nepodporujeme. LDAP server eDirectory pracuje v prostředí operačního systému Novell NetWare, který sice IPv6 podporuje, nepodařilo se nám však nalézt spolehlivé informace o robustnosti a spolehlivosti jeho podpory. Vzhledem k tomu, že autentizační služby jsou interní záležitostí TU, rozhodli jsme se zatím setrvat na protokolu IPv4. Do budoucna připravujeme replikaci LDAP údajů na linuxový server. Tímto způsobem budeme schopni zpřístupnit LDAP i protokolem IPv6. Paralelně také hodléme nadále zjišťovat stav a reálné chování IPv6 v prostředí Novell NetWare.

[2] Za předpokladu, že virtuální servery jsou řešeny pomocí jmen, nikoli vazbou na konkrétní IP adresu. Případné IPv4 adresy v konfiguraci je pochopitelně potřeba rozšířit o adekvátní IPv6 adresy, tato implementace virtuálních WWW serverů je však v současnosti již krajně neobvyklá a centrální servery TU v Liberci ji nepoužívají.

6 Závěr

IPv6 se prosazuje jen velmi pomalu. Dlouhodobě se nachází ve stavu vzájemného čekání – uživatelé jej masově nepožadují, protože pro valnou většinu těch stávajících nenabídne žádné zásadně nové služby, a nikdo se příliš nesnaží vyvíjet pro IPv6 širší služby, protože pro ně nejsou uživatelé. Dá se očekávat, že tuto patovou situaci postupně rozřeší teprve čas, zhoršující se situace s přidělováním IPv4 adres a nepřehlednost IPv4 sítě v důsledku používání neveřejných adresních rozsahů a mapování adres.

Srovnání s jinými dnes běžně používanými technologiemi, jako je telefon, osobní počítač či stávající IPv4 ukazuje, že doba 10–20 let od vzniku do masivního rozšíření je poměrně obvyklá. IPv6 Forum ve své vizi dalšího vývoje [25] předpovídá že teprve kolem roku 2010 překročí podíl sítí běžných poskytovatelů Internetu nabízejících IPv6 hranici 30 %. O pět let později by mělo být dosaženo 90% penetrace IPv6 mezi poskytovateli.

Jednou z úloh akademických a univerzitních sítí je ověřovat nové síťové protokoly a technologie, přispívat k jejich rozvoji a nabízet svým uživatelům špičkové síťové prostředí s vlastnostmi nedostupnými v běžných produkčních sítích. Proto patří akademické sítě mezi první implementátory IPv6 a jejich role při šíření protokolu je velmi důležitá.

V souladu s těmito cíli jsem se již v roce 1999 podílel na zavedení IPv6 do NREN České republiky i do univerzitní sítě LIANE. Tehdy vytvořená řešení byla postupně rozvíjena v souladu s vývojem standardů, stavem techniky a dostupnými možnostmi. Výsledkem je současná kvalitní implementace protokolu v národní páteřní infrastruktuře i v současné generaci sítě LIANE. V obou případech je protokol IPv6 podporován nativně v kvalitě srovnatelné s IPv4. Uživatelé těchto sítí tak mají k dispozici prostředí, jež jim umožňuje experimentovat se službami využívajícími IPv6 či takové služby vyvíjet.

K prosazení protokolu se pokouším přispět i činností osvětovou a vzdělávací. Soustavně sleduji vývoj protokolu a informace o něm předávám odborné komunitě prostřednictvím článků a vystoupení. Snad se mi daří posouvat Internet a jeho služby alespoň o malý kousek vpřed.

Přílohy

Příloha A Toky v IPv6

Publikováno v on-line časopisu Lupa 6. 5. 2004

Jednou z novinek, které se objevily v IP verze 6, je zavedení mechanismu toků. Jeho cílem je – jak jinak – optimalizace směrování. Směrovače po cestě mohou příslušníkům jednoho toku, což je např. přenos jednoho souboru nebo telefonní hovor (musí mít stejného odesílatele, příjemce a značku), zajistit speciální služby.

Nyní vyšlo RFC 3697, které záležitosti kolem toků upřesňuje.

Značka toku, která slouží k jeho identifikaci, má v IPv6 hlavičce vyhrazen prostor o velikosti 20 bitů. Přiznám se, že když jsem v definici IPv6 datagramu (RFC 2460) četl, že toky jsou stále experimentální a budou definovány později, byl jsem krajně skeptický. Text vzbuzoval silný dojem, že se autoři sice shodli na myšlence „toky by mohly být užitečné“, ale nemají příliš přesnou představu o jejich reálné implementaci. Něco podobného jsme zažili už u IPv4, jehož položka Type Of Service (TOS) nebyla pořádně definována dodnes.

Mou skepsi podporovalo i několikaleté mlčení, kdy kýžená definice mechanismů pro práci s toky stále nepřicházela a ani se nezdálo, že by nějak intenzívně vznikala. Nyní je vše jinak. V březnu vyšlo RFC 3697 – IPv6 Flow Label Specification. Přestože stále ponechává některé otázky otevřené, přináší do oblasti toků znatelný pokrok.

Základní rozhodnutí je, že o zařazení do toku rozhoduje odesílatel. Výlučně na něm záleží, kterým datagramům přiřadí jaké značky toků a podle toho stanoví jejich příslušnost k tokům. Během přepravy pak musí být značka toku zachována a hodnota stanovená odesílatelem musí nezměněna doputovat až k příjemci.

Toky jsou rozlišovány podle trojice údajů: IP adresa odesílatele, IP adresa příjemce a značka toku. Shodují-li se všechny tři, patří datagramy ke stejnému toku. Podstatné je, že všechny tři údaje pocházejí z IP hlavičky, není třeba brát v potaz informace z vyšších vrstev (např. ve světě IPv4 je snaha vytvářet toky podle pětice zahrnující IP adresy odesilatele a příjemce, transportní protokol a jeho porty; poslední dva údaje však pocházejí z hlavičky transportního protokolu).

RFC 3697 doporučuje, aby odesílatel zařadil do nového toku každé transportní spojení a proud aplikačních dat, pro něž zatím neexistuje vhodný tok. Měl by to dělat i v případě, že sám žádné speciální zpracování podle toků nepodporuje.

Vhodným značkováním ale umožní, aby jím vytvořené datagramy tokově zpracovávali další účastníci komunikace. Pokud se rozhodne datagram nezařadit do žádného toku, musí jeho značce toku přidělit nulovou hodnotu.

Dokument nenařizuje žádný specifický způsob, jak značky toků přiřazovat. Pouze obecně mluví o tom, že odesílatel by měl mít pro jejich přiřazování určitou konzistentní metodu – například sekvenčně nebo pseudonáhodně. Příjemce ale nesmí žádnou takovou metodu na straně odesílatele předpokládat a cokoli odvozovat z výpočtů založených na značkách toků. Na straně odesílatele musí mít nadřazené vrstvy (transportní a aplikační) možnost poručit si značku toku pro svůj provoz. Síťová vrstva by pro tento účel měla poskytnout odpovídající API, včetně přístupových práv pro jeho použití.

Tok je omezen i časově. Pokud po dobu 120 s nepřijde žádný jeho datagram, je považován za ukončený. Jestliže datagram se stejnou trojicí <odesilatel, příjemce, značka toku> dorazí později, bude již považován za příslušníka jiného toku.

Aby bylo možné s toky efektivně pracovat, musí o nich účastníci komunikace udržovat jisté stavové informace. Mechanismy pro jejich vytvoření a správu jsou však podle osvědčeného schématu ponechány k definici pozdějšímu dokumentu. RFC 3697 pro ně stanoví jen nejzákladnější požadavky (stavové informace musí být možné vymazat a mechanismus se musí dokázat vzpamatovat z nesplnitelného požadavku).

Značná pozornost je v dokumentu věnována otázkám bezpečnosti, řeší se především otázky možného zcizení provozu změnou značky toku. Tato problematika a její dopady se dost podobají falšování IP adres, ovšem s určitými rozdíly: značka toku není chráněna mechanismy IPsec, falšování samotné značky toku může být zajímavé pro nehodnou aplikaci na koncovém stroji, která díky tomu uchvátí cizí provoz.

Koncepce toků představuje další pokus o nalezení Svatého grálu všech síťařů – škálovatelného vysokorychlostního způsobu dopravy datagramů s definovanými vlastnostmi. Zatím jsou toky příliš syrové na to, abychom mohli předvídat jejich budoucnost. Nicméně vše nasvědčuje, že to s nimi IETF myslí vážně.

Příloha B IPv6 adresy – mírný pokrok v mezích zákona

Publikováno v on-line časopisu Lupa 24. 3. 2006

Letos v únoru vyšlo RFC 4291 s aktualizovanou definicí architektury adres pro IP verze 6. Jeho obsah odráží skutečnost, že IPv6 již má za sebou přes deset let vývoje a v současnosti se spíše pilují detaily. Žádnou závratnou revoluci v adresách tedy nečekejte.

Architektura adres má pochopitelně pro protokol velký význam. Zejména v situaci, kdy nedostatek IPv4 adres byl jedním z hlavních motivů jeho samotného vzniku. RFC 4291 představuje již čtvrtou generaci tohoto dokumentu. Jeho nejstarším předkem je RFC 1884 vydané v prosinci 1995. V červenci 1998 následovalo RFC 2373, jež bylo až po šesti letech, v dubnu 2003, nahrazeno RFC 3513.

S jedním vynecháním je tedy adresní architektura IPv6 aktualizována každé tři roky. Dlužno poznamenat, že změny mezi jednotlivými generacemi jsou poměrně malé a celá řada konceptů zavedených již v RFC 1884 platí dodnes. Důvodem je i to, že nejdůležitější kategorie – globální individuální adresy – je v tomto textu jen načrtnuta a její přesnou strukturu definuje samostatný dokument (aktuálně minimalistické RFC 3587, o němž jsme informovali před časem).

Co tedy obsahuje RFC 4291? V první řadě délku adresy 128 bitů a její zápis šestnáctkovými číslicemi, vždy po čtyřech oddělovanými dvojtečkami. Definuje základní tři typy adres:

Individuální (unicast) označují právě jedno síťové rozhraní.

Skupinové (multicast) identifikují skupinu rozhraní, data mají být doručena všem. Skupiny v IPv6 nahrazují i všesměrové vysílání (broadcast) z IPv4, kdy se data doručují například všem příslušníkům určité podsítě. IPv6 pro tyto účely zavádí určité standardní skupiny – například skupina s adresou ff02::1 obsahuje všechny uzly na jedné lince.

Výběrové (anycast) které také označují skupinu rozhraní, ale data se doručují jen jednomu jejímu členovi (tomu nejbližšímu).

Adresní architektura definuje také rozložení jednotlivých typů a speciálních adres v dostupném prostoru. A tady je první změna, protože před půldruhým rokem byly zrušeny místní individuální adresy, jimž byl dříve přidělen

prefix fec0::/10. Speciální chování tohoto prefixu je v nových implementacích výslovně zakázáno, musí se k němu chovat jako ke globálním individuálním adresám. Aktuálně tedy platí následující rozložení:

prefix	*význam*
::/128	neurčená
::1/128	smyčka
ff00::/8	skupinové
fe80::/10	individuální lokální linkové
všechny ostatní	individuální globální

Zatímco skupinové adresy mají svůj vlastní prefix, a jsou tedy na první pohled rozpoznatelné, výběrové adresy sdílejí prostor s individuálními. Jsou rozlišeny konfigurací zařízení, nikoli svým tvarem. U výběrových adres dochází v novém dokumentu k jistému uvolnění. Předchozí RFC 3513 je prohlašovalo za nepříliš probádané území a z toho důvodu na ně kladlo dvě podstatná omezení:

- nesměly se používat jako adresa odesílatele,
- nesměly být přidělovány počítačům, jen směrovačům.

V současnosti jsou již zkušenosti s jejich používáním větší, proto byla uvedená omezení odstraněna.

Mezi speciálními adresami lze najít dva formáty, které se týkají předchozí verze protokolu. Jedná se o IPv4-kompatibilní adresy (v prvních 96 bitech nuly, následuje 32 bitů s IPv4 adresou) a IPv4-mapované adresy (v prvních 80 bitech nuly, pak 16 bitů jedniček a 32 bitů s IPv4 adresou). Protože se první formát v aktuálních mechanismech pro přechod od IPv4 k IPv6 nepoužívá, prohlašuje jej RFC 4291 za odmítnutý.

Dílčí úpravy se dočkaly i skupinové adresy, jejichž formát zůstával prakticky beze změny již od původního RFC 1884. K tradičnímu příznaku T přibyly dva nové, P a R. Jejich významy jsou následující:

Příznak T (Transient) rozlišuje dočasné adresy (T=1) od trvalých (T=0).

Příznak P (Prefix) se používá pro skupinové adresy vycházející z individuálního prefixu. Má-li hodnotu 1, je posledních 96 bitů adresy tvořeno 64bitovým prefixem sítě pro individuální adresy, za nímž následuje 32bitový identifikátor skupiny. Cílem je usnadnit dynamické vytváření skupinových adres, které by nevyžadovalo vzájemnou koordinaci mezi různými sítěmi. Tyto adresy musí být dočasné (T=1). Podrobnější definici obsahuje RFC 3306.

Příznak R (Rendezvous Point) umožňuje do skupinové adresy zakódovat adresu rendezvous pointu pro protokol PIM-SM – viz RFC 3956.

V závěru pak architektura definuje povinné adresy, k nimž se musí hlásit každý uzel a každý směrovač. Na nich se proti předchozí generaci změnila jen přítomnost výběrových adres pro uzel. Povinné pro každý uzel tedy jsou:

- linková lokální adresa pro každé rozhraní,
- všechny konfigurované individuální a výběrové adresy,
- smyčka,
- skupinové adresy ff01::1 a ff02::1 pro všechny uzly,
- skupinová adresa pro vyzývaný uzel při objevování sousedů,
- adresy všech skupin, do nichž patří.

Směrovač se navíc musí znát k těmto adresám:

- výběrová adresa pro směrovače v podsíti (prefix podsítě, za nímž následují v části pro identifikátor rozhraní samé nuly),
- skupinové adresy ff01::2, ff02::2 a ff05::2 pro všechny směrovače.

Zbývající změny se týkají spíše vyjasnění některých formulací či editorských úprav textu. Obsah RFC 4291 svědčí o tom, že adresní architektura IPv6 je stabilizovaná. Dochází jen k nepříliš významným změnám vyvolaným zkušenostmi s praktickým nasazením protokolu.

Příloha C IPv6 adresy budou jednodušší

Publikováno v on-line časopisu Lupa 6. 11. 2003

RFC 2374 definovalo v roce 1998 strukturu globálních adres pro IPv6. Jedná se o vůbec nejdůležitější kategorii, protože právě tyto se používají při komunikaci v Internetu. Jenže navržená struktura se nedostala do reálného života a nyní byla oficiálně odvolána. RFC 3587 odráží současnou praxi v zacházení s IPv6 adresami.

Stručně připomenu, že podle RFC 2374 měla mít globální individuální agregovatelná adresa (což je oficiální název individuálních adres s globálním dosahem) následující strukturu:

První tři bity obsahují hodnotu 001 (binárně), podle které se pozná tato kategorie adres. Za ní měl následovat tak zvaný Top Level Aggregation (TLA) identifikátor, což měly být prefixy přidělované velkým poskytovatelům Internetu. Právě tyto TLA měly mít v tabulkách páteřní internetové směrovače (v default-free zóně).

Za nimi měl následovat Next Level Aggregation (NLA) identifikátor, kterým měli zmínění velcí poskytovatelé rozlišovat sítě svých podposkytovatelů či vytvářet hierarchii ve svých sítích. Prvních 48 bitů adresy tak mělo odrážet veřejnou topologii sítě a mělo být koncové síti přidělováno „zvenčí“.

Následujících 16 bitů již je ve správě připojené instituce a obsahuje adresu podsítě, oficiálně pojmenovanou Site Level Aggregation (SLA) identifikátor. Celou druhou polovinu adresy zabírá identifikátor rozhraní, podle nějž se identifikují počítače uvnitř podsítě.

Ovšem TLA prefixy byly dosud přiděleny jen tři: 3ffe::/16 pro experimentální síť 6bone, 2002::/16 pro přechodový mechanismus 6over4 a o 2001::/16 se dělí všichni regionální registrátoři (RIR, Regional Internet Registry), kteří přidělují definitivní adresy pro celý svět. Představa o default-free zóně obsahující jen TLA prefixy je od reality velmi daleko.

V srpnu letošního roku proto vyšlo RFC 3587, které uvedlo oficiální definici adresy do souladu s běžnou praxí. Výsledkem je maximálně zjednodušená podoba globální individuální adresy:

Zůstalo zahájení 001 a celá lokální infrastruktura - identifikátor podsítě (který už přiznal barvu a neskrývá se za tajemné SLA) a rozhraní. Veškerá plánovaná struktura mezi těmito prvky se scvrkla do jediné položky nazvané globální směrovací prefix. Kdyby ji nazvali podle IPv4 adresou sítě, asi by to bylo až příliš jednoduché.

IETF se vzdalo snahy diktovat v této oblasti strukturu a ponechalo ji na regionálních registrátorech (pro Evropu tuto roli hraje RIPE NCC). Registrátoři svá pravidla pro přidělování adres koordinují, takže v praxi je adresní politika shodná na celém světě.

V současnosti vypadá tak, že uchazeč (lokální registrátor, LIR, což zpravidla bývá poskytovatel Internetu) dostane tzv. SubTLA - prefix délky 32 bitů. Připomínám, že jeho počátečních 16 bitů je pevně daných, obsahuje hodnotu 2001 (šestnáctkově). Jelikož se koncovým sítím (zákazníkům) přidělují prefixy délky 48 bitů, má LIR k dispozici 16 bitů pro zavedení vlastní hierarchie (rozlišení podposkytovatelů, uzlů a podobně). Rozložení zodpovědností v IPv6 adrese je tedy následující:

Adresa nakonec dozrála do pragmatické podoby, kdy nejdůležitější části tvoří jednotlivé čtveřice šestnáctkových číslic v jejím zápisu. Přehlednější už to být nemůže.

Jak velkou změnu RFC 3587 představuje? Je to taková kapesní revoluce - asi jako kdyby na Auroře vystřelili ze špuntovky. Ve specifikaci dochází nepochybně k významné změně, v praxi však prakticky k žádné. Standard se prostě přizpůsobil reálnému životu.

Mimochodem - jedná se už o několikátý neúspěšný pokus vymyslet od zeleného stolu strukturovanou adresu, kterou pak praxe rozmetala na kousíčky. Snažilo se o to X.25, ale skončilo v propadlišti dějin (tam byla adresa strukturovaná opravdu detailně, takže se samozřejmě velmi plýtvalo a například naše univerzita dostala k dispozici 100 adres, což opravdu není mnoho). Snažilo se o to IPv4 a stálo spoustu úsilí, aby se proletáři všech sítí spojili a vybudovali beztřídní adresní společnost. Snažilo se o to IPv6, a přestože poučeno z nezdarů IPv4, opět se pokus nezdařil.

Zdá se, že nejúčinnějším nástrojem pro definici struktury adres je evoluce. Definovat jen celkovou délku, zbytek se vyvine sám.

Příloha D Pohnou se hranice v IPv6 adresách?

Publikováno v on-line časopisu Lupa 13. 10. 2005

Vnitřní struktura IPv6 adres, ač poměrně mladá, už má za sebou několik vývojových generací. Po různých výbojích a mocné tvořivé činnosti nakonec podle RFC 3587 skončila stejně jako adresy pro IPv4: skládá se z adresy sítě, podsítě a rozhraní. Jejich délky byly doposud považovány za jasně vymezené, nyní se ale možná pohnou.

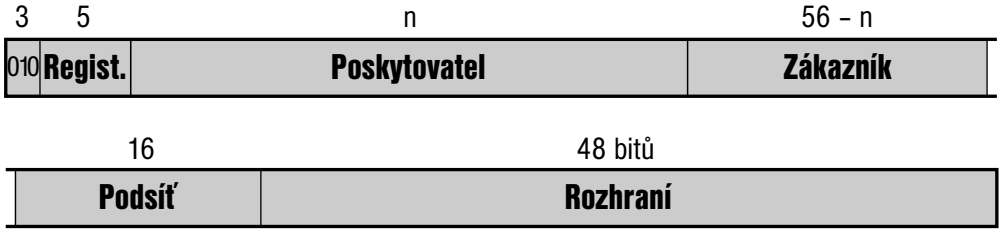
Abych se nezbláznil z různých variant, bude se tento článek držet pouze základních, tedy individuálních globálních adres. Ty pochopitelně hrají v Internetu rozhodující roli, protože je používá k identifikaci cíle drtivá většina datového provozu. Pokud máte v malíku jejich historii a aktuální stav, poskočte rovnou na část Těsné hranice obsahující jádro článku.

D.1 Jak se vyvíjely

Podívejme se nejprve ve stručnosti, jaký vývoj tento typ adres prodělal během několika generací RFC definujících adresní mechanismy IPv6.

RFC 1884 z roku 1995 ještě nebylo konkrétní. Pouze vyčlenilo tříbitový prefix 010 (binárně) pro adresy pocházející od poskytovatelů (provider-based unicast addresses), jejich strukturu však ponechalo zatím otevřenou. Jen jako příklad uvádí adresu, která používá 48bitovou MAC adresu podle IEEE 802 jako identifikátor rozhraní, před nímž se nachází identifikátor podsítě a sítě.

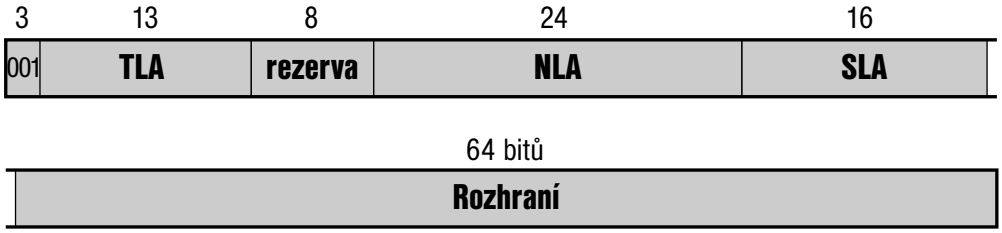
Přesnější strukturu doplnilo o dva roky později RFC 2073. Pět bitů, jež za prefixem zbývají k hranici prvního bytu, přiřklo identifikaci regionálního registrátora. Zbývajících 56 bitů z první poloviny adresy mělo být rozděleno mezi identifikátor poskytovatele Internetu a zákazníka v jeho síti. Druhou polovinu pak tvořil 16bitový identifikátor podsítě a 48bitová MAC adresa rozhraní.



RFC 2073 ale mělo jepičí život. Hned o rok později, tedy v roce 1998, vychází druhá generace dokumentů definujících IPv6, která nenechala kámen na kameni. V individuálních adresách je hlavní důraz kladen na agregovatelnost

a hierarchické přidělování. Cílem je udržet velikost globálních směrovacích tabulek v rozumných mezích. Aby se vyloučila kolize s předchozí generací adres, mění se i prefix pro „globální individuální agregovatelné adresy“, jak zní jejich oficiální pojmenování. Místo 010 je nyní 001.

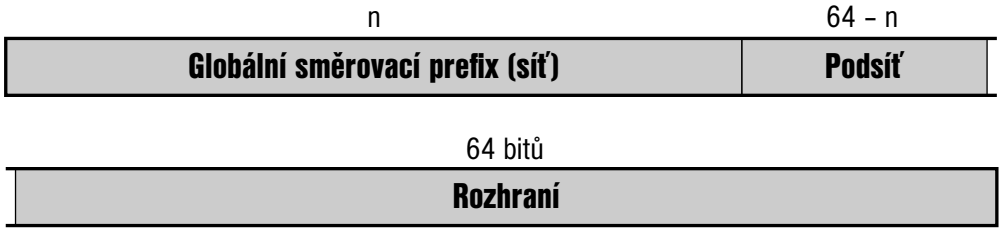
Strukturu individuálních adres definovalo RFC 2374. Podle něj za prefixem následoval 13bitový identifikátor nejvyšší úrovně agregace (TLA, Top Level Aggregation). Záznamy odpovídající TLA prefixům měly tvořit globální směrovací tabulky. Následovala osmibitová rezerva umožňující prodloužit podle potřeby jednu ze sousedních částí. Další část představoval 24bitový identifikátor druhé úrovně agregace (NLA, Next Level Aggregation). 16 bitů za ním náleželo identifikátoru místní úrovně agregace (SLA, Site Level Aggregation), což byl vznešený název pro podsíť. Adresa rozhraní byla prodloužena na 64 bitů.



D.2 Současný stav

RFC 2374 sice zůstalo v platnosti pět let, ale k jeho praktickému naplnění nikdy nedošlo. TLA identifikátory byly přiděleny jen tři: prefix 2001::/16 identifikuje adresy přidělované všemi regionálními registrátory, čili „opravdové“ adresy; prefix 2002::/16 používá přechodový mechanismus 6to4 a konečně 3ffe::/16 sloužil experimentální síti 6bone a dnes již mizí. Představa, že TLA prefixy naplní globální směrovací tabulky, se ocitla zcela mimo realitu a ani přidělování dalších částí adresy nemělo s RFC 2374 mnoho společného.

V roce 2003 proto RFC 3587 definovalo třetí generaci adres. Tentokrát velmi obecně a velmi jednoduše. Podle něj je první polovina adresy rozdělena mezi globální směrovací prefix (čili adresu sítě) a identifikátor podsítě. Druhou polovinu pak tvoří identifikátor rozhraní.



Došlo ke zrušení jakýchkoli hranic v adrese sítě. RFC 3587 pouze konstatuje, že typicky bude přidělována hierarchicky, a to podle pravidel daných registrátory a poskytovateli Internetu. Při pohledu na předchozí verze a jejich odtržení od

reality je to asi to nejrozumnější, co se o adresách dalo napsat. Vývoj pravidel pro přidělování navíc nevynucuje změnu RFC.

RFC 3587 ponechává hranici mezi adresou sítě a podsítě volnou. Jeho důležitým souputníkem je starší RFC 3177 (z roku 2001), jež důrazně doporučuje přidělovat adresy koncovým sítím následovně:

- Standardní délka prefixu pro síť je 48 bitů (z čehož plyne délka identifikátoru podsítě 16 bitů). Tyto prefixy by měly být přidělovány skoro všem.
- Pokud je jisté, že v síti nebudou potřeba žádné podsítě, lze přidělit prefix délky 64 bitů, čili bez prostoru pro adresování podsítí.
- Pokud je jisté, že se připojuje jen jediné zařízení, přidělí se mu přesná adresa, čili prefix délky 128 bitů.

Naposledy zmíněná dvojice RFC tedy stanoví, že pro valnou většinu běžně používaných adres má prefix sítě konstantní délku 48 bitů. V praxi dnes jeho struktura vypadá tak, že prvních 16 bitů je pevně daných (obsahují prefix 2001::/16), dalších 16 bitů přidělí regionální registrátor lokálnímu (tedy typicky je touto částí adresy identifikován poskytovatel Internetu) a závěrečných 16 bitů určuje lokální registrátor (obvykle poskytovatel Internetu, který touto částí adresy identifikuje zákazníka).

D.3 Těsné hranice

A právě o 48bitovou hranici se vede tuhý spor. Ne že by snad v některé části adresy už dnes tlačila bota, ale provádějí se všelijaké výpočty, zkušenosti z IPv4 se promítají do světa nových adres, uplatňují se koeficienty využití adresního prostoru a podobně. Výsledkem těchto snah je přesvědčení, že adresní prostor IPv6 při stávajících pravidlech není nevyčerpatelný a že bychom se provozních problémů s přidělováním adres mohli dočkat dříve, než se předpokládalo.

Frustrující je, že dostatek adres na věky věků je jedním ze základních požadavků na IPv6. Připadá mi, že všeobecná nálada typu „neudělat fatální chybu hned na začátku“ vede k poněkud Parkinsonovskému chování. Zcela stranou diskusí totiž zůstávají dvě skutečnosti.

Tou první je, že se bavíme o pouhé osmině adresního prostoru IPv6. Jeho valná většina je zatím rezervována pro budoucí využití. I pokud by se za několik (desítek) let ukázalo, že přijatá adresní strategie nebyla šťastná a vedla k příliš rychlému vyčerpání světových zásob adres, pořád ještě zbývá spousta místa, kde lze nastavit pravidla jinak a lépe. Připadá mi, že než dnes věštit z křišťálové koule a vyrábět vědecké výpočty, bylo by vhodnější nechat věcem volný průběh a vyjít z reálného vývoje.

Druhou skutečností je brutální plýtvání v identifikátorech rozhraní. Zatímco MAC adresám stačí 48 bitů k dosažení celosvětové jednoznačnosti, v IPv6 se

investuje o 16 bitů více do identifikátorů, jež mají být jednoznačné v rámci jediné podsítě. V praxi se přebírá MAC adresa, do níž se vkládají dva byty s konstantní hodnotou podle specifikace EUI-64. Kdyby nic jiného, tak tyhle dva byty jsou doslova vyhozené z okna.

Použití dlouhé adresy identifikátoru má pochopitelně své výhody – například velmi usnadňuje automatickou konfiguraci. Při pohledu na dnešní argumentace kolem adres se ale vkrádá myšlenka, jestli cena není příliš vysoká. Ovšem 64bitové identifikátory rozhraní už jsou natolik pevně usazeny v řadě mechanismů IPv6, že změna této hranice se zdá být naprostým tabu.

Místo toho se vedou hektické debaty, že 16 bitů pro adresování podsítí je mnohdy zbytečně mnoho. (Samozřejmě je, ovšem ve srovnání s šestnácti bity využitými k uložení konstanty fffe se adresa podsítě jeví jako ráj efektivity.) V současnosti se zdá, že konvergují k názoru zavést dvě délky prefixů pro adresu sítě:

- 48 bitů ponechat pro větší koncové sítě;
- sítím domácností či malých kanceláří přidělovat prefixy 56bitové a ponechat jim na adresování podsítí jeden byte.

Konkrétně se tyto úvahy promítly do návrhu na změnu pravidel pro přidělování IPv6 adres, kdy o délce přiděleného prefixu rozhoduje lokální registrátor (čili většinou poskytovatel Internetu). Přestože odkazuji na dokument evropského registrátora RIPE NCC, navrhovaná změna je výsledkem konsensu mezi registrátory a bude zřejmě celosvětová.

Já osobně bych daleko raději viděl zkrácení identifikátoru rozhraní na 48 bitů, přesun 16bitové adresy podsítě do druhé poloviny adresy a přidělování prefixů jednotné délky 64 bitů. Nicméně vše nasvědčuje tomu, že mi nebude přáno a v dohledné době se dočkáme revize RFC 3177 ve směru k 56bitovým prefixům.

Příloha E Dosahy IPv6 adres

Publikováno v on-line časopisu Lupa 15. 9. 2005

Jedno z rozšíření, které IPv6 zavádí do adresačního mechanismu, je koncept omezení jejich působnosti, čili dosahů. Dosah vymezuje část sítě, ve které dotyčná adresa platí a v níž musí být jednoznačná. Na jaře vyšlo RFC 4007 (IPv6 Scoped Address Architecture), popisující základní principy dosahů.

Pro individuální (unicast) adresy je situace dost jednoduchá. Zde existují jen dva dosahy – adresy lokální pro linku a adresy globální. Linkové adresy mají prefix fe80::/10 a platí jen v rámci jedné „linky“ (sítě na linkové vrstvě), například v jednom Ethernetu. Platnost lokální linkové adresy končí na nejbližším směrovači.

Globální adresy pak pokrývají celý Internet a musí v něm být jednoznačné. Původní architektura počítala ještě s jedním dosahem, lokálním pro „místo“ (čili koncovou síť). Ovšem kolem jeho interpretace panovala řada nejasností, takže byl později v RFC 3879 zavržen. To je poměrně paradoxní, protože neveřejné IPv4 adresy podle RFC 1918 jsou do značné míry analogií adres lokálních pro místo. S jejich používáním tedy existuje ze světa IPv4 řada praktických zkušeností, nicméně snaha o formalizaci ztroskotala.

Specialitu představuje adresa ::1 (smyčka, loopback), která je oficiálně považována za lokální linkovou pro fiktivní linku nacházející se uvnitř uzlu.

Jelikož výběrové (anycast) adresy pocházejí z rozsahu individuálních, sdílejí s nimi i pravidla pro omezování dosahu. Není proto třeba se jimi samostatně zabývat.

E.1 Skupinové adresy

V případě skupinových (multicast) adres je sortiment dosahů velmi košatý. Jsou identifikovány druhou čtveřicí bitů ve druhém bytu adresy. To znamená, že v textovém zápisu adresy rozsah ztělesňuje poslední číslice úvodní skupiny. K dispozici je šestnáct hodnot, z toho některé jsou rezervovány a některé zatím nepřiřazeny:

hodnota	*význam*
0	rezervováno
1	lokální pro rozhraní
2	lokální pro linku
3	rezervováno
4	lokální pro administraci
5	lokální pro místo
6–7	–
8	lokální pro organizaci
9-d	–
e	globální
f	rezervováno

Adresy lokální pro rozhraní jsou dost specifické (čtěte divné), protože jejich dosahem je jediné rozhraní. V podstatě jsou použitelné pouze pro vzájemnou komunikaci mezi programy běžícími na stejném počítači, pokud se má odehrávat síťově. Narozdíl od individuálních adres, kde k těmto účelům slouží výlučně smyčka, lze skupinovou adresu lokální pro rozhraní zkonstruovat celkem volně a přiřadit ji libovolnému rozhraní.

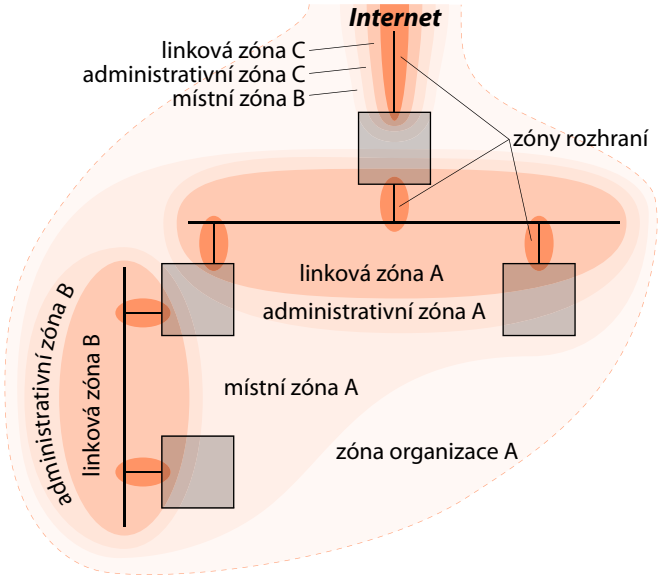
Lokální linková adresa má stejný dosah jako v případě individuálních, tedy souvislou síť podle linkové vrstvy. Adresa lokální pro administraci pokrývá nejmenší dosah, který už musí být konfigurován správcem sítě. Čili nelze jej automaticky odvodit z fyzického propojení sítě. Adresa lokální pro organizaci umožňuje pokrýt několik různě rozmístěných poboček patřících stejné instituci. A konečně globální adresa opět pokrývá celý Internet.

E.2 Zóny

S dosahy jsou těsně spjaty zóny. Zóna je vlastně část sítě odpovídající danému dosahu. Například každá ethernetová síť představuje jednu lokální linkovou zónu. Čili dosah určuje pravidla, kam až určitá adresa platí, a zóna je reálná část sítě dosahem vymezená, v níž adresa platí. Stejná neglobální adresa může být pak použita v různých zónách a v každé z nich má jiný význam. Například lokální linková adresa fe80::1 je nepochybně použita na celé řadě linek současného Internetu.

Hranice zón procházejí uzly, nikoli linkami. Platí obvyklá pravidla ohledně velikosti zón – zóny stejného dosahu se nemohou překrývat, zóna je vždy kompletně obsažena v zónách většího dosahu. Navíc se požaduje, aby každá zóna byla z hlediska směrování konvexní. To znamená, že pokud si posílají data dva uzly z téže zóny, datagramy by během přepravy neměly opustit zónu.

Příklad rozložení zón v koncové síti uvádí následující obrázek. Jedná se o zóny pro neglobální skupinové adresy. V případě adres individuálních by situace byla podstatně jednodušší, zde existují jen linkové zóny a zóna globální.



Základní rozložení zón je definováno takto:

- každé rozhraní obsahuje jednu zónu lokální pro rozhraní (skupinovou),
- každá linka a k ní připojená rozhraní tvoří jednu lokální linkovou zónu (individuální i skupinovou),
- existuje jediná globální zóna obsahující všechny linky a rozhraní v Internetu (individuální i skupinová),
- hranice všech ostatních zón (skupinových) musí definovat a konfigurovat správci sítí.

Každé rozhraní pak patří právě do jedné zóny každého z dostupných rozsahů.

E.3 Identifikace

Jakmile má počítač více než jedno rozhraní a použije se neglobální adresa, je třeba nějak specifikovat zónu, k níž se vztahuje. Řekněme, že například uživatel počítače na obrázku vlevo nahoře zadá příkaz `ping fe80::11`. Použil lokální linkovou adresu a vzniká otázka, do které linky (linkové zóny) paket poslat, zda A či B.

RFC 4007 proto zavádí identifikátory zón. Identifikátory jsou lokální v rámci uzlu a jejich jediným úkolem je rozlišit jednotlivé zóny uvnitř uzlu. Nejsou navzájem nijak synchronizovány a nikdy neopustí svůj uzel (nejsou součástí IPv6 datagramu). Proto klidně stejná zóna může mít v různých k ní připojených uzlech různé identifikátory.

Jako výchozí identifikátory používá dokument kladná celá čísla. Pro každý dostupný dosah je přitom definována jedna implicitní zóna, jež nese číslo 0. Pokud u neglobální adresy neuvedete zónu, bude automaticky zařazena do implicitní zóny příslušného rozsahu. Tím se velmi zjednodušuje situace na

běžných koncových počítačích s jediným rozhraním, kde se vystačí s implicitní zónou. Výše uvedený `ping` by tudíž zamířil do implicitní lokální linkové zóny.

V textovém zápisu se identifikátor zóny píše za adresu, oddělen znakem procento. Kdyby `ping` měl směřovat do zóny číslo 3, bylo by třeba napsat `ping fe80::11%3`.

Dokument připouští, aby implementace podporovaly i jiné identifikátory zón. Obzvláště zajímavé jsou v tomto smyslu názvy rozhraní používané v operačním systému. Jelikož každé rozhraní patří do právě jedné zóny každého dostupného rozsahu, je název rozhraní jednoznačným identifikátorem zón. Pravda, u některých zbytečně konkrétním (např. když používáte rozkládání zátěže a několik ethernetových karet vede do téhož Ethernetu, a tudíž téže linkové zóny). Ovšem takové případy jsou poměrně vzácné a rozhraní je všeobecně známý a používaný koncept. Takže zrovna této kategorii identifikátorů bych předpovídal slibnou budoucnost. Tím se náš `ping` mění na `ping fe80::11%eth2`.

E.4 Směrování

Mluvit o dosahu v souvislosti se směrováním má smysl jen pro skupinové adresy. U individuálních jsou dosahy jen dva – linkový (který se nesměruje, linkově adresovaný paket nesmí projít směrovačem) a globální, jenž představuje standardní směrování.

Nejjednodušší způsob, jak při směrování splnit požadavky na vlastnosti zón, je používat samostatné (alespoň ideově) směrovací tabulky pro jednotlivé zóny. Když směrovač dostane datagram k předání, určí cílovou zónu (podle dosahu a příchozího rozhraní) a směrovací rozhodnutí provede podle tabulky této zóny. Pokud by předání paketu znamenalo překročení hranice zóny, je povinen jej zahodit.

Při výměně směrovacích informací pak sousedům posílá jen data pro zóny toho rozhraní, jímž aktualizaci odesílá.

E.5 Shrnutí

Cílem zavedení dosahů je poskytnout nástroje pro nezávislé adresování (lokální linkové adresy) a přesnější kontrolu šíření skupinově adresovaných dat (např. videokonferencí). Ve světě IPv4 se k podobným účelům používají všelijaké kejkle s životností datagramů (položka TTL v hlavičce), které ovšem nejsou dvakrát čisté. Dosahy nabízejí koncepční řešení problému.

Na druhé straně ale mají daleko k úplnosti. Je třeba upravit aplikační rozhraní IPv6, aby vyšší vrstvy mohly určovat konkrétní zónu (návrh již existuje). A s jeho existencí a zápisem se musí také vypořádat aplikace. RFC 4007 poskytuje základní východisko, ale práce ještě zbývá dost.

Příloha F DNS pro IPv6 – konec schizmatu

Publikováno v on-line časopisu Lupa 23. 10. 2003

V DNS (Domain Name System) pro IPv6 panovala nejistota. Existovaly dvě vzájemně spolu soupeřící koncepce, každá se svými zastánci a odpůrci, postupem času střídavě posilovaly a oslabovaly své postavení. RFC 3596, jež právě vyšlo, dělá v DNS pořádek. Záznamy A6 a DNAME se tímto odkládají na smetiště dějin.

Stručně připomenu historii celé záležitosti. V prosinci 1995 vyšlo RFC 1886 a definovalo způsob ukládání informací o IPv6 adresách do DNS. Zavedlo záznam AAAA – analogii A, čtyřnásobná délka IPv6 adresy se odrazila v názvu záznamu. (Pokud jste se snad domnívali, že se jedná o reklamu na známý autobazar, zklamu vás. IETF se do kampaně zatím nezapojilo.)

Pro reverzní dotazy, kdy se ze známé IPv6 adresy zjišťuje jméno, zavedlo sekvenci šestnáctkových číslic z adresy, kdy každá číslice představuje poddoménu. Celý reverzní systém měl sídlit v doméně ip6.int.

O pět let později vyšlo RFC 2874, jež prohlásilo AAAA za zastaralé a nahradilo jej záznamem A6 (opět odvozeno z A). Jeho hlavní výhodou byla možnost řetězit záznamy. A6 umožňoval převzít začátek adresy z jiného A6 záznamu (který mohl být i ve zcela jiné doméně) a doplnit k němu konec. To dovolovalo snadné přeadresování - poskytovatel Internetu mohl změnit adresy sítí pro své zákazníky, aniž by se muselo sahat na jejich DNS.

Podobnou roli v reverzních dotazech hrál záznam DNAME. Umožňoval velmi elegantně delegovat libovolně dlouhý prefix do některé z domén. V kombinaci s binárními prefixy podle RFC 2673 se adresy navíc neobracely a prefixy se zapisovaly zepředu dozadu. Změnila se též doména nejvyšší úrovně, kterou by mělo být ip6.arpa.

Mechanismy navržené v RFC 2874 byly nepochybně mnohem elegantnější, jenže také choulostivější, což se jim stalo osudným. Jejich kritika se zaměřila především na provozní záležitosti - řešení DNS dotazu bude delší (k získání adresy je třeba posbírat několik A6 záznamů) a může záviset na celé řadě serverů, nevhodným obsahem lze v doménách vytvořit naprosté zmatení. Podobnými problémy trpí i DNAME.

Přestože byly techniky definované v RFC 1886 prohlášeny za zastaralé, řada správců je odmítala opustit (o implementacích nemluvě) a vedly se vášnivé technické debaty. Nakonec se většina přiklonila zpět k původnímu návrhu

a v srpnu roku 2002 vyšlo RFC 3364, které doporučilo pro provozní sítě používat mechanismy podle RFC 1886 a záznamy A6 a DNAME prohlásilo za experimentální s tím, že jejich reálné chování je třeba dále ověřovat.

F.1 Co nadiktovali vítězové

Nová definice DNS pro IPv6 je obsažena v RFC 3596, jež bylo vydáno teď v říjnu. V podstatě se jedná o návrat ke kořenům, zmínku o A6 či DNAME byste v něm hledali marně. Jako by RFC 2874 nikdy neexistovalo. Jediné, co se z něj dochovalo, je přesídlení reverzních dotazů do domény ip6.arpa, které zakotvilo již RFC 3152 a které lze považovat za definitivní od srpna 2001.

A jak že se podle poslední definice dělá DNS pro IPv6? Pro zjištění IP adresy ke jménu v něm slouží záznam AAAA. Jestliže počítač pepa má IPv6 adresu 2001:718:1c01:1:20b:dbff:fea1:d52c, bude v DNS záznam:

```
pepa AAAA 2001:718:1c01:1:20b:dbff:fea1:d52c
```

Reverzní informace se vkládají pomocí obvyklých záznamů PTR, stejně jako v IPv4. Liší se jen konstrukce jejich obsahu. Pro zjištění jména ke známé IPv6 adrese se dotaz vytvoří tak, že se jednotlivé šestnáctkové číslice z IPv6 adresy (musí se doplnit všechny vynechané nuly!) zapíší v pořadí od poslední do první. Každá z nich tvoří doménu, takže se navzájem oddělují tečkami. Za ně se pak připojí ip6.arpa.

Odpovídající doménu dostane do správy instituce, jíž byl přidělen daný prefix. Například TU v Liberci má IPv6 prefix 2001:718:1c01::/28, a tudíž obhospodařuje reverzní doménu 1.0.c.1.8.1.7.0.1.0.0.2.ip6.arpa (všimněte si doplněné nuly před 718 ve druhé čtveřici). Výše uvedený počítač pepa by byl v jejím zónovém souboru zaveden následovně:

```
c.2.5.d.1.a.e.f.f.f.b.d.b.0.2.0.1.0.0.0 PTR pepa.vslib.cz
```

Toto schéma umožňuje snadno delegovat prefixy, které končí na hranici mezi dvěma šestnáctkovými číslicemi textového zápisu adresy. Čili prefixy, jejichž délka je násobkem čtyř. Pokud je třeba delegovat prefix jiné délky (například RIPE NCC až do loňska přiděloval SubTLA délky 35 bitů), musí se použít metody známé ze světa IPv4 - vytváření fiktivních poddomén.

Příloha G Stav DHCPv6 na světových tocích

Publikováno v on-line časopisu Lupa 6. 2. 2003

Jedním z podpůrných protokolů pro IPv6, jehož vývoj se vleče překvapivě dlouho, je DHCPv6 pro automatickou konfiguraci. Přestože pro IPv4 je DHCP denním chlebem v celé řadě sítí, DHCPv6 ještě stále nedospělo do fáze RFC. Projekt 6NET teď publikoval dokument shrnující aktuální stav a perspektivy tohoto protokolu.

Stručně připomenu, že IPv6 nabízí dva modely automatické konfigurace stanic: bezstavovou a stavovou. Bezstavová je zabudována přímo do samotného IPv6 a nevyžaduje žádné speciální servery ani doplňkové mechanismy. Podle ní si spodní polovinu adresy určí počítač sám jednoduchou úpravou své linkové adresy. Z ethernetové adresy

00:04:76:47:8E:81

vytvoří

0204:76FF:FE47:8E81

(doprostřed vloží FFFE, aby původních 48 bitů natáhl na 64, a invertuje druhý bit prvního bajtu). Horní polovinu se dozví z ohlášení směrovačů, které každý směrovač posílá do sítí, k nimž je připojen. Složí obě poloviny a dostane globální IPv6 adresu, aniž by kdo co musel konfigurovat nebo se o něco starat. Ohlášení směrovače obsahuje zároveň informaci o tom, zda dotyčný směrovač lze použít jako implicitní.

Bezstavová konfigurace tedy naučí počítač směrovat – sdělí mu jeho adresu, masku podsítě (to je ryzí formalita, pokud se nedějí strašné věci, je adresa podsítě vždy 64 bitů dlouhá) a implicitní směrovač(e).

K čemu tedy stavovou konfiguraci čili DHCP? Například k nastavení prvků, které v bezstavové chybí. Nejvýznamnější z nich je nepochybně DNS. Bezstavová konfiguraci nesdělí počítači nic o tom, kde je jeho nejbližší DNS server a kam se tedy obracet s DNS dotazy.

Vedle něj může DHCP poskytnout i řadu dalších doplňujících informací, jako třeba lokální doménu, adresu NTP serveru pro synchronizaci času či konfiguraci dalších protokolů. Další důvody pro nasazení DHCP mohou ležet mimo technologickou oblast. Například může odporovat charakteru instituce, aby fungoval kterýkoli počítač, který si zrovna někdo přinesl a zapojil do sítě. Správce sítě může požadovat kontrolu nad přidělováním adres.

Zajímavou variantu představuje současné použití obou autokonfiguračních mechanismů – bezstavového pro přidělení adresy a stavového pro ostatní informace. Tento přístup podstatně zjednodušuje život DHCP serveru, který se nestará o adresy. Díky tomu si nemusí uchovávat stavové informace (nemusí si pamatovat, komu co a do kdy přidělil), což významně usnadňuje implementaci. Tento přístup byl pojmenován "bezstavové DHCP". Předpokládá se, že právě toto by mohl být většinový způsob nasazení DHCPv6.

Pořadové číslo 28 u aktuálního návrhu DHCPv6 jasně naznačuje, jak dlouhý a bolestný proces vzniku má za sebou. Skutečnost, že většina současných implementací podporuje nižší než 20, zase dokazuje, že implementátorům prostě došla trpělivost. Velmi dobrou zprávou v tomto kontextu je, že v prosinci 2002 získal zmíněný návrh statut navrženého standardu (proposed standard) a že by se měl v nejbližší době ustálit do podoby RFC.

Co se změnilo? Základ pochopitelně zůstal stejný. Kdesi v lokální síti je server (či několik serverů) s databází informací. Klient jej v první fázi vyhledá a ve druhé pak osloví se žádostí o konfigurační parametry. Pokud pro něj server má potřebné údaje, dodá mu je. Adresy se propůjčují na omezenou dobu, klient může požádat o prodloužení.

Změnou, která je nabíledni, je adresování. Jedno rozhraní může mít přehršel IPv6 adres a DHCPv6 server jich tedy může poslat celou řadu. Také adresa klienta se liší, protože v IPv6 si každý stroj může sám přidělit lokální linkovou adresu (která platí jen v rámci linky, tedy k nejbližšímu směrovači). Právě tu používá při komunikaci se serverem.

Významně se změnily též vnitřní formality protokolu. Formát DHCP zprávy byl zjednodušen až na naprosté minimum – povinnými položkami jsou jen typ zprávy a identifikátor transakce. Vše ostatní bylo odsunuto do voleb.

K identifikaci klienta nyní slouží tak zvaný DHCP Unique Identifier (DUID), který by v ideálním případě měl zůstat stejný i po změně síťové karty. Uvažuje se o identifikátorech přidělených výrobcem či o identifikátorech, které si počítač jednou vygeneruje, uloží do trvalé paměti a nadále bude používat během celé své existence. Realisticky se však připouští i identifikátor založený na hardwarové adrese karty jako jeden z možných druhů DUID.

V rámci klienta se pak jednotlivé karty identifikují prostřednictvím Identity Association (IA). IA v podstatě reprezentuje balíček konfiguračních informací přidělených danému rozhraní.

Zkrátka vše je obecnější, ale také jaksi rozplizlejší a méně konkrétní. Určitou představu poskytne i prosté srovnání rozsahu definic. Zatímco RFC 2131 s definicí DHCPv4 měří něco málo přes 100 kB, draft-ietf-dhc-dhcpv6-28 měří zhruba dvojnásobek. A to ještě neobsahuje definice jednotlivých voleb, které mají své vlastní návrhy a dohromady přidají bratru dalších 100 KB.

Dlouho trvající vývoj a vyšší složitost výsledného návrhu vedly k nepříliš potěšujícímu stavu implementací. Právě jejich přehled je jádrem výše zmiňo-

vaného dokumentu projektu 6NET. Velmi stručný přehled testovaných implementací a utrpěných výsledků vypadá následovně:

KAME (v prostředí FreeBSD) Jediná alespoň trochu aktuální implementace (verze 26). Výsledek nelze nazvat jinak než jako legrační. Veškerá komunikace proběhla perfektně, klient dostal vše potřebné, až na to, že získané informace k ničemu nepoužil a nenastavil konfiguraci sítě.

KAME Linport Výsledek snahy přenést KAME do Linuxu. DHCP klient však posílá nesmyslnou adresu, takže mu server nemůže odpovědět.

DHCPv6 pro INRIA implementaci Dobře dopadla jen první fáze (hledání DHCP serverů). Klient pak nedokázal server oslovit se žádostí o konfigurační parametry.

DHCPv6 NetBSD pro Alpha64 Autoři neměli k dispozici stroj s Alpha procesorem. Pokusy o překlad pod Linuxem či FreeBSD byly neúspěšné.

Modifikovaná distribuce DHCP od IST, verze 3 Klient se zhroutil. Když jej nahradili jiným klientem, choval se server nekorektně.

DHCP pro HP-UX 11i Výsledky testů chybí.

DHCP od Motorola Labs Velmi experimentální. Řeší pouze přidělování adres.

Sečteno a podtrženo: pokud uvažujete o nasazení DHCPv6 ve vaší síti, neměli byste váhat a využít výhodné poványoční slevy ke koupi pevného provazu.

Abych ale nekončil tak depresivně, minulý týden se mi dostala do rukou zpráva o nové implementaci pro Linux. Dokonce vychází z poslední verze návrhu, tak se snad blýskne na lepší časy...

Příloha H Automatická konfigurace DNS

Publikováno v on-line časopisu Lupa 4. 4. 2006

Jedním z požadavků na IPv6 je automatická konfigurace. Představa, že člověk jednoduše připojí počítač k síti a bude mu fungovat síťování, aniž by kdokoli cokoli konfiguroval, je velmi lákavá (a z pohledu správce sítě částečně děsivá). Dlouhodobým problémem ale je, jak takové chování zajistit pro DNS.

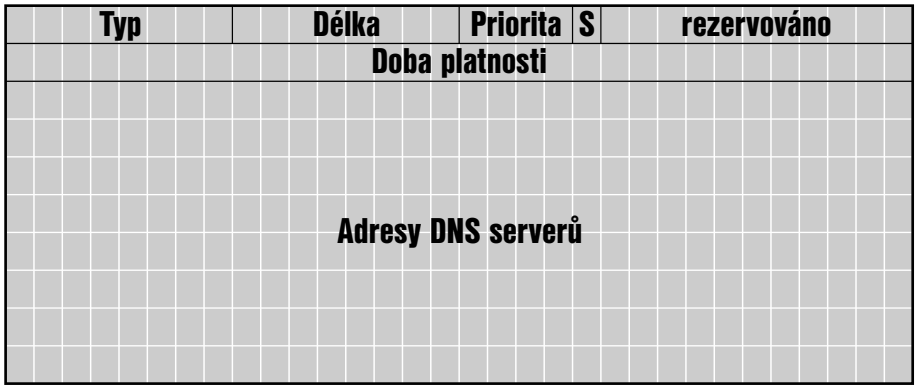
IPv6 samozřejmě umožňuje takzvanou stavovou konfiguraci prostřednictvím DHCPv6, u ní ale zpravidla správce sítě musí pro jednotlivé počítače cosi konfigurovat. Ten pravý bezobslužný ráj zajišťuje bezstavová konfigurace, jejímž základem je objevování sousedů (Neighbor Discovery, ND).

Jeho prostřednictvím počítač získá svou adresu, masku sítě i adresy implicitních směrovačů pro odesílání datagramů za hranice podsítě. Chybí v něm ale informace o místním DNS serveru, na nějž se má počítač obracet s DNS dotazy. Tato informace je nicméně velmi podstatná, protože život v síti bez DNS je jen těžko představitelný.

Značná pozornost se proto věnuje již několik let návrhu mechanismů pro automatickou konfiguraci adresy lokálního DNS serveru. Názory však dosud nejsou jednotné a ve hře je několik variant. Nedávno vyšlo informativní RFC 4339 shrnující navržené mechanismy a hodnotící jejich klady a zápory. Podívejme se, co je k mání.

H.1 Rozšíření objevování sousedů

Jestliže základem bezstavové automatické konfigurace je objevování sousedů, jedním z přirozených kandidátů je doplnit do něj chybějící informaci o místním DNS serveru. Návrh draft-jeong-dnsop-ipv6-dns-discovery (aktuálně ve verzi 8) proto navrhuje umožnit v ohlášení směrovače (Router Advertisement) novou volbu RDNSS, která by obsahovala adresy DNS serverů, které mají počítače používat.



Předností tohoto přístupu je, že počítače dostávají „vše v jednom“ – prostřednictvím jediné služby dostanou kompletní podklady pro konfiguraci. Jelikož objevování sousedů pracuje s dobou platnosti jednotlivých informací, lze zároveň dynamicky reagovat na případné změny. Navíc se jedná o nadstavbu známé služby, s níž jsou praktické zkušenosti a ví se, co od ní očekávat.

Na druhé straně objevování sousedů bývá typicky implementováno v jádře operačního systému. Jeho změna tedy vyžaduje zásah do jádra. I samotná změna již zavedené a fungující služby je sama o sobě potenciálním zdrojem problémů.

H.2 Bezstavové DHCP

DHCP samozřejmě dokáže poskytnout adresy DNS serverů. Pokud správce nechce použít DHCP ke kompletnímu nastavení komunikačních parametrů, může sáhnout po takzvaném bezstavovém DHCP definovaném v RFC 3736. Je koncipováno jako doplněk k bezstavové autokonfiguraci, tedy k objevování sousedů.

Počítač si základní síťové parametry (adresy a implicitní brány) opatří bezstavovou konfigurací a na bezstavové DHCP se obrátí pro ostatní informace, jež v objevování sousedů chybí. To samozřejmě podstatným způsobem zjednodušuje správu DHCP serverů, které v principu mohou běžet i na směrovačích (někteří výrobci již bezstavové DHCP podporují).

DHCP je dobře známá technologie, která navíc podporuje jak dobu platnosti poskytovaných informací, tak princip rekonfigurace na žádost serveru. Umožňuje tedy dynamické změny informací. Významnou předností zde je, že veškerá konfigurace může pocházet z jednoho zdroje, z jedné datové základny. V případě potřeby lze konfiguraci poskytovat individuálně, „na míru“ jednotlivým zařízením. Navíc je vše již popsáno v RFC, není třeba vyvíjet či rozšiřovat stávající mechanismy. DHCP definuje také mechanismy pro své rozšiřování, které umožňují později doplňovat další konfigurační informace.

Nevýhody bezstavového DHCP jsou spíše marginální. Vyžaduje přenos několika málo zpráv, což může být nevýhodou v prostředí velmi chudém na

přenosovou kapacitu či extrémně náročném na rychlost automatické konfigurace. Vyřízení DHCP dialogu přece jen stojí špetku času.

H.3 Dobře známá výběrová adresa

Se zajímavou myšlenkou přišel Masataka Ohta. Navrhl využít pro DNS výběrové (anycast) adresy, které zaručí, že dotaz bude doručen vždy nejbližšímu serveru hlásícímu se k dané adrese. Doporučuje zavést tři konstantní výběrové adresy pro místní DNS servery, které by se používaly vždy a všude. Byly by předkonfigurovány v DNS klientech a nic by se na nich nemuselo měnit.

DNS server by vhodným směrovacím protokolem ohlásil svou přítomnost a směrovače by mu na základě toho předávaly DNS dotazy z blízkého okolí. Aby se situace zjednodušila, v návrhu se požaduje, aby na každé lince byl nanejvýš jeden server s danou výběrovou adresou, a aby tedy doručování paketů na ni směřujících bylo vždy jednoznačné. Redundance se dosáhne tak, že při neúspěchu se klient obrátí na další z dobře známých adres.

Tato koncepce má řadu zajímavých vlastností. Nic se nepřenáší, takže není třeba definovat žádné protokoly ani datové formáty, navíc je konfigurace zařízena okamžitě. Pokud daný zákazník nemá vlastní DNS server, může snadno využívat DNS server svého poskytovatele – jednoduše bude nejbližší.

Vyžaduje ovšem, aby DNS servery aktivně vstoupily do směrovacího procesu, a s největší pravděpodobností budou nutné i konfigurační úpravy na směrovačích (povolení individuálních směrovacích záznamů, jejich filtrování, aby se nešířily mimo instituci a podobně). Za nedostatek lze považovat i skutečnost, že návrh draft-ohta-preconfigured-dns pochází z února 2004 a od té doby nebyl aktualizován.

Každá z navržených variant má rozhodně něco do sebe a teprve budoucnost ukáže, která se prosadí v nejširším měřítku, případně bude deklarována za jedinou podporovanou. Já osobně bych se lehce klonil k té prostřední. Především z toho důvodu, že umožňuje snadné potenciální budoucí rozšiřování o další informace, které možná za pár let budou považovány za stejně samozřejmé jako dnes DNS.

Příloha I Mobilní IPv6 – konečně RFC

Publikováno v on-line časopisu Lupa 9. 9. 2004

Po deseti letech jsme se konečně dočkali oficiální definice podpory mobilních zařízení v IP verze 6. Skončil tak pikantní stav, kdy povinná podpora mobility byla na jedné straně vyhlašována za jednu z významných předností IPv6, na straně druhé ale chybělo příslušné RFC a i proto byla její implementace odkládána.

Podívejme se na základní principy, podle kterých má podpora mobility fungovat. Některé z nich se za ta dlouhá léta prakticky nezměnily, ale u jiných (zejména v oblasti zabezpečení) došlo k podstatným úpravám.

I.1 Domácí agent

Jako mobilní uzel je označován počítač, který cestuje a současně komunikuje – typicky notebook či počítač do dlaně využívající bezdrátové připojení. Průběžně se připojuje do různých sítí a v důsledku toho neustále střídá své IP adresy (bývají označovány jako aktuální či dočasné adresy, anglicky care-of address). To způsobuje komplikace dvojího druhu:

- Chce-li s ním někdo navázat spojení, neví, na jaké adrese je momentálně k zastižení.
- Pokud on sám navázal spojení, vadí změna adresy protokolům vyšších vrstev (IP adresa je například součástí identifikace TCP spojení).

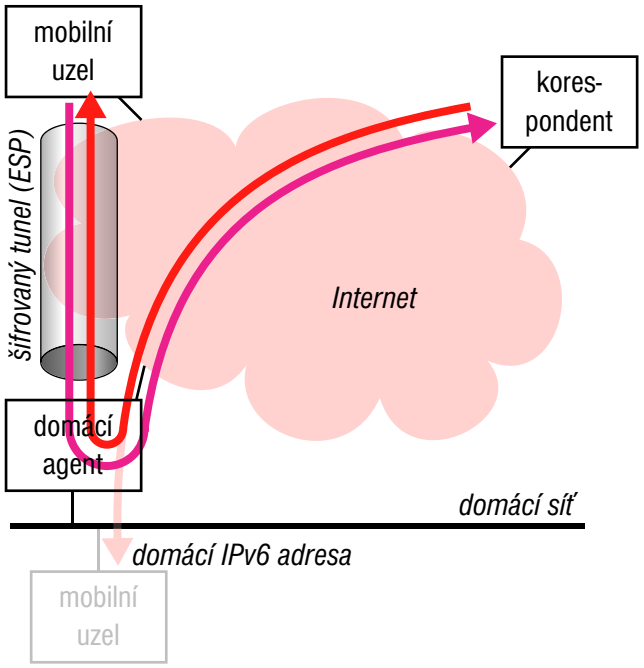
Pro řešení tohoto problému zavádí mobilní IP pojem domácí sítě a domácí adresy. Vychází z myšlenky, že každý mobilní uzel je někde doma a existuje síť, v níž je připojen, pokud zrovna není na cestách. Toto je jeho domácí síť a adresa, kterou v ní dostal přidělenu, je jeho domácí adresou. Pod touto adresou je zaregistrován v DNS, na ni se obracejí případní zájemci o spojení s ním a zpravidla ji také používá jako svoji vlastní.

Pokud se mobilní uzel zrovna nachází na cestách, zastupuje jej v domácí síti jeho domácí agent. Jedná se o jeden ze zdejších směrovačů, u nějž se mobilní uzel zaregistruje – pošle mu zprávu o své momentální dočasné adrese a požádá, aby jej zastupoval. U domácího agenta si vytvoří tak zvanou vazbu (v originále binding) mezi svou domácí a dočasnou adresou.

Od tohoto okamžiku začne domácí agent podvádět při objevování sousedů - vydává se za mobilní uzel a stahuje tak na sebe veškeré datagramy, které

směřují na jeho domácí adresu. Následně je přeposílá šifrovaným tunelem mobilnímu uzlu na aktuální adresu. Pro šifrování se používá IPsec, konkrétně hlavička ESP.

Tímto způsobem se přinejhorším může odehrávat celá komunikace. Protější partner (v terminologii mobilního IPv6 označovaný jako korespondent) posílá datagramy na domácí adresu mobilního uzlu, ty dorazí do jeho domácí sítě, odkud je domácí agent přepošle tunelem mobilnímu uzlu. Ten ve svých odpovědích použije jako adresu odesilatele opět svou domácí adresu, předá datagramy tunelem domácímu agentovi (jinak hrozí, že je zahodí některý firewall, protože by adresa odesilatele neodpovídala síti, ze které jsou odesílány) a ten je přepošle protějšímu stroji.



Obrázek I.1: Komunikace prostřednictvím domácího agenta

Popsaný režim pochopitelně zdaleka není ideální. Díky průchodu domácím agentem jsou pakety směrovány neefektivně, dochází ke zbytečnému zatěžování linek do a z domácí sítě a navíc možné selhání domácího agenta představuje potenciální riziko pro komunikaci jako takovou.

I.2 Optimalizace směrování

Proto je součástí mobilního IPv6 i optimalizace směrování. Díky ní sehraje mobilní agent svou úlohu jen při počátečním navázání komunikace mezi korespondentem a mobilním uzlem, zatímco později již datagramy proudí přímo mezi oběma koncovými body. Předpokladem pro optimalizaci je, aby se vazba mezi domácí a dočasnou adresou mobilního uzlu vytvořila i u korespondenta.

Tento krok v sobě ale skrývá potenciální bezpečnostní riziko. Je třeba zajistit, aby o sobě libovolný počítač nemohl prohlásit, že je třeba cestující www.seznam.cz a nezcizil tímto způsobem provoz, který mu nepatří.

Podle původních představ se o zabezpečení mělo postarat IPsec. To je skutečně použito, ale pouze mezi mobilním uzlem a jeho domácím agentem. Tady lze předpokládat, že se navzájem znají a že tudíž nebude problém vybavit je odpovídajícími klíči a dalšími náležitostmi. Ovšem korespondentem může být prakticky kdokoli, což činí IPsec nepoužitelným. Dokud nevznikne infrastruktura veřejných klíčů (a o stavu PKI asi nikdo z nás nemá žádné iluze), bude škálovatelnost IPsec prachmizerná a o podobných rolích si může nechat zdát.

Právě tady tkví jedna z příčin velkého zpoždění mobilního IPv6. Jeho autoři vsadili na mrtvého koně, neustále se drželi myšlenky použití IPsec a když byla v roce 2001 definitivně shozena se stolu, museli vymýšlet kompletně nové zabezpečení. Při té příležitosti to vzali od podlahy a radikálně změnili formáty používaných zpráv, takže specifikace z roku 2002 se výrazně liší od té z roku 2000.

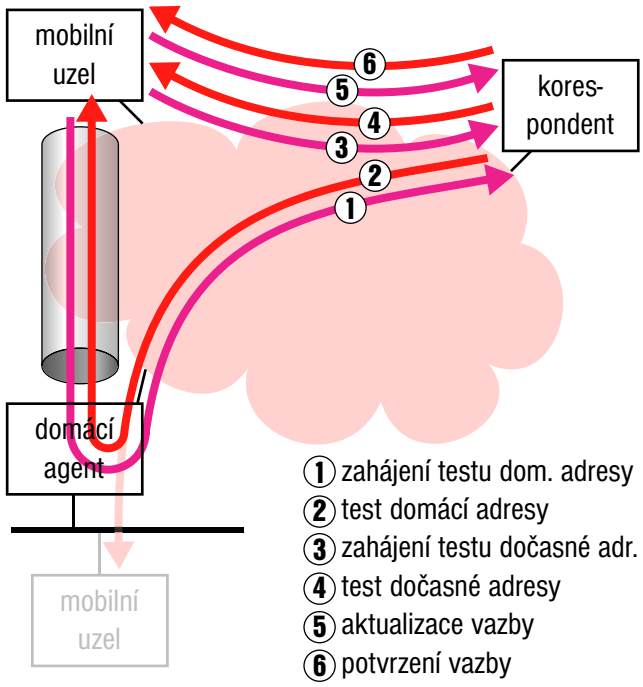
A jak to dopadlo? Bez možnosti opřít se o nějaký silnější mechanismus nakonec autoři mobilního IPv6 došli k závěru, že pro ověření totožnosti postačí, když mobilní uzel prokáže korespondentovi, že přijímá data jak na dočasné, tak na domácí adrese. Dotyčný proces byl pojmenován Return Routability Test.

Když mobilní uzel obdrží od domácího agenta tunelovaný datagram, dozví se tak, že se s ním někdo snaží komunikovat a používá jeho domácí adresu. Jako reakci pošle korespondentovi dvě zprávy: zahájení testu domácí adresy (home test init) a zahájení testu dočasné adresy (care-of test init). V první použije svou domácí adresu a tuneluje ji přes domácího agenta, zatímco druhou opatří svou dočasnou adresou a posílá ji přímo.

Jakmile korespondentovi dojde jedna z těchto inicializačních zpráv, reaguje na ni odesláním testu příslušné adresy. Test domácí posílá na domácí adresu (odkud by měl být tunelován), test dočasné opět adresuje přímo. Až mobilní uzel dostane oba testovací pakety, údaje z nich použije ke konstrukci žádosti o vytvoření vazby (tzv. aktualizace vazby), kterou pošle korespondentovi. V ní prokáže, že obdržel jak testovací zprávu směřující na domácí adresu, tak zprávu doručenou na adresu dočasnou. Pokud ji korespondent potvrdí, budou spolu oba nadále komunikovat přímo s využitím dočasné adresy.

Všech šest zmiňovaných zpráv (zahájení testů, testovací hodnoty i aktualizace a potvrzení vazby) je prošpikováno pořadovými čísly a kryptografickými konstrukcemi vycházejícími z náhodných a neveřejných čísel, aby se zabránilo různým nekalým hrátkám.

Mobilní uzel si udržuje přehled o partnerech, u nichž má registrovánu vazbu. Kdykoli změní svou aktuální adresu, posílá jim aktualizaci, aby měli neustále přehled o tom, jak s ním optimálně komunikovat. Analogicky samozřejmě informuje i svého domácího agenta.



Obrázek I.2: Aktualizace vazby u korespondenta

I.3 Rozšiřující hlavičky

Přímá komunikace ale není tak úplně jednoduchá, protože je třeba dočasnou adresu skrýt před protokoly vyšších vrstev. Každá strana proto do datagramů přidává jednu rozšiřující hlavičku. Mobilní uzel v datagramu jako odesilatele uvede svou dočasnou adresu, ale přibalí hlavičku nazvanou Domácí adresa obsahující jeho domácí adresu. Příjemce se pak podívá, zda pro danou dvojici adres má platnou vazbu a pokud ano, nahradí adresu odesilatele v datagramu domácí adresou z rozšiřující hlavičky. Jestliže platná vazba neexistuje, datagram s hlavičkou Domácí adresa se zahodí.

Z druhé strany se pak používá rozšiřující hlavička Směrování. Ta představuje obecnější mechanismus, kdy můžete datagramu předepsat průchod určitými body v síti. V každém z nich se vždy prohodí cílová adresa datagramu s další adresou uvedenou v hlavičce Směrování a jede se dál. Pro potřeby mobility byl definován jednodušší formát směrovací hlavičky. Obsahuje jen jedinou adresu. Při odeslání se jako cílová adresa datagramu uvede dočasná adresa mobilního uzlu a do hlavičky směrování se vloží jeho domácí adresa. Při příchodu do cíle se pak vymění, takže paket je zpracováván, jako by došel na domácí adresu uzlu.

Vedle těchto dvou byla ještě definována zcela nová rozšiřující hlavička Mobilita, která slouží především pro správu vazeb. Jejím prostřednictvím se zasílají aktualizace a potvrzení vazeb, údaje pro test dosažitelnosti a podobně.

Několik dalších doplňků bylo definováno do ICMP a objevování sousedů. Jejich

cílem je především automatické objevování kandidátů pro domácí klienty a rychlejší orientace mobilního uzlu v dočasné síti.

Definice mobility v IPv6 rozhodně není nic jednoduchého. Příslušné RFC 3775 měří zhruba 350 KB, a to ještě byly detaily použití IPsec pro komunikaci mezi mobilním uzlem a domácím agentem vystrčeny do samostatného RFC 3776 o délce blížící se 100 KB textu. Ovšem podstatné je, že konečně leží na stole její finální podoba a může vypuknout implementace. Dlouhodobě nejdál je v této oblasti japonský projekt Kame pro BSD. Pro ostatní platformy lze jen doufat, že se v dohledné době polepší.

Příloha J IPv6 – přechodové mechanismy (1)

Publikováno v on-line časopisu Lupa 14. 3. 2002

O tom, že nahrazení starého IPv4 novým protokolem IPv6 bude muset být pozvolné a nabídnout dostatečně dlouhou přechodovou dobu, kdy síť bude podporovat oba protokoly současně, není pochyb. Podívejme se dnes na mechanismy, které dosud byly vymyšleny k usnadnění jejich vzájemné budoucí koexistence.

Jsou především výsledkem práce skupiny Next Generation Transition (NGTRANS), která má v rámci IETF v popisu práce právě tyto aktivity. Lze je rozdělit do tří kategorií: dvojí zásobník, tunelování a překladače.

J.1 Dvojí zásobník (dual stack)

Tento přístup by zřejmě napadl každého: počítače prostě budou podporovat dva protokoly a pro komunikaci se podle potřeby použije IPv4 nebo IPv6 – v závislosti na schopnostech protějšího konce. Oba se zpravidla chovají jako navzájem nezávislé a případná komunikace mezi nimi probíhá až na úrovni aplikační vrstvy.

V tomto režimu se nyní nachází valná většina zařízení podporujících IPv6. Má pochopitelně jedno velmi zásadní omezení: vyžaduje přítomnost IPv4 a tedy IPv4 adresu. Z hlediska perspektivy dalšího rozvoje tudy cesta nepovede, protože právě IPv4 adresy začínají docházet.

Ovšem prvky s dvojím zásobníkem se objevují prakticky ve všech dalších přechodových mechanismech. V nich se datagramy převádějí z jednoho světa do druhého.

J.2 Tunelování

Nejvýznamnější specifikace	
Základní mechanismy tunelování	RFC 2473
Tunel server, tunel broker	RFC 3053
6to4	RFC 3056
6over4	RFC 2529
ISATAP	draft-ietf-ngtrans-isatap

Tunelování je obecný princip, jak protlačit data jim nepřátelským územím. V našem případě se typicky jedná o přenos IPv6 datagramů sítí, která podporuje

jen IPv4 (v pozdějších fázích přechodu se očekává, že to bude právě naopak). Tunel představuje virtuální dvoubodový spoj. Na jednom jeho konci se IPv6 datagram zabalí jako data do běžného IPv4 datagramu a pošle se na IPv4 adresu druhého konce tunelu. Tam se původní IPv6 datagram vybalí a odešle dál – buď IPv6 sítí nebo třeba dalším tunelem. To záleží na zdejších směrovacích tabulkách.

Nejjednodušší případ představují **manuální tunely**, které je třeba explicitně nakonfigurovat. Správci obou koncových systémů musí zadat příkazy, jimiž se vytvoří tunel, a podniknout kroky k jeho začlenění do směrovacích tabulek na obou zařízeních. Právě manuálně konfigurované tunely dnes drží pohromadě síť 6bone.

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

Jelikož se v praxi ukázalo, že rozhraní pro uživatele a vlastní realizace tunelu jsou dva dost odlišné úkoly, došlo k rozdělení práce. Tunel broker dostal na starosti správu systému, komunikaci s uživateli a řízení dalších komponent. Naproti tomu tunel server bývá typicky směrovač, který pouze zajišťuje vlastní tunelování. Jeden tunel broker tak může řídit celou skupinu tunel serverů a například vybírat pro každého uživatele ten z nich, který je pro něj topologicky nejvýhodnější.

Vedle manuálních tunelů jsou k dispozici i tunely automatické. Jedny vycházejí přímo z IPv6 adres. Pokud má počátečních 96 bitů nulových, představuje adresu pro automatické tunelování. Posledních 32 bitů se interpretuje jako IPv4 adresa, datagram se zabalí do IPv4 a pošle na ni. Zatím se ale nezdá, že by tento způsob komunikace čekala zářná budoucnost – například proto, že předpokládá podporu IPv4 na cílovém stroji. Zajímavější jsou jiné mechanismy pro automatické tunelování.

J.3 6to4

Jako daleko nadějnější se jeví **6to4**. Vychází z předpokladu, že máme dvě koncové IPv6 sítě, mezi nimiž leží konfekční IPv4 Internet. Na hranici mezi nimi a Internetem bude směrovač podporující 6to4. Data poběží koncovými sítěmi v nativním IPv6 a mezi oběma hraničními směrovači se budou tunelovat. K tomu hraniční směrovač potřebuje alespoň jednu IPv4 adresu.

Z ní se vytvoří 6to4 prefix pro adresy koncové sítě. Konstruuje se tak, že za počátečních 16 bitů s hodnotou 2002 (šestnáctkově) se připojí 32 bitů IPv4 adresy hraničního směrovače. Tím vznikne obvyklý 48 bitů dlouhý prefix,

kterým lze adresovat podsítě a počítače v koncové síti. Jediná IPv4 adresa tak pro ni umožňuje zavést plnohodnotné IPv6 adresy.

Kdykoli hraniční směrovač dostane datagram s prefixem začínajícím 2002::/16, vyzvedne si z následujících 32 bitů IPv4 adresu a na ni datagram pošle tunelem. Pokud naopak dorazí tunelovaná data na jeho vlastní IPv4 adresu, vybalí IPv6 datagram a odešle jej do "své sítě". Báječnou vlastností tohoto schématu je, že nevyžaduje žádné úpravy v uzlech. Vše je postaveno na standardních mechanismech, jediným novým prvkem je hraniční 6to4 směrovač. Stačí, aby ohlašoval do lokální sítě směrovací informaci, že přes něj vede cesta do sítě 2002::/16 a vše bude skvělé.

J.4 6over4

Zatímco 6to4 řeší otázku vzájemné komunikace mezi koncovými IPv6 sítěmi, **6over4** míří přímo do nich. Počítá s tím, že koncová síť umí pouze IPv4 a snaží se zajistit, aby v ní mohly působit IPv6 stroje. V podstatě používá IPv4 síť jako linkový protokol pro přenos IPv6 datagramů.

6over4 staví na standardních mechanismech, jako je objevování sousedů a podobně. Když chce odeslat data jinému počítači ve zdejší síti, zjistí si prostřednictvím objevování sousedů jeho IPv4 adresu a na ni pak odešle tunelovaný IPv4 datagram. Vlastní adresu si může zjistit z ohlášení směrovače a podobně.

Je tu ale nemalý zádrhel. Mechanismy objevování sousedů používají skupinové adresy (multicast). 6over4 definuje postup, jak se tyto adresy mapují na IPv4 skupiny (převezmou se jejich poslední dva bajty a před ně se předřadí 239.192). Vyžaduje však, aby koncová síť podporovala skupinové adresování. Bohužel při současném stavu multicastu na datových tocích to není vůbec triviální požadavek. Nad praktickou použitelností 6over4 tak visí velký otazník.

J.5 ISATAP

Analogické cíle, ale menší nároky má **Intra-Site Automatic Tunnel Addressing Protocol** (ISATAP). Také zde se řeší otázka vzájemné komunikace IPv6 strojů v koncové síti, která podporuje jen IPv4. A rovněž se IPv4 používá jako protokol linkové vrstvy. Tentokrát se však nekladou na IPv4 žádné speciální nároky.

ISATAP kóduje IPv4 adresy strojů do identifikátoru rozhraní, tedy do závěrečných 64 bitů. Konstruuje identifikátor tak, že jeho počátečních 32 bitů obsahuje 0000:5EFE. Za ně se připojí 32 bitů s IPv4 adresou odpovídajícího rozhraní.

Když ISATAP rozhraní dostane datagram ze své podsítě s takto konstruovaným identifikátorem, tuneluje jej uvnitř IPv4 datagramu na adresu, kterou získá z jeho závěrečných čtyř bajtů. Pokud tento leží v jiné síti či podsíti, přijde ke slovu směrování. Aby vše fungovalo, měl by "next hop" ve směrovací tabulce

používat zdejší ISATAP adresu, aby byl dosažitelný prostřednictvím ISATAP sítě.

ISATAP nemá žádné požadavky na prefix sítě a podsítě (prvních 64 bitů adresy) – ty mohou být zcela libovolné. Například se může jednat o 6to4 prefix. Je tedy docela dobře představitelné schéma, že v lokální IPv4 síti se IPv6 datagramy budou tunelovat na bázi ISATAP k hraničnímu 6to4 směrovači, který je protuneluje do cílové sítě a zde opět nastoupí ISATAP, aby datagramy dopravil k adresátovi.

Největším zádrhelem ISATAP je plnění tabulky implicitních směrovačů. Hromadné ohlášení směrovače tu není k dispozici (od IPv4 se neočekává podpora skupinových či oznamovacích adres). Plánuje se tedy využití DNS, případně manuální konfigurace, následované ověřováním prostřednictvím individuálně adresované výzvy směrovači a jeho odpovědi.

ISATAP se zatím nachází ve fázi pracovního návrhu (draft). Svými minimálními požadavky na IPv4 je lákavý, ale obávám se, že vyžaduje příliš zásadní úpravy na straně všech uzlů lokální sítě. Uvidíme, zda se mu podaří oslovit širší spektrum uživatelů.

Všechny dosud popsané metody měly jednu společnou vlastnost: oba komunikující partneři hovořili stejným protokolem. Co když ale budu chtít ze svého IPv6 klienta hovořit se serverem, který podporuje výlučně IPv4. Toto je úloha pro překladače, kterým se budu věnovat příště.

Příloha K IPv6 – přechodové mechanismy (2)

Publikováno v on-line časopisu Lupa 28. 3. 2002

Po předchozím kursu tunelování se dnes podíváme na ty přechodové mechanismy, které usilují o soužití obou světů. Převádějí datagramy z jednoho formátu do druhého a umožňují, aby si třeba IPv6 aplikace popovídala s IPv4 serverem.

K dispozici jsou následující prostředky:

SIIT	RFC 2765
NAT-PT	RFC 2766
BIS	RFC 2767
BIA	draft-ietf-ngtrans-bia
TRT	RFC 3142

K.1 SIIT aneb Praotec Převodník

Srdcem většiny konverzních mechanismů je vlastní převod mezi IPv4 a IPv6 datagramem. Je definován pod jménem **SIIT (Stateless IP/ICMP Translation)** v RFC 2765. Obsahuje přesná pravidla, jak se jednotlivé položky datagramu převádějí do položek druhého formátu.

Asi nejzajímavější je převod adres. Pro směr z IPv4 do IPv6 používá tak zvané IPv4-překládané adresy, které mají tvar 0::ffff:a.b.c.d. Čili v počátečních 80 bitech jsou samé nuly, následuje 16 bitů jedničkových a v závěrečných 32 bitech je IPv4 adresa, kterou chceme vyjádřit. Třeba adresa Lupy (62.84.129.156) by v IPv4-překládaném tvaru zněla 0::ffff:62.84.129.156.

Horší je to v opačném směru – když je třeba převést IPv6 adresu do IPv4 světa. V tomto případě se SIIT zařízení musí chovat jako klasický NAT. Musí mít k dispozici sadu IPv4 adres, které k tomuto účelu používá, a IPv6 adresu prostě nahradí jednou z nich. SIIT sám o sobě neřeší otázku přidělování IPv4 adres – tohle ponechává na okolních mechanismech. V důsledku to znamená, že tvoří jen jakýsi základní stavební kámen, na kterém je třeba vybudovat něco, co bude doopravdy fungovat.

K.2 NAT-PT

Jedním z cílů IPv6 je smést NAT s povrchu zemského. Ovšem když teče do bot, je občas třeba spojit se i s nepřítelem. Proto vznikl návrh, jak zapojit

NAT do práce pro světlou stranu Síly. Umožňuje strojům z lokální IPv6 sítě komunikovat s globálním IPv4 Internetem.

Network Address Translation – Protocol Translation (NAT-PT) je v zásadě starý špatný NAT, ale tentokrát převádí mezi IPv4 a IPv6 adresami. Typická pozice pro něj je na hraničním směrovači mezi lokální sítí a Internetem.

Je založen na SIIT a doplňuje k němu chybějící prvky. Nevyžaduje striktně použití IPv4-překládaných adres, stačí mu libovolný prefix zvolený správcem sítě. Za něj se připojí 4 bajty s IPv4 adresou. NAT-PT stroj šíří do vnitřní sítě směrovací informaci, že "umí tento prefix", aby se datagramy určené do vnějšího Internetu posílaly jemu.

Když některý z lokálních IPv6 počítačů odešle takový datagram, na NAT-PT se vytvoří vazba mezi jeho IPv6 adresou a některou z volných IPv4 adres, kterými NAT-PT disponuje. Podle pravidel SIIT se datagram přepracuje na IPv4 a odešle do Internetu. Když po chvilce dorazí odpověď, NAT-PT využije stávající mapování, změní jej na IPv6 s odpovídající adresou (odesilatele přemapuje na prefix:původní_IPv4) a odešle do vnitřní sítě.

Návrh připouští statické mapování (každý z lokálních strojů má pevně přidělenu IPv4 adresu), i dynamické (přidělují se za chodu podle potřeby). NAT-PT také švindluje DNS. Při dotazech zvenčí předělává A (dotaz na IPv4 adresu) na AAAA či A6 a předává zdejší serverům. Když server odpoví, vytvoří si mapování pro IPv6 adresu z odpovědi a vrátí původnímu tazateli A záznam s mapovanou IPv4 adresou. Díky tomu lze navazovat spojení i směrem dovnitř zdejší sítě.

Pro DNS dotazy směřující z vnitřní sítě ven přidává k AAAA/A6 i dotaz na A záznam a pokud přijde odpověď, změní jej na AAAA či A6 s adresou v obvyklé podobě prefix:IPv4.

Existuje ještě divočejší podvarianta s názvem NAPT-PT, která vedle IP adres mapuje i porty. Klasický NAT-PT nechává porty být a mění jen adresy. V případě NAPT-PT se mapuje dvojice lokální IPv6 adresy a UDP/TCP portu na dvojici IPv4 adresy a portu. Díky tomu překladač vystačí s podstatně menším počtem adres (třeba i jen s jedinou).

Očekává se, že NAT-PT sehraje v přechodné fázi mezi IPv4 a IPv6 poměrně významnou úlohu. Rozhodně patří do "základní výbavičky" přechodových mechanismů.

K.3 BIS aneb utajované operace v každém počítači

BIS čili **Bump In the Stack** řeší problém nedostatku IPv6 aplikací. Vychází z představy, že váš počítač podporuje IPv4 i IPv6 a je připojen k síti přenášející oba protokoly. Ovšem některé zdejší aplikace umí jen IPv4.

Proto uvnitř počítače (konkrétně mezi IPv4 a ovladačem síťové karty) číhá

BIS. Zachytává IPv4 DNS dotazy a vedle původního dotazu na A záznam přidá i AAAA či A6. Dorazí-li IPv4 odpověď, předá ji aplikaci a nechá vše vyřídit starším protokolem.

Problém vznikne, když dojdou pouze odpovědi s IPv6 adresami. Těm by aplikace nerozuměla, takže je hbitě namapuje na IPv4 a předá aplikaci A záznam s mapovanou adresou. Když pak aplikace odesílá datagramy na danou IPv4 adresu, BIS je zachytává, transformuje na IPv6 a předává na původní adresu. Analogicky mění odpovědi.

Vzhledem k tomu, že mapované IPv4 adresy nikdy neopustí daný počítač (jsou vnitřní záležitostí mezi BIS a aplikací), klidně lze pro ně použít privátní adresní rozsahy 10.0.0.0 a spol.

BIS funguje i v opačném směru, když spojení navazuje protější IPv6 počítač. Tentokrát však není nutno harašit s DNS, stačí jen namapovat adresy a měnit datagramy.

Určitou variantou tohoto přístupu je **Bump In the API (BIA)**, které dělá v podstatě totéž, ale jinde. Tentokrát není agent ukryt mezi IP a ovladačem karty, ale v systémových knihovnách zajišťujících přístup k síťovým službám. Když aplikace volá knihovní funkce pro IPv4, jsou interně změněny na volání IPv6 služeb. Čili nedochází k překladu datagramů, ale vytváří se již čisté IPv6 pakety, zatímco aplikace si myslí, že používá IPv4 služby.

Osobně bych neočekával závratné rozšíření těchto metod. Podle znalců není úprava aplikace pro podporu IPv6 nijak náročná a toto řešení je přece jen o poznání systémovější.

K.4 TRT

Transport Relay Translator se hodně podobá NAT-PT. Tentokrát se však překlad odehrává až v transportní vrstvě, nikoli v síťové. TRT překladač funguje podobně jako některé firewally. Umí IPv4 i IPv6, sedí mezi oběma komunikujícími partnery a každému z nich předstírá, že je ten druhý.

Zatím byl definován pouze postup při navazování TCP spojení ve směru od IPv6 počítače k IPv4 stroji. Jedinou překážkou pro opačný směr je nalezení vhodného mechanismu pro mapování adres. Pro mapování IPv4 na IPv6 se používá výše zmiňovaný postup: vyhradí se prefix (tentokrát 64 bitů dlouhý, pocházející z prefixu pro zdejší síť) a adresy počítačů z IPv4 světa se mapují jako prefix:IPv4_adresa.

Řekněme, že cílový počítač bude Lupa (62.84.129.156) a dotyčný prefix bude 3ffe:a:b:c::/64. Chce-li IPv6 počítač navázat TCP spojení s Lupou, pošle žádost o navázání spojení na 3ffe:a:b:c::62.84.129.156. TRT překladač šíří v lokální síti směrovací informaci, že on je ta pravá cesta do 3ffe:a:b:c::/64, takže mu tato žádost dorazí.

Iniciátorovi spojení odpoví sám a bude předstírat, že on je Lupa. Paralelně naváže spojení s Lupou – cílovou adresu si vyzvedne z posledních 4 bajtů původní adresy a pro odesilatele použije svou vlastní IPv4 adresu. Lupě pro změnu bude předstírat, že je onen klient.

Místo jednoho spojení mezi serverem a klientem budou tedy existovat dvě. Klient-překladač po IPv6 a překladač-server po IPv4. Následně bude prostě z datagramů přicházejících z jednoho vybalovat jejich obsah a předávat jej do druhého.

Pro UDP se chová obdobně, jen zde odpadá nutnost navazovat spojení. Návrh neřeší otázku, kde proběhne konverze adres z IPv4 do výše zmiňovaného IPv6 tvaru s vyhrazeným prefixem. Připouští modifikaci DNS serveru v síti, případně úpravu DNS klienta v jednotlivých počítačích.

Příloha L Jak jsou na tom čeští ISP s IPv6?

Publikováno v on-line časopisu Lupa 17. 3. 2005

Što takóje IPv6? Zkoušeli jsme prozkoumat stav implementace IPv6 u českých poskytovatelů Internetu. Nebudeme dlouho chodit kolem horké kaše a řekneme si to na rovinu: stav IPv6 v sítích tuzemských ISP neskýtá příliš utěšený pohled. Nemálo z nich se v tomto ohledu ani nevyjádřilo, což určitě nevyznívá v jejich prospěch.

V touze zmapovat podporu IPv6 jsem se obrátil s patřičným dotazem na nejvýznamnější domácí komerční poskytovatele Internetu. Vedle „klasických“ firem jsem do průzkumu zařadil i dvě kabelové společnosti s celostátním pokrytím a všechny tři mobilní operátory, protože mobilní telefony jsou považovány za segment, pro nějž je IPv6 obzvláště zajímavé. Jistě už tušíte, že ani jeden z mobilních operátorů mi neodpověděl...

Sběr informací přinesl některé netušené zážitky. Například se od té doby zabývám úvahami, k čemu jsou informační linky, jež nikdo ani po několika minutách vyzvánění nezvedá. Snad jako jukebox, hrají tam docela dobře. Není to špatná služba, ale ještě by bylo záhodno implementovat výběr písniček.

Na osmnáct rozeslaných dotazů jsem dostal osm odpovědí. Tedy více než polovině oslovených nestálo za námahu reagovat. Dovolím si předpokládat, že s IPv6 to v jejich sítích nebude slavné. Neúspěšný pokus vyhledat Googlem v jejich doménách IPv6 mne v tom utvrzuje. Jedná se o společnosti: Český telecom (IOL), eTel, Eurotel, Karneval, Nextra, Oskar, SkyNet, T-Mobile, T-Systems a UPC.

Na dorazivší odpovědi se podíváme v abecedním pořadí:

L.1 Contactel

IPv6 není implementováno a zatím nezaznamenali žádný požadavek ze strany zákazníků na tuto službu. Nicméně zjevně se snaží být připraveni – mají přidělen prostor IPv6 adres a v krajských městech mají připraveno zařízení pro nasazení 6PE.

L.2 Czech On Line (COL)

První dobrá zpráva – COL nabízí svým zákazníkům IPv6. Je k dispozici zdarma pro komutované připojení službou Volný (viz informační stránku), u ostatních

zákazníků závisí na typu připojení – v testovacím režimu se nachází několik firemních zákazníků. Ze strany COL je služba zatím považována za vývojovou a testovací, k zájemcům se snaží přistupovat individuálně a postupně nasazení IPv6 rozvíjet. Protokol se nabízí jako přídavek k IPv4, a to bez příplatku. Nativní připojení lze realizovat přibližně v polovině sítě, pro ostatní zákazníky připadají v úvahu tunely. V páteřní síti je IPv6 implementováno nativně.

Slušný je sortiment služeb. Servery všech služeb poskytovaných COL mají IPv6 konektivitu, ne všechny ji však využívají. IPv6 transport nabízejí všechny DNS servery, unixové FTP servery a news server. Postupně plánují aplikační služby využívající IPv6 rozšiřovat (WWW, pošta). Pro koexistenci IPv4 a IPv6 nabízejí Teredo server a 6to4 relay. V síti COL je umístěn i server XS26, nabízející tunely pro připojení k IPv6 síti.

Zájem zákazníků je ojedinělý. Počet uživatelů IPv6 se pohybuje v řádu jednotek.

L.3 České radiokomunikace

IPv6 nepoužívá, ani o jeho zavedení neuvažuje.

L.4 GTS Novera

IPv6 testovali v laboratorních podmínkách. Zákazníkům je ale nenabízejí, ani to nepřipravují.

L.5 ha-vel

Absolvovali zkušební a ověřovací provoz IPv6 v síti a jsou připraveni poskytnout IPv6 jako provozní službu, a to v libovolném místě své sítě. Zatím však postrádají zájem ze strany zákazníků. Cenová ani informační politika nebyly zatím oficializovány – s prvními zájemci bude zavedení služby řešeno individuálně.

L.6 InWay

Momentálně IPv6 nenabízí, ale pracuje na tom. V současnosti probíhají testy a předpokládají, že zákazníkům je nabídnou na podzim.

L.7 Tiscali

Druhá společnost, která již v současnosti nabízí IPv6. V síti je implementováno nativně. Můžete si pořídit buď oba protokoly, nebo se připojit jen přes IPv6. V prvním případě nic nepřiplácíte, ve druhém je cenová politika stejná jako pro

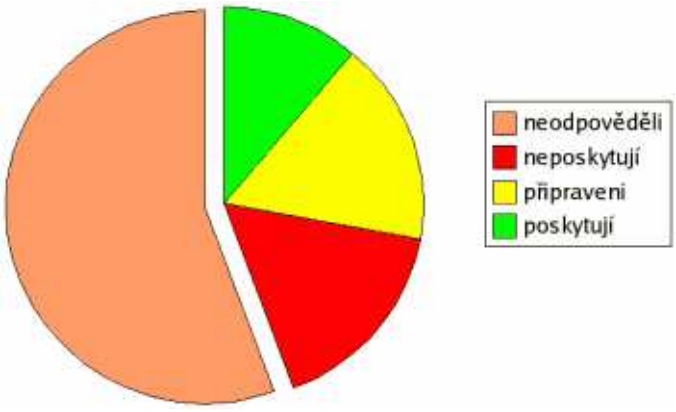
IPv4. IPv6 je nabízeno všude tam, kde je k dispozici připojení do páteřní sítě Tiscali. Pokud se služeb týče, je k dispozici DNS pro IPv6 (včetně reverzních záznamů). Zájem je však zatím malý, podle odhadu Tiscali využívá IPv6 méně než procento zákazníků. Dostal jsem i odkaz na web, kde však najdete jen obecné informace o IPv6 jako takovém, nikoli o službách Tiscali v této oblasti. Ale je tam alespoň odkaz na formulář se žádostí o aktivaci služby či doplňující informace.

L.8 Tele2

IPv6 otestovali v páteřní síti i na aplikačních serverech, zatím je však zákazníkům nenabízejí, ani o tom neuvažují.

L.9 Shrnutí

Převeden do podoby koláčového grafu vypadá výsledek průzkumu následovně:



Firmy, jež na můj dotaz nedopověděly, s největší pravděpodobností IPv6 nepodporují. Čili 72 procent z nejvýznamnějších komerčních poskytovatelů Internetu v naší republice tento protokol neposkytuje, 17 procent je na něj připraveno nebo jej chystá a u zbývajících jedenácti procent se můžete přes IPv6 připojit již dnes.

Je to dobrý či špatný stav? Zpočátku mě výsledky připadaly bídné, ale čím více o nich přemýšlím, tím více jsem nakloněn tomu, považovat je vlastně za docela dobré. IPv6 vězí v problému slepice vs. vejce. Uživatelé jej příliš nepoužívají, protože je jeho prostřednictvím dostupných jen málo služeb. A kdo by pro IPv6 portoval služby, když jej nikdo nevyužívá?

Z toho důvodu je zájem zákazníků nizoučký, jak ostatně dokládají zkušenosti Czech On Line a Tiscali. Nabídnutí IPv6 lze v současné době z pozice komerčního poskytovatele považovat spíše za misionářskou činnost než za zlatý důl. Proto vnímám jako pozitivní, že vůbec nějací takoví poskytovatelé jsou a že se zjevně jejich řady rozšiřují. Jen houšť a větší kapky.

Příloha M IPv6 v evropských akademických sítích

Publikováno v on-line časopisu Lupa 17. 4. 2003

Od té doby, co nejvýznamnější výrobci směrovačů nabídli podporu IPv6 ve svých řadových produktech, nastal v rozšíření protokolu nezanedbatelný posun. Jako obvykle najdeme mezi pionýry této nové technologie akademické sítě. Ostatně právě experimentování s novými technologiemi a službami je jejich největším přínosem.

Když se rozhlédneme po národních akademických sítích evropských zemí, najdeme více či méně pokročilé nasazení IPv6 víceméně všude. Zpravidla staví na tunelech, kdy jsou IPv6 datagramy zabaleny do IPv4 a přepravovány na místo určení běžnou IPv4 sítí. Existují však výjimky, které jsou s podporou IPv6 dál a snaží se integrovat nový protokol jako běžnou službu sítě. Právě těm se dnes budu věnovat.

M.1 SURFnet (Nizozemsko)

Nizozemci notoricky patří v síťování k absolutní evropské špičce, a proto jistě nepřekvapí, že s podporou IPv6 jsou dnes nejdál. Jejich akademická síť existuje již v páté generaci. SURFnet5 byl uveden do provozu v roce 2001 a od samého začátku nativně podporoval IPv6. To znamená, že směrovače páteřní sítě podporují jak IPv4, tak IPv6 (tzv. dual stack řešení).SURFnet5 lze celkově považovat za sen každého mladého síťaře. Jádrem sítě je čtveřice do kruhu propojených směrovačů a každý uzel je připojen nezávislými okruhy ke dvěma směrovačům jádra. To vše na rychlosti 10 Gbit/s technologií IPoverDWDM s POS rámci. Používají se směrovače Cisco GSR 12416.

Také připojení koncových sítí se zpravidla odehrává pod obojí způsobou. Ve výjimečných případech je koncová síť připojena dvěma okruhy – jedním pro IPv4 a druhým pro IPv6. Připouštějí i připojení tunelem, ovšem pouze jako dočasné řešení. Takový zájemce musí připravit plán, jak přejít na serióznější IPv6 komunikaci, tedy dual stack či nativní IPv6 okruh.

Jako směrovací protokol používají IS-IS, který dokáže pod jednou střechou řešit směrování obou protokolů. Databáze linek, z níž IS-IS vychází, je společná a IPv4 se od IPv6 odlišuje jen atributy.

Provozovatelé SURFnetu přiznávají, že postavení IPv6 není zcela rovnocenné starší verzi protokolu, protože je pomalejší. To je způsobeno použitým hard-

warem. Zatímco IPv4 směruje přímo karta rozhraní, IPv6 je předáváno centrálnímu procesoru směrovače a jeho směrování tudíž neprobíhá plnou rychlostí (wirespeed). Proto chystají výměnu karet rozhraní za novější model, který již podporuje rovnocenné směrování obou verzí IP.

M.2 Funet (Finsko)

Skandinávie patří mezi další notorické příklady kvalitní síťové infrastruktury. Z pohledu IPv6 je ze skandinávských zemí nejdále Finsko, které také podporuje jak IPv4, tak IPv6 v nativní podobě. Páteřní směrovače tedy mají implementovány oba protokoly.Finská páteřní síť byla v roce 2001 povýšena na 2,5 Gbit/s s technologií POS (v roce 2001 se v síťové Evropě vůbec děly Věci, ten letopočet ještě uvidíte). Zároveň změnili dodavatele klíčových prvků. Dřívější Funet stavěl výlučně na směrovačích Cisco, nová generace sítě k nim přidala Juniper M20.

Právě toto smíšené prostředí způsobilo správcům sítě nejednu vrásku na čele. Rozhodli se totiž nasadit dva samostatné směrovací protokoly - OSPFv2 pro IPv4 a IS-IS pro IPv6. Bohužel se ukázalo, že Juniper odmítá použít IS-IS jen pro IPv6 a přibaluje k němu i některé IPv4 informace, s nimiž mělo pro změnu problém Cisco. Zkrátka ladění vzájemné spolupráce obou platforem a objevování nedokumentovaných vlastností, jež umožnily problém vyřešit, bylo pracné a frustrující.

Cíle se však nakonec podařilo dosáhnout a ve druhé polovině roku 2002 začalo jádro Funetu nativně podporovat IPv6. Problematičtější je situace v přístupových sítích, jejichž prostřednictvím se připojují koncové sítě. Zavádění IPv6 do nich teprve probíhá, takže ne každý se zatím může k Funetu připojit po nativním IPv6.

M.3 Renater (Francie)

Francie sice nemá pověst síťové velmoci, nicméně v oblasti IPv6 hraje významnou roli již od velmi raného stadia příprav nového protokolu. Současná akademická páteř nese označení Renater3 a nativní IPv6 podporuje přibližně od poloviny roku 2002.Páteřní linky mají kapacitu 2,5 Gbit/s a jsou osazeny směrovači Cisco GSR. Podpora IPv4 a IPv6 je zcela rovnocenná, a to i z hlediska výkonnostního. Pro směrování se používá kombinace IS-IS a iBGP.

Síť Renater3 má ovšem poměrně málo uzlů, přibližně 30. Přístup jednotlivých institucí k páteři proto zprostředkovávají regionální sítě, které nejsou, přinejmenším z pohledu IPv6, nijak koordinovány. Radikálně se liší míra jejich podpory IPv6 i způsoby, kterými je realizována. Použité metody sahají od 6PE přes virtuální sítě a dual stack až po tunely či vyhrazené ATM PVC kanály.

Mezi zajímavostí patří, že v síti Renater3 je poměrně dobře rozvedena virtuální síť M6Bone, která je určena pro přenos skupinově adresovaných IPv6

datagramů (čili IPv6 multicast). Právě skupinové adresování je na stávajících platformách málo podporováno a v dopisech Ježíškovi patří u všech akademických sítí na přední místa.

M.4 GARR (Itálie)

Tady se s nativním podporou IPv6 prostřednictvím dual stack směrovačů teprve začíná. Klíčové směrovače jádra sítě již byly povýšeny (jedná se o modely Cisco GSR 12416 a Juniper M20) a v současné době pracují na konfiguraci směrování. Zatím se IPv6 směruje jen staticky, cílovým stavem by mělo být použití OSPFv2 pro IPv4 a OSPFv3 pro IPv6 (vzhledem k neutěšenému stavu implementací OSPFv3 mi to připadá jako potenciální zdroj problémů). Přibližně do poloviny roku plánují rozšířit IPv6 na celou síť.

M.5 6WiN (Německo)

Všechna doposud popsaná řešení vycházela ze stejného konceptu – dual stack směrovačů s podporou obou protokolů. Lišily se jen technické detaily. Naproti tomu v Německu se rozhodli vyrazit jinou cestou. Zdejší akademická síť G-WiN s páteří o rychlosti 2,5 Gbit/s má zůstat čistě IPv4 sítí.Pro IPv6 se odhodlali postavit novou, samostatnou síť nazvanou 6WiN. V současnosti zahrnuje šest směrovačů propojených okruhy s kapacitou 34 Mbit/s, určených výlučně pro přenos IPv6. IPv6 směrovače jsou umístěny vedle svých IPv4 sousedů a jsou s nimi propojeny Fast Ethernetem, především pro potřeby tunelů.

Většina koncových sítí (konkrétně 10 ze 12) je totiž připojena tunelem. Alternativou je mít dvě samostatné linky, pro každý protokol jednu, což přece jen představuje poněkud nákladné řešení. Aby se optimalizovaly datové přenosy, je koncová síť připojena vždy k topologicky nejbližšímu IPv6 směrovači.

Hlavní motivací pro tento oddělený model bylo, aby provoz IPv6 neměl negativní dopad na stabilitu, spolehlivost či výkon základní IPv4 sítě. Toho se jistě podařilo dosáhnout, ovšem zvolené řešení nebude příliš dobře škálovat. Troufnu si předpovědět, že s rostoucím objemem IPv6 provozu a počtem připojených institucí budou Němci nuceni svou koncepci přepracovat.

M.6 GÉANT (evropská páteř)

Na konec jsem si nechal evropskou páteřní síť GÉANT, která propojuje akademické sítě jednotlivých zemí. Do provozu byla uvedena – jak jinak - v roce 2001 a již tehdy se pyšnila jádrem s kapacitou 10 Gbit/s.Plány ohledně IPv6 nejsou nijak ambiciózní. V projektu bylo poskytování IPv6 přislíbeno do listopadu 2004. S jeho praktickou realizací se však začíná právě teď. Stejně jako u většiny zde zmiňovaných sítí vsadili architekti GÉANTu na nativní podporu obou protokolů, čili dual stack.

Příprava na IPv6 si již vyžádala jednu poměrně bolestivou změnu - přechod na jiný směrovací protokol. Do prosince roku 2002 GÉANT používal OSPFv2, který IPv6 nepodporuje. Do provozování dvou směrovacích protokolů se správcům sítě nechtělo, proto se rozhodli přejít na IS-IS. Tento protokol používá (pro IPv4) řada sítí a je tedy dostatečně ověřen. Navíc umožňuje směrovat obě verze protokolu zároveň. Koncem loňského roku proto GÉANT úspěšně přešel na IS-IS.

To však byl teprve první, přípravný krok. K poskytování plnohodnotné IPv6 služby zbývá ještě dost práce – jak technické, tak organizační. Nicméně není důvod se domnívat, že se nepodaří stihnout slíbený listopad 2004. Spíš bych očekával, že GÉANT nabídne IPv6 dříve.

Příloha N 6PE – nenásilné zavedení IPv6 do páteřní sítě

Publikováno v on-line časopisu Lupa 3. 3. 2005

Celá řada páteřních sítí dnes používá technologii MPLS (MultiProtocol Label Switching). Vedle rychlé dopravy paketů nabízí i řadu zajímavých doplňkových služeb, jako jsou virtuální privátní sítě, hrátky s parametry provozu a podobně. Právě na MPLS staví 6PE, jehož cílem je bezbolestně nabídnout podporu IPv6 na stejné úrovni jako IPv4.

Při pohledu do historie jsem zjistil, že článek vysvětlující MPLS na Lupě ještě nevyšel, takže alespoň ve stručnosti tuto technologii představím. V MPLS se rozlišují tři kategorie směrovačů. Vezměme to z vnější strany:

N.1 Customer Edge (CE)

Tímto pojmem bývá označován zákazníkův směrovač, jímž je jeho síť připojena k páteři. Představuje hranici zákaznické sítě a je jediným jejím směrovačem zajímavým (viditelným) z pohledu páteřní sítě. Nejsou na něj kladeny žádné speciální požadavky, s páteří komunikuje celkem běžnými mechanismy. (Což je pochopitelné – nelze chtít po zákaznících, aby měnili své směrovače, když si poskytovatel usmyslí zavést MPLS.)

N.2 Provider Edge (PE)

V PE směrovačích se soustředí valná většina inteligence. Jejich hlavní úlohou je přijímat datagramy přicházející ze zákaznických sítí a podle směrovacích tabulek je opatřovat značkami (MPLS labels). Přeprava MPLS sítí je pak založena právě na těchto značkách. Jinými slovy PE směrovač rozhodne, kam a jak bude datagram přenesen. Jádro pak již jen zajistí svižné splnění úkolu.

N.3 Provider (P)

Nacházejí se v jádru sítě. Bývají poměrně hloupé (mají jen omezený sortiment funkcí), ale velmi rychlé. Přepravují datagramy na základě značek přidělených PE směrovači.

MPLS je postaveno na koncepci „chytrý obal, hloupé jádro“. Valnou většinu rozhodnutí provádějí PE směrovače, jimiž protéká jen omezený objem provozu

(pro zdejší zákazníky) a tudíž nejsou tak zatíženy. Naproti tomu P směrovače v jádru sítě, v nichž se mohou koncentrovat značné datové toky, mají zjednodušenou roli a mohou se soustředit na maximální výkon při předávání datagramů.

N.4 6PE

Cílem 6PE je propojit mezi sebou „IPv6 ostrovy“ (čili zákaznické sítě podporující IPv6) a použít k tomu MPLS páteř, jež sama o sobě nemá o IPv6 ponětí. MPLS je tedy de facto použito v roli spojové vrstvy, která mezi sebou propojí prvky podporující IPv6, aniž by tomuto protokolu sama rozuměla.

Technologie 6PE se soustředí na PE směrovače, což naznačuje jak její název, tak i samotná koncepce MPLS. Základní myšlenkou je, že PE směrovače se navzájem informují o IPv6 sítích (prefixech), jež jsou jejich prostřednictvím dostupné. Když pak PE směrovači dorazí datagram adresovaný některé z nich, prostě jej opatří odpovídající MPLS značkou a předá P směrovačům k doručení zcela obvyklou cestou.

K dosažení tohoto chování musí PE směrovače podporovat jak IPv4, tak IPv6 (dual stack). Navíc musí být schopny se navzájem informovat o připojených IPv6 sítích, k čemuž se ještě vrátím. Příjemnou vlastností je, že PE směrovače jsou jediné, na nichž se nasazení 6PE projeví.

Jádro sítě (P směrovače) zůstává beze změny. Pracuje stejně jako při přepravě IPv4 datagramů. K tomu je ale potřeba, aby MPLS značky používané pro 6PE byly hierarchické. Vyšší vrstva je odvozena z IPv4 adresy cílového PE směrovače a právě ji využívají P směrovače k doručení. Až když datagram dorazí k danému PE směrovači, přijde ke slovu spodní vrstva značky, která jej identifikuje jako přepravovaný pomocí 6PE, a tudíž bude nadále zpracován podle směrovací tabulky pro IPv6.

CE směrovače jsou v rukách zákazníků. Stačí-li jim IPv4, mohou si nechat původní a IPv6 jim jednoduše nebude doručováno. Jestliže o ně ale mají zájem, dohodnou se s poskytovatelem, jakým způsobem si přejí IPv6 dostávat. Mohou mít dva fyzicky oddělené CE směrovače, jeden pro IPv4 a druhý pro IPv6. Může se jednat o jediný stroj, jemuž bude IPv6 dopraveno nativně po stejném připojení jako IPv4, nebo je lze třeba oddělit do virtuálních lokálních sítí na bázi 802.1Q. Zkrátka vše závisí na domluvě mezi zákazníkem a poskytovatelem.

Tím se dostávám k dalšímu kladu 6PE – nemusí být zavedeno naráz. Klidně je možné jednotlivé PE směrovače převádět na 6PE postupně, až když se objeví v daném uzlu zájemce. Investice, které to může způsobit (pokud jsou dotyčné směrovače postarší), tak budou rozloženy v čase.

Ke komunikaci mezi 6PE směrovači byl zvolen protokol MP-iBGP (čili MultiProtokolové Interní BGP), který bylo nutno lehce rozšířit, aby bylo možné

jeho prostřednictvím přenášet informace o IPv6 prefixech a jim odpovídajících MPLS značkách. Z pohledu BGP jsou všichni navzájem svými sousedy, vyměňují si informace o dostupnosti IPv6 prefixů každý s každým. Zde se skrývá jedna potenciální komplikace, protože BGP sousedy je typicky třeba ručně konfigurovat. To může u rozlehlejších sítí správcům hodně znepříjemňovat život. Naštěstí je možné použít route reflectory – několik málo směrovačů, s nimiž ostatní udržují sousedské vztahy a jejichž prostřednictvím předávají své informace všem ostatním. Pak stačí mít v konfiguraci jako sousedy jen reflektory a přidání dalšího 6PE směrovače neznamená zásah do konfigurace všech ostatních.

Přesně toto uspořádání používá od loňského roku pro přepravu IPv6 síť CESNET2. Praktické zkušenosti ukazují, že 6PE je velmi stabilní a z provozního hlediska nezpůsobuje žádné problémy. Prostě funguje a neví se o něm.

Abych však jen nechválil, nelze zamlčovat, že 6PE má i své stinné stránky. Asi nejvýznamnější je, že nedovede přepravovat skupinově adresované datagramy (multicast). Sítě, které jej nepodporují ani pro IPv4, to asi příliš pálit nebude, ale pro CESNET2 je to nedostatek dost citelný.

Druhou nezvyklostí je, že celá MPLS páteř se tváří jako jeden „hop“ – jako by PE směrovače byly navzájem přímo propojeny. To na jedné straně komplikuje život správcům sítě a znesnadňuje vyhledávání problémů. Na druhé straně ale může být chápáno jako bezpečnostní mechanismus, protože skrývá před nezvanými hosty vnitřní strukturu sítě. Vyberte si sami, jestli se vám tato vlastnost spíše líbí, či nikoli.

A konečně posledním negativem je, že 6PE není standardizováno. Firma Cisco Systems, jež je jeho autorem, podnikla svého času pokus v tomto směru. Příslušný draft to dotáhl až do čtvrté verze (draft-ietf-ngtrans-bgp-tunnel-04), ale pak vyšuměl. Ovšem dotyčný mechanismus se dočkal podpory i u konkurentů, například firma Juniper jej ve svých směrovačích nabízí také.

Poskytovatelům Internetu, pokud mají svou páteř založenu na MPLS, se tak nabízí relativně bezbolestná cesta, jak zavést podporu IPv6.

Příloha O 6bone končí: čest jeho památce

Publikováno v on-line časopisu Lupa 18. 5. 2006

6bone je experimentální síť, která deset let umožňovala získávat praktické zkušenosti s provozem protokolu IPv6 a ověřovat jeho implementace či navrhované protokoly a mechanismy. S rozšiřující se podporou IPv6 v běžném Internetu však pominuly důvody pro její existenci. V roce 2004 proto bylo rozhodnuto o jejím ukončení, k němuž dochází právě teď.

Síť 6bone vznikla v roce 1996 s cílem poskytnout především experimentální platformu pro navrhovaný protokol IPv6 a související technologie. Na něm se měla ověřit životaschopnost navrhovaných konceptů, otestovat jejich chování v reálném prostředí a odhalit případné slabiny či komplikace, které v praktickém životě přicházejí.

Když síť 6bone zahajovala svou činnost, bylo IPv6 opravdovým unikátem. Komunikace mezi jednotlivými počítači a koncovými sítěmi procházela běžným Internetem, který v té době podporoval výlučně IPv4. Jako standardní způsob propojení se proto využívaly tunely – virtuální spoje, na jejichž jednom konci byly IPv6 datagramy zabaleny jako datový obsah do IPv4, přeneseny běžnou infrastrukturou a na druhém konci zase vybaleny.

Tunelování provázelo síť 6bone po celou dobu její existence. Přestože později některé spoje přešly do nativního režimu, kdy se data přepravovala přímo protokolem IPv6, tunely zůstaly většinovým řešením. Je to dáno charakterem sítě, do níž se často zapojovala koncová pracoviště zajímající se o IPv6, ovšem připojená k poskytovateli, který tento protokol nepodporuje.

Počítače zapojené do 6bone lze snadno poznat podle adresy, jež začíná prefixem 3ffe::/16. Veškeré 6bone adresy začínají touto skupinou.

Odhaduje se, že svého maxima dosáhla síť v roce 2003, kdy do ní bylo zapojeno kolem 1000 koncových sítí z 50 zemí. Od samého počátku byla síť prezentována jako experimentální a dočasná. To samozřejmě nemusí mnoho znamenat. Podobné ambice (ostatně i technickou realizaci) má například síť Mbone zabývající se distribucí skupinově adresovaných datagramů (multicast). Vzhledem k mizivému pokroku v jeho nasazování do komerčních sítí se její dočasnost zřejmě dost protáhne.

6bone je jiný případ. Po roce 2000 začali registrátoři přidělovat produkční IPv6 adresy s prefixem 2001::/16 a podpora nového protokolu se začala objevovat v běžném Internetu. Řada institucí přešla ze 6bone adres na produkční a odpojila se od 6bone, potřeba existence experimentální sítě začala klesat.

Jako reakce na tento stav vyšlo v březnu 2005 RFC 3701 oznamující postupné ukončení činnosti sítě. Podle něj od 1. ledna 2004 již nebudou přidělovány žádné další adresy z rozsahu 3ffe::/16 a od 6. června 2006 (na návrhu zjevně spolupracoval nějaký cimrmanolog) nebudou adresy s tímto prefixem nadále směrovány. Existence sítě 6bone se tedy uzavře za pár dní.

Přesun zájmu ze 6bone na produkční adresy se velmi dobře odráží i ve směrovacích tabulkách IPv6, jež soustavně sleduje Gert Döring. Na sedmé stránce jeho prezentace z posledního setkání RIPE najdete graf vývoje počtu záznamů v páteřních směrovacích tabulkách. Od roku 2003 je zřetelný setrvalý pokles záznamů ze 6bone prostoru a naopak rychlý nárůst produkčních prefixů. V současných tabulkách je poměr záznamů 3ffe proti 2001 zhruba 1:8.

Názor na to, jak se chovat k adresám s prefixem 3ffe::/16 po 6. červnu, není jednotný. Jedna škola doporučuje striktně zamezit jejich směrování a nasadit na úrovni poskytovatelů Internetu filtry, jež takto adresované datagramy nepropustí. Někteří Stachanovci to dokonce dělají již dnes. Cílem je donutit správce koncových počítačů a sítí opustit tuto část adresního prostoru a přejít na produkční adresy. Významní členové IPv6 skupiny kolem RIPE (např. její vedoucí David Kessens či výše zmiňovaný Gert Döring) se ale vyjádřili proti drsnému postupu. Místo technických prostředků doporučují obrátit se na správce sítí, jež dosud používají 6bone adresy, a pomoci jim se změnou.

V každém případě lze očekávat problémy se směrováním těchto adres, částečně k nim již dochází. Jestliže stále používáte adresy z prostoru 3ffe::/16, je třeba je opustit. Obecně lze formulovat zhruba následující doporučení:

- Nejspíš jste připojeni tunelem k někomu, kdo vám poskytl přístup k IPv6. On má stejný problém. Domluvte se sním, jestli a jak jej bude řešit.
- Porozhlédněte se po domácích poskytovatelích Internetu nabízejících IPv6. Před rokem jsem je mapoval v článku *Jak jsou na tom čeští ISP s IPv6?* Od té doby se jistě něco změnilo k lepšímu, i když k žádnému velkému rozmachu nejspíše nedošlo.
- Rychlé, jednoduché, ale spíše provizorní řešení: využít služeb některého volného tunel serveru. Například Freenet6 poskytuje tunely a adresy z produkčního prostoru.

Síť 6bone svou úlohu splnila a významně přispěla k rozvoji protokolu IPv6. Její úloha nyní končí, ale své místo v historii Internetu má jisté.

Příloha P 6NET

Publikováno v on-line časopisu Lupa 17. 1. 2002

Před koncem roku jsme se na Lupě v článku "IPv6 na sklonku roku" zmiňovali o dvou významných evropských projektech zaměřených na IP verze 6 (6NET a Euro6IX). O prvním z nich jsou nyní k dispozici podrobnější informace, takže se vám jej pokusím přiblížit. Jak již bylo řečeno, je tento projekt značně akademický.

Koordinátorem je firma Cisco Systems, ovšem velmi významnou úlohu mezi účastníky hrají provozovatelé akademických sítí a jednotlivé univerzity. Na řešení projektu se celkem podílí 31 institucí, z toho více než 20 tvoří univerzity, výzkumné instituce a jejich sdružení.

Hlavními cíli projektu jsou:

- postavit a provozovat mezinárodní síť vyhrazenou pro IPv6 a vyhodnotit, zda tento protokol splňuje požadavky pro další rozvoj Internetu
- přispět k tomu, aby Evropa hrála vedoucí roli při vytváření nové generace sítí a jejich služeb

Vedle nich však existuje ještě celá řada cílů vedlejších. Z těch nejvýznamnějších lze jmenovat:

- ověřovat nástroje a postupy pro přechod od IPv4 k IPv6
- sledovat aktuální stav IPv6 z hlediska softwarových a hardwarových produktů
- zkoumat kombinaci pevné a mobilní sítě
- šířit dosažené výsledky na veřejnost

Projekty EU bývají členěny na tak zvané "pracovní balíčky" (workpackage), které vymezují jednotlivé dílčí úkoly a aktivity. Lze z nich poměrně dobře odvodit, co vlastně bude skutečným obsahem projektu. V případě 6NETu si jeho předkladatelé definovali následující balíčky:

1. výstavba a provozování sítě
2. koexistence IPv4 a IPv6 a přechod na nový protokol
3. základní služby sítě (směrování, DNS, bezpečnost sítě)
4. podpora IPv6 aplikací a služeb

5. IPv6 middleware a ověřování uživatelských aplikací v náročném prostředí
6. architektura a nástroje pro správu IPv6 sítě
7. šíření a využití výsledků

Konkrétní návrh sítě a jejího technologického řešení by měl vzniknout během ledna letošního roku. Zatím se předpokládá, že jádrem sítě bude okruh vedoucí ze Skandinávie přes Nizozemí, Německo, Rakousko, Itálii, Švýcarsko, Francii a Velkou Británii zase zpět do Skandinávie. Tento okruh by měl být tvořen nativními IPv6 trasami (žádné tunely) s rychlostí řádově 100 Mb/s. Řecko bude zřejmě - alespoň v první fázi - připojeno tunelem k italskému uzlu páteřního okruhu.

Zmiňované jádro by mělo být uvedeno do provozu do konce prvního čtvrtletí. Přibližně za rok se předpokládá nasazení tras s rychlostí 2,5 Gb/s a transkontinentální napojení sítě (USA, Japonsko). To vše bude používat nativní IPv6.

Zatímco o základní IPv6 služby se budou starat spíše síťové organizace, v oblasti aplikací se otevírá prostor pro zapojené univerzity a komerční firmy. Počítá se s videokonferencemi, přenosy multimediálních dat, elektronickou komercí a jeden z aplikačních podúkolů zahrnuje i on-line hry.

V oblasti šíření svých výsledků nemůže chybět WWW server (ten již běží, ale stále se na něm nic nedozvíte). Vedle něj se však počítá i s různými demonstracemi a dokonce i pořádáním kursů o IPv6.

Projekt je koncipován jako tříletý a limity pro splnění některých dílčích cílů jsou dost tvrdé. Pokud se je podaří dodržet, měly by se dost brzy objevit reálné výsledky.

Česká republika v současné době nemá v 6NETu žádného zástupce. Projekt však bude těsně spolupracovat s dalším evropským projektem GÉANT, do jehož řešení je zapojeno sdružení CESNET. To také v současnosti podniká kroky k tomu, aby se přímo zapojilo i do vlastního 6NETu.

Příloha Q EduRoam: možnost roamingu v akademických počítačových sítích

Publikováno v on-line časopisu Lupa 18. 11. 2004

Už vás někdy napadlo, že by mohl fungovat roaming mezi počítačovými sítěmi? Když přijdete do práce, připojíte se do sítě, a ta vás pustí ke svým zdrojům. Toto by ale mohlo fungovat i v jiné instituci, a to i na mezinárodní úrovni. Na základě autentizace si ověří vaše údaje a rozhodne, zda vás do sítě pustit, či ne. K tomu právě směřuje projekt EduRoam.

Roaming mobilních telefonů dnes považujeme za naprostou samozřejmost. Vyrazíte-li do ciziny, váš mobil se bez nejmenších problémů zahnízdí v tamní síti a vše funguje, jak jste zvyklí (až na výši poplatků). Projekt EduRoam směřuje k dosažení podobného stavu pro mobilní uživatele počítačových sítí, prozatím alespoň těch akademických.

Jeho cílem je, aby se uživatelé mohli přesouvat mezi sítěmi zapojených institucí a připojovali se k nim stejně snadno, jako ke své síti domácí. Pokud možno aby nepoznali žádný rozdíl. Nejvýznamnější komplikaci pochopitelně představuje různorodost techniky, a to jak na straně uživatelů, tak na straně zúčastněných sítí. EduRoam je vyvíjen zejména s ohledem na bezdrátové sítě, ale jeho prostředky by měly fungovat i v sítích drátěných.

Základem celého řešení je autentizace. Do bezdrátové sítě se může připojit kdokoli, kdo jde zrovna s notebookem kolem. Je třeba rozlišit oprávněné uživatele od ostatních, ty první do sítě vpustit, zatímco ty druhé nikoli. To vše má na starosti autentizační a autorizační infrastruktura (AAI).

Její páteří je hierarchie serverů komunikujících protokolem RADIUS. Ke zvýšení bezpečnosti je jejich vzájemná komunikace šifrována prostřednictvím IPsec. Hierarchie má tři úrovně: lokální (servery připojených institucí), národní (centrální server pro naši republiku) a kořenový (pro celou Evropu).

Základní koncepce AAI vychází z toho, že informace o každém uživateli jsou uloženy jen na jednom místě – v jeho domovské instituci. Pokud se připojí mimo ni, postará se AAI o přenos autentizačních informací mezi aktuálním místem připojení a domovským RADIUS serverem a ověří, zda uživatel má oprávnění se připojit či nikoli.

Aby se usnadnilo směrování autentizačních dotazů, mají používaná uživatelská jména tvar uživatel@realm, kde realm odpovídá doméně instituce, z níž dotyčný pochází – například pepa.vomacka@cesnet.cz. Díky tomu se ví, kterou částí hierarchie je třeba projít, a lze snadno najít zodpovědný server.

Vzhledem k různorodosti používaných technologií vypracoval EduRoam pro své potřeby tři alternativní autentizační mechanismy:

802.1x Když se klient připojí do hostitelské sítě, najde porty přístupového zařízení uzavřené, propouštějí jen autentizační protokol EAP. Na klientském počítači musí běžet program (tzv. supplicant), jenž prostřednictvím EAP požádá o autentizaci. Přístupové zařízení se obrátí na lokální RADIUS server, jenž pro lokální uživatele odpoví ze svých zdrojů, pro externí zprostředkuje styk s domácím serverem uživatele. Pokud vše dobře dopadne, přístupový port se otevře a uživatelskému stroji bude umožněna komunikace (případně jej lze zařadit i do určité virtuální sítě, což ovlivní jeho možnosti).

Použití 802.1x je nejlepší variantou. Je bezpečné, efektivní a dává největší možnosti. Vyžaduje ale podporu na straně klientského počítače. Pokud je nelze z nějakého důvodu použít, nabízejí se dvě další varianty.

VPN tunely Při nasazení VPN tunelů se předpokládá, že každá ze zúčastněných sítí bude mít svůj VPN koncentrátor. K němu se mohou připojovat uživatelé odkudkoli z Internetu a prokáží-li totožnost, bude jejich provoz procházet přes koncentrátor a bude s nimi zacházeno jako s plnoprávnými uživateli dotyčné sítě. Hostitelské sítě podle této varianty budou blokovány firewally, jež pro nelokální uživatele povolí provoz pouze na VPN koncentrátory ostatních institucí.

Hostující počítač tedy z hostitelské sítě naváže spojení se svým domácím VPN koncentrátorem a vytvoří si tunel. Veškerá komunikace pak bude procházet tímto tunelem k VPN koncentrátoru a jeho prostřednictvím pak dále do Internetu. Tato alternativa je sice bezpečná, ale neefektivní (veškerý provoz prochází přes domácí instituci hostujícího stroje). V mezinárodním měřítku je to pak zoufale neefektivní.

WWW formulář Nejméně bezpečná, ale naprosto univerzální metoda. I zde je hostitelská síť blokována firewallem, který neumožní nic jiného, než se spojit s vybraným WWW serverem, na němž je k dispozici autentizační formulář. Ten je obsluhován programem napojeným na AAI, a pokud uživatele ověří, odemkne mu připojení – překonfiguruje firewall tak, aby z daného stroje umožnil volnou komunikaci.

Jak už jsem nakousl výše, EduRoam je mezinárodním projektem. Spolupracují na něm sítě národního výzkumu a vzdělávání (NREN) řady evropských zemí. Jejich provozovatelé v dané zemi koordinují připojování zdejších institucí a spravují prostřední úroveň RADIUS hierarchie. Kořenový RADIUS server má na starosti pracovní skupina pro mobilitu při organizaci TERENA.

Z výše uvedeného je zřejmé, že koordinátorem pro Českou republiku je sdružení CESNET. Ostatně bylo vysokými školami a AV ČR založeno právě pro takovéto účely. V Čechách jsou nebo v nejbližší době budou do projektu zapojeny následující instituce (abecedně):

- CESNET
- ČVUT FEL
- UK FAF v Hradci Králové
- TU v Liberci
- VŠB-TU Ostrava
- ZČU v Plzni

Podrobnější a aktuální informace najdete na serveru www.eduroam.cz. Vedle obecných textů jsou tu k dispozici i zcela konkrétní návody pro správce sítí i uživatele – například jak konfigurovat klienty pro jednotlivé systémy a karty.

Příloha R Seznam zkratek

ARP Address Resolution Protocol, protokol ke zjištění linkové adresy pro IPv4 adresu sousedního počítače

ATM Asynchronous Transfer Mode, síťový protokol naplňující vrstvy 1–3 referenčního modelu OSI

BGP Border Gateway Protocol, distribuovaný protokol pro dynamické směrování

CESNET Czech Education and Scientific Network, národní síť pro vědu, výzkum a vzdělávání České republiky; také jméno sdružení síť provozujícího

DNS Domain Name System, distribuovaný systém pro vzájemné převody mezi doménovými jmény a IP adresami

FTP File Transfer Protocol, protokol pro uživatelem řízený přenos souborů v síti Internet

HTTP HyperText Transfer Protocol, přenosový (aplikační) protokol pro službu WWW

IANA Internet Assigned Numbers Authority, organizace zajišťující centrální správu IP adres a identifikátorů

ICMP Internet Control Message Protocol, protokol pro výměnu chybových hlášení a režijních zpráv souvisejících s IP, součást protokolu IP

IETF Internet Engineering Task Force, organizace dobrovolníků vyvíjejících internetové technologie a protokoly

LDAP Lightweight Directory Access Protocol, protokol pro autentizaci uživatelů a poskytování informací o nich

LIANE Liberec Academic Network, síť Technické univerzity v Liberci

LIR Local Internet Registry, organizace zajišťující správu a přidělování adres koncovým sítím

IMAP Internet Message Access Protocol, protokol pro vzdálený přístup ke schránce elektronické pošty

IP Internet Protocol, protokol síťové vrstvy používaný v síti Internet

IPv4 Internet Protocol verze 4, současná verze protokolu

IPv6 Internet Protocol verze 6, nastupující verze protokolu

IPsec Internet Protocol Security, bezpečnostní architektura pro IP

LDAP Lightweight Directory Access Protocol, protokol pro práci s informacemi adresářového charakteru

MAC Medium Access Control, podvrstva linkové vrstvy OSI modelu zajišťující řízení fyzické vrstvy

MPLS Multi-Protocol Label Switching, metoda rychlé přepravy paketů založená na jejich označení v okamžiku vsupu do MPLS sítě

MTU Maximum Transmission Unit, maximální velikost datového paketu, který je schopna přenést najednou technologie druhé vrstvy OSI RM

ND Neighbor Discovery, součást IPv6 zajišťující některé podpůrné úkony (vztah k linkovým adresám, detekce dosažitelnosti a podobně)

NREN National Research and Education Network, páteřní síť propojující výzkumné a vzdělávací instituce v daném státě

OSI RM Open Systems Interconnection Reference Model, obecná architektura síťové komunikace

OSPF Open Shortest Path First, distribuovaný protokol pro dynamické směrování

PKI Public Key Infrastructure, infrastruktura pro důvěryhodnou distribuci veřejných klíčů pro kryptografické algoritmy

QoS Quality of Service, síťové služby s definovanou (zaručenou) kvalitou

RFC Request for Comments, označení pro dokumenty internetové komunity; obsahují mimo jiné definice všech klíčových protokolů Internetu

RIP Routing Information Protocol, distribuovaný protokol pro dynamické směrování

RIPE NCC regionální registrátor (RIR) pro Evropu

RIR Regional Internet Registry, organizace spravující přidělování IP adres v dané oblasti

SSL Secure Sockets Layer, vrstva vložená mezi vrstvy transportní a aplikační zajišťující zabezpečení přenášených dat

STAG informační systém pro evidenci studijní agendy

TCP Transmission Control Protocol, v Internetu nejčastěji používaný protokol transportní vrstvy; zajišťuje spolehlivý přenos dat

URL Uniform Resource Locator, standardní forma pro identifikaci zdrojů v Internetu

VPN Virtual Private Network, virtuální logicky oddělená síť vedoucí společnou síťovou infrastrukturou

WWW World-Wide Web, nejrozšířenější informační služba současného Internetu, hypertextově orientovaná

X.500 skupina standardů přijatých ISO, které se zabývají adresářovými službami

Literatura

[1] Arkko J., Devarapalli V., Dupont F.: *Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents.*
Request for Comments 3776, Internet Engineering Task Force, 2004

[2] Bates T., Chandra R., Katz D., Rekhter Y.: *Multiprotocol Extensions for BGP-4.*
Request for Comments 2283, Internet Engineering Task Force, 1998

[3] Carpenter B., Moore K.: *Connection of IPv6 Domains via IPv4 Clouds.*
Request for Comments 3056, Internet Engineering Task Force, 2001

[4] Coltun R., Ferguson D., Moy J.: *OSPF for IPv6.*
Request for Comments 2740, Internet Engineering Task Force, 1999

[5] Conta A., Deering S.: *Generic Packet Tunneling in IPv6 Specification.*
Request for Comments 2473, Internet Engineering Task Force, 1998

[6] Crawford M., Huitema C.: *DNS Extensions to Support IPv6 Address Aggregation and Renumbering.*
Request for Comments 2874, Internet Engineering Task Force, 2000

[7] Davies J.: *Changes to IPv6 in Windows Vista and Windows Server „Longhorn“.*
Microsoft Corporation, 2006

[8] Deering S., Haberman B., Jinmei T., Nordmark E., Zill B.: *IPv6 Scoped Address Architecture.*
Request for Comments 4007, Internet Engineering Task Force, 2005

[9] Deering S., Hinden R.: *Internet Protocol, Version 6 Specification.*
Request for Comments 1883, Internet Engineering Task Force, 1995

[10] Deering S., Hinden R.: *Internet Protocol, Version 6 Specification.*
Request for Comments 2460, Internet Engineering Task Force, 1998

[11] Deering S., Hinden R.: *IP Version 6 Addressing Architecture.*
Request for Comments 2373, Internet Engineering Task Force, 1998

[12] Droms R., Bound J., Volz B., Lemon T., Perkins C., Carney M.: *Dynamic Host Configuration Protocol for IPv6.*
Request for Comments 3315, Internet Engineering Task Force, 2003

[13] Durand A., Fasano P., Guardini I., Lento D.: *IPv6 Tunnel Broker.*
Request for Comments 3053, Internet Engineering Task Force, 2001

[14] Evans K. S.: *Transition Planning for Internet Protocol Version 6 (IPv6).* memorandum M-05-22, Office of Management and Budget, White House, 2005

[15] Fink R., Hinden R.: *6bone (IPv6 Testing Address Allocation) Phaseout.* Request for Comments 3701, Internet Engineering Task Force, 2004

[16] Hall, E. A.: *Internet Core Protocols.* O'Reilly & Associates, 2000, ISBN 1-56592-572-6

[17] Hinden R., Deering S.: *IP Version 6 Addressing Architecture.* Request for Comments 4291, Internet Engineering Task Force, 2006

[18] Hinden R., Deering S., Nordmark E.: *IPv6 Global Unicast Address Format.* Request for Comments 3587, Internet Engineering Task Force, 2003

[19] Hopps C. E.: *Routing IPv6 with IS-IS.* internet draft draft-ietf-isis-ipv6-06, Internet Engineering Task Force, 2005

[20] IAB, IESG: *IAB/IESG Recommendations on IPv6 Address Allocations to Sites.* Request for Comments 3177, Internet Engineering Task Force, 2001

[21] Johnson D., Perkins C., Arkko J.: *Mobility Support in IPv6.* Request for Comments 3775, Internet Engineering Task Force, 2004

[22] Kent S.: *IP Authentication Header.* Request for Comments 4302, Internet Engineering Task Force, 2005

[23] Kent S.: *IP Encapsulating Security Payload (ESP).* Request for Comments 4303, Internet Engineering Task Force, 2005

[24] Kent S., Seo K.: *Security Architecture for the Internet Protocol.* Request for Comments 4301, Internet Engineering Task Force, 2005

[25] Ladid L.: *IPv6 Forum Roadmap & Vision.* IPv6 Forum, 2006

[26] kolektiv autorů (editor Dunmore M.): *An IPv6 Deployment Guide.* 6NET, 2005, ISBN 1-86220-173-0

[27] kolektiv autorů: *Cisco IOS IPv6 Command Reference.* Cisco Systems, 2006

[28] kolektiv autorů: *EduPerson Object Class Specification.* Internet2, 2006, internet2-mace-dir-eduPerson-200604

[29] kolektiv autorů: *Implementing IPv6 for Cisco IOS Software.* Cisco Systems, 2006

[30] kolektiv autorů: *Vysokorychlostní síť národního výzkumu a její nové aplikace.* zpráva o řešení výzkumného záměru za rok 1999, CESNET z. s. p. o., Praha, 2000, ISBN 80-238-5107-X

[31] kolektiv autorů: *Vysokorychlostní síť národního výzkumu a její nové aplikace.*
zpráva o řešení výzkumného záměru za rok 2000, CESNET z. s. p. o., Praha, 2001, ISBN 80-238-6490-4

[32] kolektiv autorů: *Vysokorychlostní síť národního výzkumu a její nové aplikace.*
zpráva o řešení výzkumného záměru za rok 2001, CESNET z. s. p. o., Praha, 2002, ISBN 80-238-8174-4

[33] kolektiv autorů: *Vysokorychlostní síť národního výzkumu a její nové aplikace.*
zpráva o řešení výzkumného záměru za rok 2002, CESNET z. s. p. o., Praha, 2003, ISBN 80-238-9978-3

[34] kolektiv autorů: *Vysokorychlostní síť národního výzkumu a její nové aplikace.*
zpráva o řešení výzkumného záměru za rok 2003, CESNET z. s. p. o., Praha, 2004, ISBN 80-239-2175-4

[35] kolektiv autorů: *Internet Domain Survey.*
Internet Software Consorcium, 2001, http://www.isc.org/ds/WWW-200101/index.html

[36] Malkin G., Minnear R.: *RIPng for IPv6.*
Request for Comments 2080, Internet Engineering Task Force, 1997

[37] Mockapetris P. V.: *Domain names – concepts and facilities.*
Request for Comments 1034, Internet Engineering Task Force, 1987

[38] Mockapetris P. V.: *Domain names – implementation and specification.*
Request for Comments 1035, Internet Engineering Task Force, 1987

[39] Narten T., Nordmark E., Simpson W.: *Neighbor Discovery for IP Version 6.*
Request for Comments 2461, Internet Engineering Task Force, 1998

[40] Nordmark E.: *Stateless IP/ICMP Translation Algorithm (SIIT).*
Request for Comments 2765, Internet Engineering Task Force, 2000

[41] Pinxteren B. a kol.: *TERENA Compendium of Research and Education Networks in Europe, 2005 Edition.*
TERENA, 2005, ISSN 1569-4496

[42] Rajahalme J., Conta A., Carpenter B., Deering S.: *IPv6 Flow Label Specification.*
Request for Comments 3697, Internet Engineering Task Force, 2004

[43] Rekhter Y., Moskowitz B., Karrenberg D., de Groot K. J., Lear E.: *Address Allocation for Private Internets.*
Request for Comments 1918, Internet Engineering Task Force, 1996

[44] Satrapa P.: *IPv6*.
Neokortex, Praha, 2002, ISBN 80-86330-10-9

[45] Satrapa P.: *IP verze 6 – kam kráčí Internet (možná)*.
v časopise *Softwarové noviny* číslo 1/2002, Praha, 2002, ISSN 1210-8472, str. 88–93

[46] Satrapa P.: *6NET*.
v on-line časopise *Lupa*, Praha, 2002, ISSN 1213-0702
http://www.lupa.cz/clanek.phtml?show=2031

[47] Satrapa P.: *IPv6 – přechodové mechanismy (1)*.
v on-line časopise *Lupa*, Praha, 2002, ISSN 1213-0702
http://www.lupa.cz/clanek.php3?show=2162

[48] Satrapa P.: *IPv6 – přechodové mechanismy (2)*.
v on-line časopise *Lupa*, Praha, 2002, ISSN 1213-0702
http://www.lupa.cz/clanek.php3?show=2192

[49] Satrapa P.: *Změny v přidělování adres*.
v on-line časopise *Lupa*, Praha, 2002, ISSN 1213-0702
http://www.lupa.cz/clanek.php3?show=2270

[50] Satrapa P.: *Jak si stojí IPv6?*
v on-line časopise *Lupa*, Praha, 2001, ISSN 1213-0702
http://www.lupa.cz/clanek.phtml?show=1335

[51] Satrapa P.: *IPv6 na sklonku roku*.
v on-line časopise *Lupa*, Praha, 2001, ISSN 1213-0702
http://www.lupa.cz/clanek.phtml?show=1977

[52] Satrapa P.: *IP verze 6*.
ve sborníku *SLT 2001*, KONVOJ, Brno, 2001, ISBN 80-7302-009-2, str. 181–187

[53] Satrapa P., Adamec P.: *Konfigurace lokální sítě připojené k eduroam.cz*.
technická zpráva CESNET z. s. p. o. číslo 5/2005, Praha, 2005

[54] Satrapa P., Lhotka L.: *CESNET IPv6 Addressing Scheme*.
technická zpráva CESNET z. s. p. o. číslo 3/2001, Praha, 2001

[55] Satrapa P., Novák V., Adamec P.: *IPv6 in CESNET2 Network – 6PE Deployment Experience*.
na konferenci IPv6 Global Summit, Barcelona, 6.–10. 6. 2005

[56] Thomson S., Huitema C.: *DNS Extensions to Support IP version 6*.
Request for Comments 1886, Internet Engineering Task Force, 1995

[57] Thomson S., Huitema C., Ksinant V., Souissi M.: *DNS Extensions to Support IP Version 6*.
Request for Comments 3596, Internet Engineering Task Force, 2003

[58] Tsirtsis G., Srisuresh P.: *Network Address Translation – Protocol Translation (NAT-PT).*
Request for Comments 2766, Internet Engineering Task Force, 2000