

# Mechanismy přechodu na IPv6

Vladimír Kotal

MFF UK

e-mail: vlada@devnull.cz,

WWW home page: <http://techie.devnull.cz/>

## 1 Úvod

Protokol IPv6<sup>1</sup> je nástupce více než 20 let starého<sup>2</sup> protokolu IPv4, který se dnes používá nejen pro přenos dat běžných pro prostředí Internetu (jako je HTTP protokol), ale např. pro IP telefonii, kamerové monitorovací systémy apod.

IPv6 přináší oproti IPv4 zejména větší adresní prostor - zatímco IPv4 adresu lze reprezentovat pomocí 32 bitů, IPv6 adresa má 128 bitů.

Jedním z argumentů pro vývoj nového IP protokolu byl zmenšující se adresní prostor a agre-gace směrovacích informací související s kontinuálním růstem Internetu. Tento problém je řešen např. pomocí mechanismu překladu adres<sup>3</sup>, který používá privátní adresní prostory<sup>4</sup>. Tímto byla sice zažehnána hrozba rapidního úbytku adres, ale za cenu konfiguračních problémů (např. pasivní/aktivní FTP) a hlavně zpronevěření se původní filosofii Internetu - každý by měl mít možnost komunikovat s každým. To se dnes nemusí jevit jako překážka, nicméně to může představovat netriviální problémy pro sítě typu HAN<sup>5</sup> nebo pro PDA a jiná mobilní zařízení s přístupem do Internetu.

Tento článek má za cíl podat základní přehled mechanismů pro přechod na IPv6. Nejprve podám přehled pozitiv IPv6 a překážek přechodu, pak rozeberu vybrané techniky a nakonec načrtnu strategie přechodu na určitých typech sítí. Tyto strategie budou využívat techniky z první části článku.

### 1.1 Výhody IPv6

- velký adresní prostor  
Adresní prostor IPv6<sup>6</sup> je zhruba o 30 řádů větší<sup>7</sup> než adresní prostor IPv4.
- podpora pro směrování v hardware  
Velikost základní IPv6 hlavičky je fixní - 40 bajtů. Toto umožňuje jednodušší implementaci hardwarového směrování<sup>8</sup>.
- povinná implementace bezpečnostních prvků  
Povinná implementace IPsec stacku je důležitá pro stále rozšířenější používání VPN připojení a dále je nutná pro podporu mobility.
- podpora pro *QoS - Quality Of Service*
- škálovatelnost
- adresní schema zajišťující lepší agregaci směrovacích informací
- podpora mobility

<sup>1</sup> Internet Protokol verze 6

<sup>2</sup> RFC Internet Protocol v rámci programu DARPA je ze září 1981

<sup>3</sup> NAT - Network Address Translation, RFC 1631

<sup>4</sup> dle RFC 1918

<sup>5</sup> Home Area Network - síť spotřebičů v domácnosti, ke kterým chceme přistupovat odkudkoliv

<sup>6</sup> IPv6 adresa je většinou reprezentována včetně počtu bitů sítě (podobně jako koncept CIDR v IPv4).

Takové adrese (např. `3ffe:80ef:101::/64`) se říká *prefix*

<sup>7</sup> což vede ke spekulativním výpočtům, že na čtvereční palec zemského povrchu připadá cca  $4.3 \cdot 10^{20}$  unikátních IPv6 adres

<sup>8</sup> jak dokládá např. projekt Liberouter - <http://www.liberouter.org>

## 1.2 Překážky migraci

Než přejdu k jednotlivým přechodovým mechanismům, pokusím se nejprve analyzovat hlavní překážky pro migraci na IPv6. Tyto překážky lze rozdělit z hlediska uživatele a z hlediska poskytovatele.

**Pro uživatele** jsou podstatné následující:

- nejasnosti v preferencích odpovědí na DNS dotazy v rámci aplikací  
Dosud není uspokojivě vyřešeno, zda mají aplikace (nebo *resolver* knihovna daného OS) preferovat IPv4 nebo IPv6, případně za jakých podmínek.
- nedostatek obsahu / žádná "killer app"  
Neexistuje žádná výrazná aplikace, která by uživatele vědomě donutila zajímat se o přechod na nový protokol. Peer-to-peer sítě, pro které by IPv6 byl vhodným protokolem, si dnes většinou poradí s překladem adres celkem dobře. Stejně tak IPv6 sítě neobsahují dostatek obsahu, který by přilákal uživatele.

**Z hlediska poskytovatele** jsou to především:

- neexistence/nedokonalost technických řešení  
Nejsou např. prostředky pro účtování<sup>9</sup> (*billing*), routery a switche neumí pracovat s IPv6 v hardware, nejsou dokončeny implementace některých prvků protokolu.
- obavy z možných útoků na implementaci IPv6  
V implementacích TCP/IP stacku pro IPv4 se objeví čas od času triviální chyby<sup>10</sup>. Komplexnost IPv6 vede mnohé poskytovatele k názoru, že chyb v implementacích IPv6 bude více. Prozatím se jich vyskytlo jen minimálně<sup>11</sup>. Pro lepší stav v tomto smyslu je zapotřebí nástrojů pro testování IPv6 implementací.
- 6bone *phase-out* neboli postupné vyřazování z činnosti<sup>12</sup>  
6bone je experimentální globální IPv6 síť, která slouží pro testování IPv6 protokolu. Od 1. ledna 2004 se již nepřidělují 6bone prefixy nejvyšší úrovně<sup>13</sup> a k 6.6.2006 má 6bone ukončit svoji činnost úplně. Separace produkčních IPv6 sítí od 6bone nadále probíhá, přičemž mnoho obsahu leží stále v 6bone.
- cena za migraci
  - Ve velkých společnostech (tzv. *enterprises*) by měl být pro migraci vytvořen tým - to znamená vyčlenit čas několika pracovníků a tedy z pohledu zisků snížit jejich výkonnost.
  - Zanedbatelná nemusí být ani cena za technické provedení - např. v případě, kdy se z databáze generují konfigurační soubory nebo jsou v ní uloženy data pro billing svázaná s bloky IP adres. Modifikace databáze a všech navazujících služeb může představovat možství práce, nehledě na nutnost rozšířit a aplikovat bezpečnostní politiku na IPv4 i IPv6 síť.
- "negeneruje to peníze"  
Pro poskytovatele připojení je jedním z argumentů proč nepřejít na IPv6 rentabilita služeb. Místo technického řešení přechodu na IPv6 překonávají poskytovatelé nedostatek adres pomocí překladu adres. Pevné IP adresy jsou dnes dokonce u některých typů připojení zpoplatňovány. Tento postoj se může proti poskytovatelům obrátit, protože ve chvíli, kdy přestane být IPv6 konkurenční výhodou, začne poskytovatel díky neschopnosti poskytnout IPv6 připojení ztrácet zisky.
- propojení a komunikace s dalšími poskytovateli IPv6 konektivity  
Veřejná fóra pro komunikaci odborné veřejnosti<sup>14</sup> jsou sice k dispozici, ale v současné době jsou "zticha".

<sup>9</sup> ať už založené na Cisco Netflow nebo radius protokolu

<sup>10</sup> např. v nedávné době útoky založené na špatném vyhodnocení TCP paketu s flagem RST - viz. [5]

<sup>11</sup> např. CVE (Common Vulnerabilities and Exposures) candidate CAN-2004-0370

<sup>12</sup> specifikované v RFC 3701

<sup>13</sup> tzv. pTLA prefixy podle (zastaralého) RFC 2374 - `3ffe::/24-28`

<sup>14</sup> u nás např. mailová konference na `ipv6.cz`

Tyto překážky tvoří jakýsi bludný kruh - dokud nebude uživatel motivován k přechodu, nebude tlačit na poskytovatele, aby mu zajistil technické řešení a naopak - dokud poskytovatel nezajistí technické řešení, nebude mít uživatel motivaci přejít.

### 1.3 Současný stav

**Stav protokolu IPv6** je ve stabilnější fázi, i když se občas objeví méně očekávaná změna<sup>15</sup>. Návrhová aktivita se přesouvá pomalu mezi pracovními skupinami IETF<sup>16</sup>, které se zabývají IPv6 - od *ipv6* k *v6ops*.

**Stav operačních systémů** je uspokojivý, nepoužívanější operační systémy nabízejí aspoň základní implementaci IPv6, překladové mechanismy jsou implementovány zatím málo nebo v nedostačující podobě.

## 2 Technické prostředky pro migraci

### 2.1 Migrace z hlediska vrstev ISO/OSI

Řešení navázání IPv6 na jednotlivé linkové technologie s sebou nese několik zajímavých konceptů, nicméně v zásadě se jedná o oblast, ve které se pravděpodobně nebudou z hlediska návrhu dít velké změny. Z hlediska implementačního je to věc jiná, např. dosud nedošlo<sup>17</sup> k implementaci IPV6CP protokolu v rámci protokolu PPP v OS Windows, což by umožnilo nativní ipv6 dial-up i ve Windows.

Rozbor migrace na IPv6 z hlediska nižších vrstev ISO/OSI je mimo rozsah tohoto článku.

### 2.2 Tunelovací mechanismy

Tunely slouží k přenosu IPv6 paketů uvnitř paketů jiného protokolu - buď na stejné nebo vyšší vrstvě ISO/OSI. Tunely mohou být buďto automatické nebo statické. Automatické tunely jsou vytvářeny ad hoc, statické jsou nakonfigurovány mezi dvěma uzly "napevno".

Tunely jsou používány všude, kde není možné nativní IPv6 připojení - to může být způsobeno např. tím, že operační systém přístupového bodu neobsahuje implementaci IPv6 nebo daná organizace nedisponuje IPv6 připojením.

**Statické tunely** slouží pro přenos IPv6 paketů uvnitř IPv4 paketů - základní IPv6 hlavička následuje hned za IPv4 hlavičkou. Každá strana má přiřazenou veřejnou IPv4 adresu<sup>18</sup>. Na "klientské" straně tunelu je nastaveno směrování veřejných IPv6 adres do tunelu, na straně poskytovatele je do tunelu nastaveno směrování klientského IPv6 prefixu.

Tyto tunely se používají tam, kde je potřeba překonat IPv4 síť a kde zpravidla druhý konec tunelu končí v IPv6 síti s dobrou konektivitou.

**6to4** je přechodový mechanismus<sup>19</sup> založený na automatickém tunelování IPv6 paketů uvnitř IPv4 paketů. 6to4 slouží k propojení IPv6 sítí/ostrovů prostřednictvím IPv4 sítě.

6to4 rozlišuje následující entity:

- *6to4 router* - hraniční router mezi IPv6 sítí a globálním IPv4 Internetem. Tento typ routeru slouží pro komunikaci v rámci 6to4 sítě.

<sup>15</sup> např. stažení *site-local* adres - draft-ietf-ipv6-deprecate-site-local03.txt

<sup>16</sup> The Internet Engineering Task Force - komunita produkující mj. návrhy a RFC dokumenty

<sup>17</sup> a nedojde až do verze Longhorn - dle Leigh Huanga, program managera Microsoftu pro IPv6

<sup>18</sup> a někdy pro účely testování a identifikace tunelu i /64 IPv6 prefix

<sup>19</sup> specifikovaný v RFC 3056

- *6to4 relay router* - 6to4 router nakonfigurovaný pro směrování mezi 6to4 uzly a nativními IPv6 uzly. Tento typ routeru slouží pro komunikaci v rámci 6to4 sítě a mezi 6to4 sítí a globálním IPv6 Internetem.
- *6to4 klient* - IPv6 uzel používající služeb 6to4 (relay) routeru

Pro 6to4 byl vyhrazen<sup>20</sup> prefix 2002::/16. Prvních 16 bitů je tedy fixních, dalších 32 je vyhrazeno pro reprezentaci IPv4 adresy 6to4 routeru. Zbýlých 80 bitů může být využito na podsítě pro uzly za danou 6to4 gatewayí. Např. 2002:c058:6301::/48 je prefix pro síť, kde 6to4 router má adresu 192.88.99.1<sup>21</sup>.

Uzly v IPv6 síti za 6to4 routerem používají 6to4 prefix zkonstruovaný podle veřejné IPv4 adresy 6to4 routeru.

Prostřednictvím tohoto routeru se dostanou k ostatním 6to4 klientům. Pokud 6to4 routeru přijde IPv6 paket s cílovou adresou z jiného 6to4 prefixu, IPv6 paket zabalí do IPv4 paketu se zdrojovou adresou ze svého 6to4 interface a cílovou adresou, kterou přečetl z 6to4 prefixu IPv6 a pošle do IPv4 sítě.

Aby se 6to4 klienti dostali do celého IPv6 Internetu, musí použít služby 6to4 relay routeru.

Zde je potřeba rozlišit dvě varianty komunikace:

1. Pokud chce komunikovat nativní IPv6 uzel s 6to4 klientem, pošle jednoduše paket na jeho adresu. Směrování v IPv6 síti zajistí, že se paket dostane ke správnému 6to4 relay routeru<sup>22</sup>.
2. Pokud posílá 6to4 klient paket nativnímu IPv6 uzlu, měl by jej 6to4 router směřovat na nejbližší 6to4 relay router.

Dříve musel být udržován seznam 6to4 routerů ručně (viz. [4]), dnes se využívá anycastového směrování<sup>23</sup>. 192.88.99.0/24 je prefix, který slouží jako anycastový prefix pro veřejné 6to4 relay routery. 6to4 klienti si tedy mohou nastavit adresu 192.88.99.1 jako svůj 6to4 router a díky anycastovému směrování budou používat ten 6to4 (relay) router, který je k nim z hlediska topologie nejbližší.

6to4 router musí mít aspoň jednu veřejnou IPv4 adresu, nejlépe statickou. Běžně je 6to4 implementován jako síťové rozhraní, které je nakonfigurováno na hraničním směrovači. V systémech typu BSD je takové rozhraní nazýváno `stf` ("Six To Four") nebo podobně. Toto rozhraní je nutné nakonfigurovat pouze na 6to4 routeru.

Hlavními výhodami 6to4 jsou schopnost jednoduše propojit IPv6 sítě pomocí existující IPv4 infrastruktury, jednoduchost použití a dostupnost na nejrozšířenějších operačních systémech (viz. tabulka č. 2).

**Teredo** je jeden ze složitějších protokolů pro přiřazení IPv6 adres a transport IPv6 paketů přes IPv4 síť ([3]). Byl navržen za účelem "překračování" překladu adres - NAT<sup>24</sup>, čehož dosahuje pomocí tunelování IPv6 paketů. V tomto případě jsou IPv6 pakety zabaleny do UDP paketů. Základní IPv6 hlavička následuje hned za UDP hlavičkou.

Složitost Tereda spočívá v množství jeho komponent, a dále v požadavku na univerzálnost použití. Tvůrci tohoto protokolu v článku [3] zdůrazňují, že Teredo je nutné brát jako protokol, k jehož použití lze sáhnout až v případě, kdy nelze použít žádné jiné řešení. (porovnání s jinými protokoly viz. tabulka č. 1)

Mechanismy překladu adres se rozdělují do několika typů, podle toho, jak mapují interní IP adresy a čísla portů na externí IP adresu a port na tzv. *restricted*, *cone* a *symmetric*. Poslední typ překladu (interní adresa a port se mohou mapovat pro různé cílové adresy různě) znemožňuje provoz Tereda.

Teredo používá následující komponenty:

<sup>20</sup> organizací IANA, která se stará o "rozdělování" adresních prostorů na nejvyšší úrovni

<sup>21</sup> c058:6301 je hexadecimální zápis 192.88.99.1

<sup>22</sup> každý 6to4 relay router propaguje via externí routovací protokol svůj 6to4 prefix

<sup>23</sup> dle RFC 3068

<sup>24</sup> je to prakticky jediný protokol pro *NAT traversal* implementovaný ve více operačních systémech

- Teredo klienty
- Teredo servery
- Teredo relaye
- Teredo host-specific relaye

Teredo klient<sup>25</sup> je uzel, který obsahuje podporu pro tunelovací rozhraní pro Teredo protokol. Teredo server přiřazuje klientům IPv6 prefixy a zajišťuje jejich připojení do IPv6 Internetu. Teredo server dále zajišťuje inicializaci komunikaci mezi dvěma Teredo klienty nebo Teredo klienty a nativně připojenými IPv6 uzly.

Teredo se hodí všude, kde router, za který je dané zařízení připojeno, neumožňuje tunelování IPv6 paketů nebo tam, kde je zařízení umístěno za jednou nebo několika úrovněmi překladu adres. Teredo server lze umístit na okraj takové sítě nebo úplně mimo tuto síť.

Teredo klient je schopen detekovat, za jakým typem překladu adres se nachází. Podle toho pak vypadá komunikace s *Teredo serverem* nebo *host-specific relay*. Protokol dále musí řešit různé varianty komunikace - především oboustrannou komunikaci mezi Teredo klientem a nativním IPv6 uzlem. Průběh specifického případu takové komunikace je na obr. č. 1.

Struktura adres přiřazených klientům se skládá z

- Teredo prefixu - `3ffe:831f::/32`. Tento je společný pro všechny klienty.
- IPv4 adresy Teredo serveru
- pole příznaků
- změněného externího portu
- změněné externí adresy

Externí adresa a port vznikly při překladu adresy klienta. V adrese se vyskytuje jejich reprezentace změněná bitovou operací XOR, aby nemohlo dojít k situaci, kdy je překlad adres změněn<sup>26</sup>.

Teredo servery a relaye mají nastaveno směrování IPv6 paketů s Teredo prefixem do Teredo rozhraní, implicitní směrování IPv6 paketů<sup>27</sup> je nastaveno do IPv6 Internetu. Teredo server musí mít dále přiřazeny dvě veřejné IPv4 adresy.

Teredo klienti při směrování rozlišují, zda cílová adresa patří

- Teredo klientu ve stejné IPv4 síti
- Teredo klientu v jiné síti
- uzlu v IPv6 Internetu

Pro udržování stavu mezi Teredo klientem a Teredo serverem v překladové tabulce se používají tzv. *bubble pakety*, což jsou IPv4 UDP pakety, které obsahují pouze IPv6 hlavičku a žádná data. Tyto pakety se používají rovněž ke zjišťování sousedů ve stejné IPv4 síti.

**ISATAP** neboli *Intra-Site Automatic Tunnel Addressing Protocol* slouží k propojení IPv6 uzlů/routerů přes IPv4 síť. Z jeho pohledu slouží IPv4 jako linková vrstva pro IPv6. ISATAP podporuje automatické tunelování.

ISATAP je protokol navržený pro použití uvnitř sítí typu "enterprise" - to jsou takové sítě, které mohou zahrnovat několik oddělení s různou bezpečnostní politikou a mohou mít několik připojení ke globálnímu Internetu, ale s jednotnými zájmy. Toto je typicky prostředí korporátních a akademických sítí.

Identifikátor síťového rozhraní pro použití s ISATAP je modifikovaný formát EUI-64.<sup>28</sup> ISATAP počítá pouze s tím, že IPv4 síť, nad kterou běží disponuje pouze unicastovým směrováním.

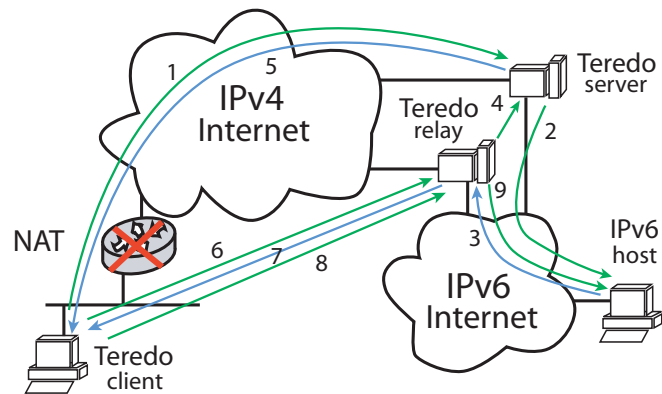
Scénář použití ISATAP protokolu se skládá ze zavedení několika ISATAP routerů, každý s přístupem do IPv4 sítě dané organizace a připojením do IPv6 Internetu. Klienti pak využívají autokonfiguraci.

<sup>25</sup> dále jen klient

<sup>26</sup> To se může stát v případě, kdy se v rámci překladu adres prohledává datová část paketu a řetězec odpovídající adrese nebo portu je nahrazen něčím jiným

<sup>27</sup> tzv. default route - `::/0`

<sup>28</sup> EUI-64 je definovaný organizací IEEE a použitý např. v RFC 2464



**Obrázek 1.** Teredo klient posílá paket uzlu v IPv6 síti ze sítě s restricted NAT. Nejprve zjistí IPv4 adresu Teredo relaye nejbližší k IPv6 uzlu via Teredo server (pomocí ICMPv6 echo request paketu) a pak přes tuto Teredo relay pošle IPv6 paket.

Návrh protokolu ISATAP je sice relativně nový (2002), ale má "pohnutou" historii:

Poté co byl tento protokol implementován<sup>29</sup> v operačních systémech Cisco IOS, Linux, Windows XP a KAME<sup>30</sup> SNAP kitu, bylo vzneseno prohlášení o držení patentových práv na tento protokol.

Podle IPR (Intellectual Property Rights) vydaného v r. 2003 patří patent firmě SRI (viz. [6]). Sdružení KAME po vydání IPR stáhlo implementaci ISATAP ze své distribuce. Firma SRI na dotazy KAME neodpovídá. Autor původního návrhu protokolu už ve firmě SRI nepracuje, nemůže být tedy nápomocen.

ISATAP zůstal pouze jako draft (vyprší v 11/2004), zatím se nedočkal podoby RFC.

Pokud vezmeme v úvahu všechny výše uvedené informace, dalo by se říci, že se ISATAP pravděpodobně příliš nerozšíří.

**Tunnel brokers** jsou provozovatelé služby, která nabízí (zpravidla zdarma) nastavení statických tunelů nesoucích IPv6 pakety zabalené v IPv4 paketech.

Nevýhodou tohoto typu připojení je zpravidla vysoká latence a nestabilita tunelu. To je většinou dáno tím, že provozovatel této služby je připojen do sítě 6bone - experimentální síť pro IPv6<sup>31</sup> a tunel "končí" daleko (v topologickém slova smyslu) od klienta.

Tento typ připojení se hodí zejména tam, kde poskytovatel IPv4 připojení nenabízí nativní<sup>32</sup> IPv6 služby. Bohužel, často je takové prostředí právě za překladem adres, s kterým si statické tunely nedokáží poradit.

Pozadí těchto služeb spočívá v databázi, kde jsou uloženy informace o delegaci IPv6 klientských prefixů a koncích tunelů. Tyto údaje může uživatel modifikovat pomocí webového formuláře.

Projekt XS26<sup>33</sup> je jedním z tunnel brokerů, nicméně s jiným přístupem - vstupní brány<sup>34</sup> do IPv6 Internetu jsou rozptýleny a tvoří distribuovaný systém. (viz. obr. 2) V tomto systému se propagují směrovací informace pro klientské prefixy a nastavení jejich tunelů. XS26 používá pro distribuci směrovacích informací protokoly OSPFv6 a BGP4+, pro distribuci dat o tunelech je použit proprietární protokol. Toto zajišťuje částečnou redundanci - pokud vypadne konektivita

<sup>29</sup> dle draftu pracovní skupiny *ngtrans*, který je v současné době ve verzi *draft-ietf-ngtrans-isatap-22*

<sup>30</sup> KAME je seskupení šesti japonských společností vytvořené za účelem poskytnutí svobodné IPv6 implementace pro systémy typu BSD

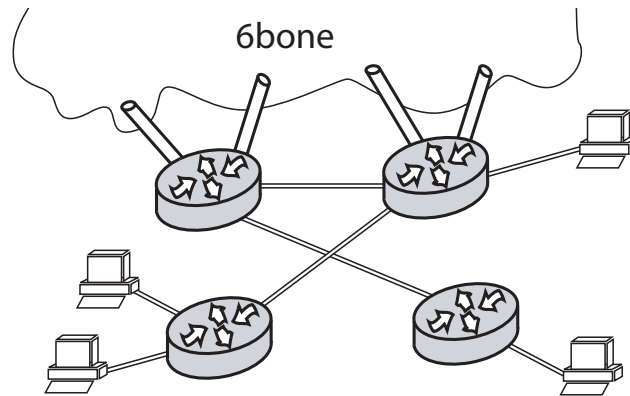
<sup>31</sup> tato síť končí svůj "provoz" v roce 2006

<sup>32</sup> to je takové připojení, kdy IPv6 paket není zabalen do paketu 3. úrovně modelu ISO/OSI

<sup>33</sup> Access to IPv6 project - <http://www.xs26.net>

<sup>34</sup> tzv. POPs - Points of Presence neboli "místa přítomnosti", každý POP je zpravidla umístěn v jiném státě; v současné době jsou v České republice dva POPy. (z celkového počtu 9)

některého z POPů, směrování se upraví tak, aby byla IPv6 konektivita zachována. Uživatel si dále může zvolit, ke kterému z POPů bude připojen, čímž může částečně ovlivňovat latenci svého tunelu.



**Obrázek 2.** Model sítě distribuovaného systému tunnel brokera (XS26 network). Tlusté "trubky" znázorňují tunelované BGP4+ sessions mezi routery XS26 sítě a dalšími poskytovateli v 6bone. Slabší "trubky" znázorňují klientské tunely nebo tunely pro internal BGP/OSPF6 mezi XS26 routery.

### 2.3 Překladové mechanismy

Na úroveň tunelovacích protokolů lze postavit překladové mechanismy, které převádějí IPv6 pakety na IPv4 a zpět. Tento úkol je sice z pohledu 3. vrstvy ISO/OSI celkem jednoduchý, je třeba si nicméně uvědomit, že adresy mohou být obsaženy v datové části paketů, kde už převod závisí na konkrétním aplikačním protokolu<sup>35</sup>.

Z překladových mechanismů uvedu pouze NAT-PT, existuje ještě množství dalších, např. SIIT(RFC 2765), BIS (RFC 2767), Transport relay (RFC 3142), SOCKS64 (RFC 3089), BIA (RFC 3338), DSTM (IETF draft).

**NAT-PT** je mechanismus navržený<sup>36</sup> pro jednu z posledních fází přechodu na IPv6, kdy budou nově připojené sítě disponovat pouze IPv6 adresami a bude třeba vyřešit problém komunikace se zbytky IPv4 sítě.

NAT-PT je implementován na routeru, který "sedí" mezi sítí s IPv6 uzly a IPv4 sítí.

NAT-PT pracuje podobně jako překlad IPv4 adres, pouze na jedné straně překladového mechanismu jsou IPv6 adresy a na druhé IPv4 adresy. NAT-PT tedy překládá IPv6 adresy na IPv4 a vice versa.

Existují následující typy NAT-PT:

- statický NAT-PT  
Mapuje jednu IPv6 adresu na jednu IPv4 adresu. Hodí se v případě, kdy IPv6 server potřebuje přistupovat k pevné množině IPv4 adres, např. pro dotazy na IPv4 DNS servery.
- dynamický NAT-PT  
Překladový mechanismus udržuje stavovou tabulku spojení a pro každé nové spojení použije adresu z daného rozsahu.

<sup>35</sup> v rámci IETF (The Internet Engineering Task Force) existuje skupina *vbops*, která se mj. zabývá popisem používaných standardů z hlediska IPv4 adres

<sup>36</sup> NAT-PT je specifikovaný v RFC 2766 a RFC 2765

- *Port Address Translation (PAT)* neboli *Overload*

Spojení z různých IPv6 adres se mohou že mapovat na jednu IPv4 adresu s různými porty.

Na vnitřním (IPv6) rozhraní NAT-PT routeru je přiřazen /96 IPv6 prefix, který slouží IPv6 uzlům pro identifikaci IPv4 uzlů. Při posílání paketu z IPv6 sítě do IPv4 sítě je IPv4 adresa "přilepena" za tento prefix. V případě, že bude třeba zprostředkovat komunikaci iniciovanou IPv4 uzly do IPv6 sítě, je třeba propojit DNS server pro IPv6 síť s NAT-PT routerem, který bude podle DNS dotazů manipulovat se stavovou tabulkou pro překlad.

Výhodou NAT-PT je transparentnost. Uzly používající NAT-PT nevyžadují žádnou změnu konfigurace.

NAT-PT by neměl být použit pro komunikaci *dual-stack uzlů*<sup>37</sup> s uzly, které mají pouze IPv6 nebo IPv4 konektivitu.

Záleží na implementaci NAT-PT, do jaké míry poskytuje překlad na aplikační úrovni<sup>38</sup>. Běžně jsou podporovány protokoly FTP a DNS.

## 2.4 Souhrn přechodových mechanismů

Každý přechodový mechanismus je vhodný pro jiný typ sítě, má jiné výhody a nevýhody. Tabulky č. 1 a 2 přinášejí srovnání několika vybraných mechanismů z hlediska některých jejich vlastností a současného stavu implementace.

Protokol	NAT tr.	Režie	adr. tunelu
Teredo	Ano	Velká	explicitně
6to4	Ne	Střední	IPv6 prefix
ISATAP	Ne	Střední	IPv6 intfc ID
Statické tunely	Ne	Nízká	explicitně

**Tabulka 1.** Porovnání tunelovacích mechanismů z hlediska jejich vlastností a možností aplikace.

OS	Statické	Teredo	6to4	ISATAP	NAT-PT
Linux	Ano	Ano	Ano	Ano	Ano
BSD	Ano	FreeBSD	Ano	Ne	Ano
Windows XP	Ano	Ano	Ano	Ano	Ne
Cisco IOS	Ano	Ne	Ano	Ano	Ano
Apple OS X	Ano	Ne	Ano	Ne	Ne

**Tabulka 2.** Stav Implementací jednotlivých tunelovacích mechanismů v nejrozšířenějších operačních systémech.

## 3 Migrační strategie

Množství přechodových mechanismů dává rozmanité varianty přechodu. Podle typu organizace a sítě je možné zvolit strategii přechodu při použití určitých mechanismů.

### 3.1 Enterprise

*Enterprise* je organizace, která provozuje velkou síť, na které závisí *mission critical* služby. U takové organizace se dá předpokládat, že přechod na IPv6 bude probíhat ve fázích, přičemž některé IPv4 sítě budou muset být provozovány ještě několik let poté, co většina sítě přešla na IPv6.

Pro komunikaci mezi *legacy* IPv4 sítěmi a zbytkem organizace je pak možné úspěšně použít NAT-PT, případně jiné překladové mechanismy.

<sup>37</sup> tj. uzlů připojených do IPv4 i IPv6 Internetu

<sup>38</sup> Tuto službu zajišťují tzv. *Application Layer Gateway*

### 3.2 ISP - Internet Service Provider

Větší poskytovatelé budou muset řešit při přechodu hned několik problémů - přechod samotné síťové infrastruktury, změny informačního systému, bezpečnostní politiky a přechod na aplikační úrovni.

Podstatné při plánování přechodu je zejména vytvoření adresovacího schématu budoucí IPv6 sítě.

Ke slovu se v první fázi přechodu<sup>39</sup> dostanou zřejmě hlavně tunelovací mechanismy<sup>40</sup>; do jaké míry, to závisí na rychlosti a ochotě k přechodu.

### 3.3 Small network

Pro malou síť s několika pracovními stanicemi a jedním místem připojení do IPv4 Internetu přichází v úvahu v podstatě řešení první fáze přechodu na bázi tunelu. (v případě, že poskytovatel připojení nenabízí nativní IPv6 připojení)

Vhodné jsou zejména statické tunely s nízkou latencí (nejlépe od poskytovatele IPv4 konektivity) nebo 6to4.

## 4 Závěr

Výběr strategie a přechodových mechanismů závisí na několika faktorech - velikosti organizace, plánované rychlosti přechodu, dostupnosti implementací zvolených přechodových mechanismů, apod.

Zároveň je potřeba vytvořit adresovací schema pro IPv6 síť tak, aby odpovídalo potřebám dané organizace na dlouhou dobu dopředu a zároveň bylo v případě potřeby flexibilní.

O tom už bude řeč ale někde jinde.

## Reference

1. Cisco systems. *IPv6 deployment strategies*, 2001
2. Pavel Satrapa. *IPv6*, edice CESNET, 2002
3. Davies, Huitema, Tansley, Talwar, Thaler. *Teredo Overview*, Microsoft Corporation, 2003-2004
4. Nick Sayer, Public 6to4 relay routers, <http://www.kfu.com/~nsayer/6to4/>, 2004
5. TCP with large windows RST attack, CAN-2004-0230, 2004
6. SRI International's statement about IPR claimed in <draft-ietf-ngtrans-isatap-13.txt>, 2003

<sup>39</sup> kdy "rozsah" IPv4 Internetu je daleko větší než IPv6 Internetu

<sup>40</sup> pro určité segmenty zákazníků může být nutné použít Teredo