

Pavel Satrapa

Internetový  
protokol  
verze 6

Třetí  
vydání

# IPv6

Edice CZ.NIC

Pavel Satrapa

## **INTERNETOVÝ PROTOKOL VERZE 6**

Třetí, aktualizované a doplněné vydání

Vydavatel:  
CZ.NIC, z. s. p. o.  
Americká 23, 120 00 Praha 2  
<http://www.nic.cz/>



Vydání této publikace podpořil  
CESNET, z. s. p. o.  
Žitná 4, 160 00 Praha 6  
<http://www.cesnet.cz/>



3. vydání, Praha 2011  
Kniha vyšla jako 1. publikace v Edici CZ.NIC.  
ISBN 978-80-904248-4-5

© 2002, 2008, 2011 Pavel Satrapa

Toto autorské dílo může být kýmkoliv volně šířeno a překládáno v písemné či elektronické formě, na území kteréhokoliv státu, a to za předpokladu, že nedojde ke změně díla a že zůstane zachováno označení autora díla a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o.

Pavel Satrapa

**Internetový  
protokol  
verze 6**

Třetí  
vydání

# IPv6

Edice CZ.NIC

<http://knihy.nic.cz/>

Toto autorské dílo může být kýmkoliv volně šířeno a překládáno v písemné či elektronické formě, na území kteréhokoliv státu, a to za předpokladu, že nedojde ke změně díla a že zůstane zachováno označení autora díla a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o.

Pokud není výslovně uvedeno jinak, jsou všechny domény a IP adresy v této knize smyšlené. Jakákoli podobnost se skutečnými IP adresami či doménovými jmény je čistě náhodná.

Unix je zapsaná ochranná známka X/Open Company Ltd.  
Microsoft a Microsoft Windows jsou zapsané ochranné známky Microsoft Corporation.  
Názvy ostatních produktů a firem mohou být ochrannými známkami nebo registrovanými ochrannými známkami příslušných vlastníků.

## Předmluva vydavatele

Vážení čtenáři,

téma této knihy, tedy protokol IPv6, je v současnosti mnohem více aktuální, než v dobách jejího prvního či druhého vydání. V této době již správci současného Internetu bojují s nedostatkem adres protokolu IPv4, vymýšlejí různé technické triky, jak si s tímto stavem poradit, a vesměs doufají, že masivní zavádění protokolu IPv6 už konečně začne. Vzhledem k tomu, že žádný plán B neexistuje, čeká spoustu správců po celém světě a samozřejmě tedy i v České republice učení se něčemu novému.

Když mi tedy Pavel Satrapa oznámil, že plánuje další aktualizaci jeho knihy o IPv6 a že by ji opět rád vydal v rámci Edice CZ.NIC, přivítal jsem to s nadšením. Málokdo má vlohy a trpělivost číst dlouhé anglicky napsané dokumenty RFC, málokdo má čas sledovat, co všechno se v této oblasti za poslední tři roky změnilo. Pavel tímto vlastně naplňuje ono okřídlené heslo „Think globally act locally“. Pomáhá totiž s řešením globálního problému tím, že vzdělává místní internetovou komunitu a dlužno podotknout, že navíc velmi svěží formou.

Přeji vám příjemné čtení této skvělé knihy a zároveň hodně sil a štěstí při budování „nového“ Internetu.

Ondřej Filip

Chelčice, Listopad 2011



## Předmluva ke třetímu vydání

Síťové protokoly se dělí na dvě kategorie: ty, které byly za standard oficiálně prohlášeny, a ty, které se jim doopravdy staly. IP, nosný protokol Internetu, nepochybně patří do druhé skupiny. Jednoznačně ovládl pole a představuje dnes standardní cestu ke vzájemné komunikaci počítačů.

Své popularitě však vděčí i za určité problémy, které se objevily při masovém nasazení. Tím nejpalcivějším je nedostatek adres, který pocítují především noví uživatelé (staří mazáci mají nahrabáno). Proto se od první poloviny devadesátých let vyvíjí jeho nástupce – IP verze 6.

Nový protokol si klade za cíl nejen zvětšit adresní prostor, ale i přidat některé pokročilé vlastnosti, které posunou možnosti Internetu zase o kus dál. Ovšem nelze zamlčovat, že se prosazuje pomalu a bolestně. Firmám se příliš nechce investovat do vývoje, protože návratnost je nejistá, zatímco na současném IPv4 se dá vydělat hned. Takže všichni chodí opatrně kolem rybníka, trousí optimistické fráze, tu a tam se někdo osmělí, ale do vody se stále příliš nehrnou.

Cílem této knihy je popsat, jak rybník vypadá a co se v něm děje. Snažil jsem se velmi zevrubně vysvětlit principy a mechanismy, na kterých IPv6 stojí. Najdete zde formát datagramu, adresování, automatickou konfiguraci, směrování i pokročilé prvky, jako je IPsec či podpora mobilních zařízení. Nemalý prostor jsem věnoval také metodám, které mají umožnit hladký přechod od staré verze protokolu k nové a které tak nepěkně drhnou.

Tyto teoretické pasáže jsou shromážděny v první části knihy. Druhá se věnuje praxi – jak nakonfigurovat IPv6 ve vybraných operačních systémech či směrovačích a jak používat některé programy s jeho podporou.

Přestože byl základ IPv6 položen v polovině 90. let, protokol se stále vyvíjí. Přesněji řečeno jeho jádro je stabilní, ale váže se k němu celá řada doprovodných mechanismů vytvářejících košatý strom vzájemně souvisejících protokolů, na němž stále raší nové listy a nahrazují své předchůdce. V posledních letech už se spíše pilují detaily, odstraňují objevené problémy a upřesňují nejasná místa, nicméně občas je přijata i zásadnější specifikace, jako například NAT64 z jara letošního roku.

Nesnažil jsem se popsat vše do posledního detailu. U složitějších protokolů (jako je OSPFv3) by takový přístup vydal na samostatnou knihu. V těchto případech jsem dal přednost popisu základních prvků a principů, na kterých daný mechanismus stojí, abyste pochopili jeho funkci. Zajímají-li vás detaily, jako jsou přesné formáty zpráv, podmínky pro jejich odesílání, přesná definice chování účastníků komunikace a podobně, budete se muset obrátit na RFC a další dokumenty.

Přesto si troufám tvrdit, že zejména u komplikovanějších témat, jako je IPsec, mobilita či některé směrovací protokoly, jde kniha do výrazně větší hloubky, než je v kraji zvykem. Dostupné publikace o IPv6 tyto oblasti zpravidla jen naznačují. Nevím o tom, že by byl (a to v celosvětovém měřítku) k dispozici text s takto uceleným a aktuálním popisem problematiky IPv6.

První vydání této knihy vyšlo v roce 2002 u společnosti Neocortex, s. r. o., druhé vydal o šest let později CZ.NIC jako první publikaci své nově zahájené *Edice CZ.NIC*. Nyní, bezmála deset let od prvního vydání, vychází vydání třetí, jež je opět aktualizováno podle současného stavu světa IPv6. Změny proti jeho předchůdci nejsou dramatické, ve většině kapitol se jedná spíše o údržbu.

Nicméně několik podstatných událostí a změn se do obsahu promítlo. Nejvýznamnější je nepochybně vyčerpání IPv4 adres, k němuž po létech více či méně úspěšných prognóz skutečně došlo a od letošního února zeje jejich centrální zásoba prázdnou. Další významnou novinkou byla – opět letošní – standardizace překladače NAT64, který zacelil Macochu v přechodových mechanismech vzniklou likvidací NAT-PT. Třetí změna, jež stojí za zmínku, je zařazení softwarového směrovače BIRD, který se má v posledních letech čile k světu. Společně s desítkami drobných aktualizací a doplňků navýšily tyto úpravy počet stránek přibližně o padesát.

Text předpokládá, že čtenář má jisté základní znalosti o IPv4 a fungování Internetu. Pravděpodobně byste se obešli i bez nich, ale pochopení některých pasáží by se tak o poznání ztížilo.

Děkuji všem, kteří přispěli ke vzniku tohoto textu. V první řadě své ženě Marcele a celé rodině, která mi jako vždy poskytla zázemí pro práci a měla se mnou trpělivost. Dále si speciální poděkování zaslouží kolegové, jejichž poznámky a rady pomohly dovést text do konečné podoby, zejména Luboš Pavlíček, Pavel Moravec, Petr Adamec, Stanislav Petr a Emanuel Petr.

Pavel Satrapa

Liberec, listopad 2011



# Obsah

Předmluva vydavatele . . . . .	5
Předmluva ke třetímu vydání . . . . .	7
Obsah . . . . .	9
<b>1 Úvod</b>	<b>17</b>
1.1 Vlastnosti a vývoj . . . . .	17
1.2 Současný stav . . . . .	21
1.3 Základní principy . . . . .	23
1.4 Implementace . . . . .	24
1.5 IPv6 Forum a program IPv6 Ready . . . . .	25
1.6 6bone . . . . .	29
1.7 Politická podpora a projekty . . . . .	30
1.8 Webové zdroje . . . . .	31
<b>I Jak funguje IPv6</b>	<b>33</b>
<b>2 Formát datagramu</b>	<b>35</b>
2.1 Datagram . . . . .	35
2.2 Zřetězení hlaviček . . . . .	38
2.3 Volby . . . . .	40
2.4 Směrování . . . . .	43
2.5 Fragmentace . . . . .	45
2.6 Velikost datagramů . . . . .	48
2.7 Jumbogramy . . . . .	49
2.8 Rychlý start . . . . .	50
2.9 Toky . . . . .	51

<b>3</b>	<b>Adresy v IPv6</b>	<b>55</b>
3.1	Jak se adresuje . . . . .	55
3.2	Podoba a zápis adresy . . . . .	56
3.3	Rozdělení aneb typy adres . . . . .	58
3.4	Globální individuální adresy . . . . .	60
3.5	Identifikátory rozhraní – modifikované EUI-64 a spol. . . . .	61
3.6	Lokální adresy . . . . .	63
3.7	Adresy obsahující IPv4 . . . . .	66
3.8	Skupinové adresy . . . . .	68
3.9	Výběrové adresy . . . . .	75
3.10	Povinné adresy uzlu . . . . .	79
3.11	Dosahy adres . . . . .	81
3.12	Výběr adresy . . . . .	84
3.13	Vicedomovci čili multihoming . . . . .	88
3.14	Přidělování adres . . . . .	91
<b>4</b>	<b>ICMPv6</b>	<b>97</b>
4.1	Chybové zprávy . . . . .	99
4.2	Informační zprávy . . . . .	101
4.3	Bezpečnostní aspekty ICMP . . . . .	102
<b>5</b>	<b>Objevování sousedů (Neighbor Discovery)</b>	<b>103</b>
5.1	Hledání linkových adres . . . . .	104
5.2	Detekce dosažitelnosti souseda . . . . .	106
5.3	Inverzní objevování sousedů . . . . .	108
5.4	Bezpečnostní prvky objevování sousedů – SEND . . . . .	110
5.5	Lehčí verze ochrany . . . . .	116

<b>6</b>	<b>Automatická konfigurace</b>	<b>119</b>
6.1	Ohlášení směrovače . . . . .	119
6.2	Určení vlastní adresy . . . . .	123
6.3	Konfigurace směrování . . . . .	124
6.4	Konfigurace DNS . . . . .	126
6.5	DHCPv6 . . . . .	128
6.6	Bezstavové DHCPv6 . . . . .	134
6.7	Jak tedy konfigurovat? . . . . .	135
6.8	Jednoduchá detekce připojení . . . . .	136
<b>7</b>	<b>Směrování a směrovací protokoly</b>	<b>139</b>
7.1	Elementární směrování . . . . .	139
7.2	Směrovací protokoly . . . . .	140
7.3	RIPng . . . . .	142
7.4	OSPF . . . . .	148
7.5	IS-IS . . . . .	156
7.6	BGP4+ . . . . .	158
<b>8</b>	<b>Skupinové radovánky čili multicast</b>	<b>163</b>
8.1	Doprava po Ethernetu a Wi-Fi . . . . .	163
8.2	Multicast Listener Discovery (MLD) . . . . .	164
8.2.1	MLD verze 1 . . . . .	165
8.2.2	MLD verze 2 . . . . .	167
8.3	Směrování skupinových datagramů . . . . .	176
8.3.1	PIM Sparse Mode (PIM-SM) . . . . .	178
8.3.2	PIM Dense Mode (PIM-DM) . . . . .	185
8.3.3	Bidirectional PIM (BIDIR-PIM) . . . . .	186
8.3.4	Source-Specific Multicast (PIM-SSM) . . . . .	187

<b>9</b>	<b>Domain Name System</b>	<b>189</b>
9.1	IPv6 adresy v DNS . . . . .	190
9.2	Obsah domén . . . . .	193
9.3	Provozní záležitosti . . . . .	195
<b>10</b>	<b>IPsec čili bezpečné IP</b>	<b>199</b>
10.1	Základní principy . . . . .	199
10.2	Authentication Header, AH . . . . .	205
10.3	Encapsulating Security Payload (ESP) . . . . .	206
10.4	Správa bezpečnostních asociací . . . . .	209
10.4.1	IKEv2 . . . . .	210
10.4.2	Autentizace . . . . .	216
<b>11</b>	<b>Mobilita</b>	<b>221</b>
11.1	Základní princip . . . . .	221
11.2	Hlavičky a volby . . . . .	223
11.3	Získání domácího agenta . . . . .	229
11.4	Optimalizace cesty . . . . .	232
11.5	Přenosy dat . . . . .	236
11.6	Změny a návrat domů . . . . .	238
11.7	Rychlé předání . . . . .	239
11.8	Hierarchická mobilita . . . . .	242
11.9	Proxy mobilita . . . . .	246
11.10	Mobilní sítě (NEMO) . . . . .	249
<b>12</b>	<b>Kudy tam</b>	<b>251</b>
12.1	Dvojí zásobník . . . . .	252
12.2	Obecně o tunelování . . . . .	253
12.3	6to4 . . . . .	257
12.4	IPv6 Rapid Deployment (6rd) . . . . .	261
12.5	6over4 . . . . .	263

12.6	ISATAP	264
12.7	Teredo	266
12.8	Dual-Stack Lite	271
12.9	Stateless IP/ICMP Translation Algorithm (SIIT)	273
12.10	Network Address Translation – Protocol Translation (NAT-PT)	277
12.11	NAT64 a DNS64	280
12.12	Transport Relay Translator (TRT)	283
12.13	Bump-in-the-Host (BIH)	284
12.14	Přechodové nástroje v praxi	286
<b>II</b>	<b>IPv6 v praxi</b>	<b>289</b>
<b>13</b>	<b>IPv6 na vlastní kůži</b>	<b>291</b>
13.1	Lehké ořukávání	291
13.2	Trvalé připojení	293
13.3	Testování a měření	300
13.4	IPv6 v lokální síti	301
13.5	Adresování místní sítě	304
13.6	Aplikace	308
13.7	Život bez NATu	309
13.8	Bezpečnost koncových strojů a sítí	310
13.9	IPv6 v páteřní síti	314
<b>14</b>	<b>BSD</b>	<b>317</b>
14.1	IPv6 v jádře	317
14.2	Konfigurace rozhraní	318
14.3	Konfigurace směrování	319
14.4	Přechodové mechanismy	320

<b>15 Linux</b>	<b>323</b>
15.1 Distribuce . . . . .	323
15.2 Překlad jádra . . . . .	324
15.3 Konfigurace síťových parametrů . . . . .	325
15.4 Přechodové mechanismy . . . . .	327
15.5 Další informace . . . . .	329
<b>16 Microsoft Windows</b>	<b>331</b>
16.1 Windows 7 a Vista . . . . .	331
16.1.1 Konfigurace rozhraní . . . . .	333
16.1.2 Konfigurace směrování . . . . .	336
16.1.3 Přechodové mechanismy . . . . .	336
16.2 Windows XP . . . . .	338
16.2.1 Instalace . . . . .	338
16.2.2 Konfigurace rozhraní . . . . .	339
16.2.3 Směrování . . . . .	341
16.2.4 Přechodové mechanismy . . . . .	342
16.2.5 Ostatní . . . . .	342
16.3 Další informace . . . . .	343
<b>17 Cisco</b>	<b>345</b>
17.1 Konfigurace rozhraní . . . . .	345
17.2 Směrování . . . . .	348
17.2.1 RIPng . . . . .	348
17.2.2 OSPFv3 . . . . .	349
17.3 Mobilita . . . . .	350
17.4 Přechodové mechanismy . . . . .	351
17.5 Skupinové adresování . . . . .	353
17.6 Další informace . . . . .	354

<b>18 Směrovací programy</b>	<b>355</b>
18.1 BIRD Internet Routing Daemon . . . . .	355
18.1.1 Základy konfigurace . . . . .	356
18.1.2 Protokoly . . . . .	358
18.1.3 Řízení běžícího BIRDu . . . . .	362
18.2 Quagga . . . . .	363
18.2.1 Základy konfigurace . . . . .	364
18.2.2 zebra . . . . .	367
18.2.3 ripngd . . . . .	368
18.2.4 ospf6d . . . . .	370
<b>19 Ohlašování směrovače</b>	<b>371</b>
19.1 Ohlašování – radvd . . . . .	371
19.2 Likvidace „pirátských“ ohlášení – ramond . . . . .	374
<b>20 BIND</b>	<b>377</b>
<b>21 Server pro DHCPv6</b>	<b>381</b>
21.1 Dnsmasq . . . . .	381
21.2 ISC DHCP . . . . .	383
21.3 Určení DUID . . . . .	387
<b>III Přílohy</b>	<b>389</b>
<b>A Rezervované adresy a identifikátory</b>	<b>391</b>
A.1 Skupinové adresy . . . . .	391
A.2 Skupinové identifikátory . . . . .	392
A.3 Výběrové adresy . . . . .	392

<b>B</b>	<b>Specifikace IPv6</b>	<b>393</b>
B.1	Jádro protokolu . . . . .	393
B.2	Přenos po linkových technologiích . . . . .	393
B.3	Adresy . . . . .	394
B.4	Směrování . . . . .	394
B.5	Skupinově adresovaná data . . . . .	395
B.6	DNS . . . . .	395
B.7	Automatická konfigurace . . . . .	395
B.8	IPsec . . . . .	396
B.9	Mobilita . . . . .	396
B.10	Přechodové mechanismy . . . . .	397
	<b>Literatura</b>	<b>399</b>
	<b>Rejstřík</b>	<b>401</b>



# 1 Úvod

*Internet Protocol verze 6 (IPv6)* se má stát následníkem nosného protokolu současného Internetu, kterým je Internet Protocol verze 4 (IPv4). Ve starší literatuře bývá označován též jako *IP Next Generation (IPng)*.

## 1.1 Vlastnosti a vývoj

**cíle a vlastnosti** Jeho kořeny sahají do začátků devadesátých let, kdy začalo být zřejmé, že se adresní prostor dostupný v rámci IPv4 rychle tenčí. Tehdy vypracované studie ukazovaly, že s perspektivou přibližně deseti let dojde k jeho úplnému vyčerpání. Jelikož na řešení problému bylo k dispozici poměrně dost času, rozhodlo se IETF navrhnout zásadnější změnu, která by kromě rozšířeného adresního prostoru přinesla i další nové vlastnosti.

U kolébky IPv6 proto stály následující požadavky:

- rozsáhlý adresní prostor, který vystačí pokud možno navždy
- tři druhy adres: individuální (unicast), skupinové (multicast) a výběrové (anycast)
- jednotné adresní schéma pro Internet i vnitřní sítě
- hierarchické směrování v souladu s hierarchickou adresací
- zvýšení bezpečnosti (zahrnout do IPv6 mechanismy pro šifrování, autentizaci a sledování cesty k odesílateli)
- podpora pro služby se zajištěnou kvalitou
- optimalizace pro vysokorychlostní směrování
- automatická konfigurace (pokud možno plug and play)
- podpora mobility (přenosné počítače apod.)
- hladký a plynulý přechod z IPv4 na IPv6

Jak je vidět, cíle nebyly skromné. Chopili se jich především Steven Deering a Robert Hinden, kteří mají největší podíl na vzniku nového protokolu.

**vývoj** Jejich snaha vyústila koncem roku 1995 ve vydání sady RFC definujících základ IPv6. Jedná se o [RFC 1883: Internet Protocol, Version 6 \(IPv6\) Specification](#) a jeho příbuzné.

Oficiální specifikace protokolu tedy byla na stole a mohlo se začít s implementováním a uváděním do života. Jenže nezačalo. IPv6 bylo příliš ožehavou a nejistou půdou, zatímco na poli IPv4 čekaly zisky *ted' hned*. Většina

fírem se proto věnovala raději snaze o rozvoj IPv4, než aby se angažovala v IPv6, protože návratnost investic byla v prvním případě rychlejší.

Mimo jiné se podařilo otupit ostří největšího nože na krku IPv4 – nedostatku adres. Začalo se používat beztrždní adresování CIDR, zpřísnila se kritéria pro přidělování síťových adres a byly zavedeny mechanismy pro překlad adres (NAT, viz níže).

Tím IPv6 přišlo o svou hlavní hnací sílu a jeho nasazení se začalo odkládat. Aby se dokázalo prosadit do praxe, musí nabídnout nějaké zásadní výhody. Ovšem všechny jeho lákavé vlastnosti byly mezitím implementovány i pro IPv4. Pravda, ne vždy tak elegantně a zdaleka ne každá implementace je podporuje, ale principiálně jsou k dispozici. A jak již bylo řečeno, většina hráčů na tomto poli preferuje rychlé a velké zisky před vzdálenými a nejistými.

To neznamená, že by se vývoj IPv6 zastavil. Koncem roku 1998 vyšla *revidovaná sada RFC* dokumentů s definicí základních protokolů a služeb a postupně jsou aktualizovány či doplňovány další kousky této velké mozaiky. Poslední verze adresní architektury pochází z roku 2006, podpora mobility byla dokončena v roce 2004 (a revidována v roce 2011), o rok později došlo k revizi bezpečnostních prvků ... Navíc – a to je nejdůležitější – se začaly množit a zlepšovat implementace v nejrůznějších operačních systémech. Také řada aplikací dnes již podporuje nový protokol.

<b>aktivní</b>	
<i>6man</i>	údržba a aktualizace specifikací
<i>v6ops</i>	provoz IPv6 sítí
<i>6renum</i>	přeadresování IPv6 sítí
<i>mext</i>	rozšíření mobility
<i>6LoWPAN</i>	IPv6 v nízkonapěťových osobních sítích
<b>uzavřené</b>	
<i>ipv6</i>	(původně <i>ipng</i> ) vytvořila většinu základních specifikací
<i>mip6</i>	mobilita
<i>multi6</i>	multihoming
<i>shim6</i>	multihoming
<i>6bone</i>	vytvoření sítě <i>6bone</i>

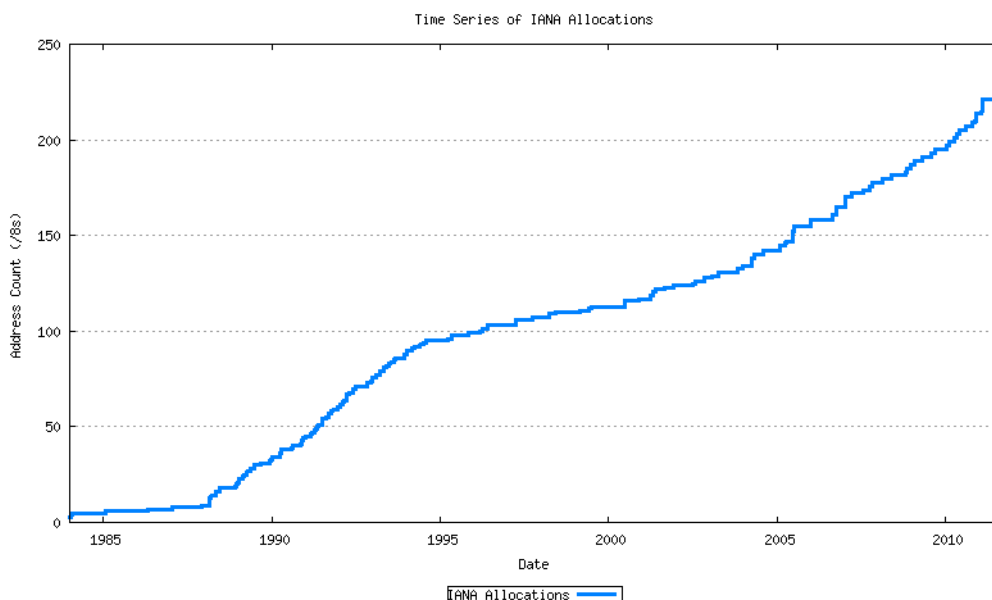
**Tabulka 1.1:** Pracovní skupiny IETF zapojené do vývoje IPv6

Na vývoji IPv6 a jeho komponent se podílela a podílí celá řada pracovních skupin IETF. Přehled těch nejvýznamnějších uvádí tabulka 1.1. Veškeré jejich dokumenty najdete na adrese

**www►** <http://www.ietf.org/html.charters/wg-dir.html>

Priority pro nasazení se časem měnily. Tlak nedostatku adres sice polevil, zato se do popředí začaly drát jiné přednosti IPv6, zejména podpora mobility. Při rychle rostoucím zájmu o nejrůznější přenosná zařízení a jejich zapojení do Internetu by se právě jejich podpora, která je v IPv6 výrazně lepší než u jeho předchůdce, mohla stát rozhodujícím argumentem.

Ovšem nelze nepřiznat, že trvalo bezmála deset let, než se podařilo dokončit specifikaci mobilního IPv6 – RFC 3775: *Mobility Support in IPv6* vyšlo v roce 2004. Po celou tu dobu byla podpora mobility všude vyhlášována za povinnou součást IPv6 a jeden z důvodů, proč přejít na nový protokol. Právě rozpor mezi slibnými vlastnostmi na papíře a tristním stavem implementací, v nichž pokročilé prvky zpravidla chyběly, odvedl IPv6 medvědí službu.



**Obrázek 1.1:** Spotřeba IPv4 adres (zdroj: *ipv4.potaroo.net*)

**adresy jsou zpět** Jenže rok se s rokem sešel a adresní prostor vrátil úder, a to rovnou KO. Internet si sice našel způsob, jak zpomalit jeho konzumaci, ale i ten má své meze. Obrázek 1.1 ukazuje historický vývoj počtu osmibitových prefixů přidělených jejich centrálním správcem IANA. Je v něm pěkně vidět, jak opatření z poloviny 90. let razantně snížila tempo spotřeby, proč prognózy kolem roku 2000 ukazovaly dostatek adres na 20 let a jak později začala křivka zase ošklivě stoupat.

Aktuálně se nacházíme v situaci, kdy je vyčerpána centrální zásoba IANA a jednotlivé regionální registry (RIR) postupně spotřebovávají své zásoby.

Nejrychleji rostoucí APNIC skončil s adresami velmi brzy po IANA, vyčerpání ostatních registrů je očekáváno během několika let – evropský RIPE NCC kolem poloviny roku 2012, zbývající tři zhruba o rok až dva později.

vyčerpáno	
IANA	3. února 2011
APNIC	19. dubna 2011
prognóza (podle <a href="http://ipv4.potaroo.net">ipv4.potaroo.net</a> z 29. listopadu 2011)	
RIPE NCC	červenec 2012
ARIN	červen 2013
LACNIC	leden 2014
AFRINIC	srpen 2014

**Tabulka 1.2:** Vyčerpání IPv4 adres

Vyčerpání registru neznamena, že v dané oblasti nelze získat IPv4 adresu. Ale místní poskytovatelé Internetu (v roli lokálních registrů, LIR) už nedostanou žádný větší blok. V režimu po vyčerpání regionální registry přidělují jen velmi omezené množství adres – každý lokální registr může získat jen jeden malý blok. Oficiálně jsou tyto adresy určeny pro přechodové mechanismy.

Jak rychle lokální registry vyčerpají své zásoby IPv4 adres závisí na tom, kolik si jich stačily nashromáždit, jakým tempem roste jejich zákaznictvo a která úsporná opatření nasadí. Zároveň se všeobecně očekává rostoucí obchodování s adresami, jehož některé případy již proběhly s nemalou mediální pozorností<sup>1</sup>. IPv4 adresy z pohledu provozovatelů sítí a zákazníků nejsou a hned tak nebudou zcela nedostupné, ale přístup k nim se postupně komplikuje a prodražuje.

**NAT** Opatření k úspoře adres navíc porušují nezákladnější principy Internetu – možnost přímé komunikace libovolných dvou zařízení. Začaly se totiž masivně šířit nástroje pro překlad adres – *Network Address Translation, NAT*. Fungují tak, že přístupový směrovač sítě mění IP adresy paketů, které jím procházejí ze sítě do Internetu a naopak. Díky tomu celá koncová síť vystačí s jednou jedinou veřejnou IP adresou, ale počítače uvnitř nejsou z vnějšího Internetu adresovatelné. To znamená, že komunikace se dá zahájit jen směrem zevnitř sítě ven.

Zavedením NAT se ztrácí přímocí komunikace. Vstupuje do ní nový prostředník, který představuje citelnou překážku. Zcela protichůdnou tendencí je rostoucí popularita služeb pro přímou komunikaci mezi uživateli (ICQ a podobné komunikátory, IP telefonie, videokonference, síťové hry a další). Potřebují vytvářet přímá spojení mezi komunikujícími zařízeními.

<sup>1</sup> Na jaře 2011 koupil Microsoft od bankrotujícího Nortelu blok přesahující 600 tisíc IPv4 adres za 7,5 milionu USD.

Leží-li každý v jiné NATované síti, není jak je navázat. Vymýšlejí se tedy různé berličky, kontaktní servery s veřejnými adresami, na nichž se mohou neveřejně adresovaní klienti spojit, komunikace přes prostředníky a podobně. Tunelovací mechanismus Teredo popsany na straně 266 je pěknou ukázkou, jakou lahůdkou je život v síti protkané NATy.

Jako lék nabízí IPv6 svůj olbřímí adresní prostor. Již nikdy nedostatek adres, již nikdy více NAT. Každý počítač, hodinky, lednička či další zařízení bude mít svou vlastní, celosvětově jednoznačnou IP adresu.

**zápory** V předchozím textu jsem opakovaně naznačil, že IPv6 nepřináší jen samá pozitivita a sociální jistoty. Podívejme se na nejdůležitější píhy jeho krásy. Tou největší nepochybně je, že je příliš jiný a především zpětně nekompatibilní s IPv4. To podstatným způsobem komplikuje jeho nasazení – uživatelé s počítači hovořícími pouze novým protokolem se nedostanou ke službám poskytovaným pouze po IPv4. Byla sice vymyšlena celá řada protokolů a mechanismů pro přechod od starého protokolu k novému, včetně překladu datagramů mezi nimi, v praxi ale toto úsilí vyznívá do prázdna.

IPv6 se potácí v bludném kruhu slepice versus vejce. Uživatelé o něj nemají zájem, protože v něm nejsou dostupné služby. A kdo by převáděl služby pod IPv6, když tam nejsou žádní uživatelé? Existují sice snahy postrčit poskytovatele služeb i připojení směrem k novému protokolu, jako byl například Světový den IPv6 v červnu 2011, ale statistiky stále ukazují objem IPv6 provozu v desetinách procenta vůči IPv4.

V poslední době je zřetelná snaha přispět k rozetnutí tohoto kruhu politicky. Vlády vydávají prohlášení a výzvy podporující přechod na IPv6, financují se projekty rozvíjející infrastrukturu a služby. Podařilo se dosáhnout mírného pokroku v mezích zákona, ale nástup IPv6 je stále velmi pomalý.

Své nepochybně vykonal i pomalý vývoj některých specifikací. O nejkřiklavějším případě mobility jsem se již zmínil. Bohužel není sama, DHCPv6 bylo definováno jen o rok dříve, přestože se jedná o protokol ve světě IPv4 dobře známý a hojně používaný. Standardizace jednotlivých součástí světa IPv6 stále probíhá, i když nyní už se spíše jen doladují detaily. Nejisté výnosy<sup>2</sup> v kombinaci s nestabilními specifikacemi jsou silně odrazující pro všechny, kteří by chtěli nový protokol implementovat. Proto jim to šlo jako psí pas-tva, počáteční implementace byly značně nedokonalé a zlepšovaly se jen velmi zvolna.

## 1.2 Současný stav

Sečteno a podtrženo: IPv6 je zajímavý a nadějný protokol, který je mnohými považován za jedinou možnost pro budoucnost Internetu. Přesto míra jeho nasazení dlouhodobě pokulhává za vizemi a plány. Ještě pořád se nedá

<sup>2</sup> respektive spíše jisté nevýnosy

vyloučit, že se stane stejně slepou vývojovou větví, jako svého času ISO OSI, ale pravděpodobnost takového vývoje klesá. IETF nevyvíjí žádnou alternativu a největším konkurentem nového protokolu je stávající IPv4, od něž se nikomu moc nechce ustupovat. Jenže Internet s NATem na každém rohu či obchodování s adresami, což jsou nejčastěji citované scénáře dalšího vývoje IPv4 při vyčerpání adresního prostoru, prodrazí provozování sítí a bude motivovat k přechodu na nový protokol.

Geoff Huston, autor grafů spotřeby IPv4 adres a matematických modelů jejich vyčerpání, vytvořil několik pěkných prezentací na téma současného i budoucího nasazení IPv6.

**www►** <http://www.potaroo.net/presentations/>

Jeho *Measuring IPv6 Day* ze září 2011 odhaduje počet strojů používajících IPv6 na 0,4%. Číslo nikterak oslnující, které ale zahrnuje jen ty počítače, které při přístupu otevřeném oběma protokoly dávají přednost IPv6. K obsahu, který je vystaven jen protokolem IPv6 se dostane zhruba desetinásobek strojů. A pokud není třeba použít DNS, je takový obsah dostupný bezmála 30% uživatelských strojů. Situace se pozvolna zlepšuje, ale tempo je stále mnohem menší, než by bylo potřeba.

**Google** Jedním z velmi viditelných subjektů na poli IPv6 je Google. Protokolu se soustavně věnuje od roku 2008 a řeší dilema, zda své servery zpřístupnit nativně po IPv6 za cenu ztráty malého počtu zákazníků. Jenže i desetina procenta je v případě světové vyhledávací jedničky obrovský počet uživatelů. Výsledkem je šalamounské řešení, kdy se k serverům Google sice dá dostat nativním IPv6, ovšem uživatel musí aktivně chtít. Nejjednodušší variantou je použít doménové jméno

**www►** <http://ipv6.google.com/>

Koncepčnější cesta je k dispozici pro organizace, které mohou získat plnohodnotný IPv6 přístup ke službám Google. Je postaven na proměnlivém chování DNS. Pokud se průměrný stroj dotáže DNS, zda existuje IPv6 adresa pro *www.google.com*, skončí neúspěšně. Jestliže se však zeptá ze sítě, již Google povolil IPv6 přístup, dostane kladnou odpověď (a pravděpodobně se připojí novějším protokolem, protože operační systémy mu obvykle dávají přednost).

Google tedy eviduje seznam sítí, jimž má poskytovat IPv6 služby, a pro ně se jeho DNS servery chovají jinak. Chcete-li se mezi ně zařadit, je třeba o to požádat a mimo jiné se zavázat, že budete řešit případné problémy v IPv6 komunikaci, které by se vyskytly. Seznam sítí zapojených do IPv6 programu není veřejný, v České republice vím o několika univerzitách, jež jsou do něj zapojeny. Podrobnější informace najdete na adrese

**www►** <http://www.google.com/ipv6/>

**světový den IPv6** Jednou z novějších aktivit byl *Světový den IPv6*, který se konal 8. června 2011. Cílem bylo vyzkoušet si IPv6 v ostrém provozu, protože řada významných zdrojů<sup>3</sup> během tohoto dne poskytovala své služby nativně oběma protokoly. Vše se pečlivě sledovalo a měřilo. Pokud je mi známo, nedošlo k žádným dramatickým problémům na straně uživatelů, ale kupodivu ani k dramatickému nárůstu IPv6 provozu. Někteří z účastníků už své servery ponechali přístupné nativním IPv6. Celkově lze den IPv6 považovat za úspěšný a nepochybně nezůstane jen u jednoho. V době vzniku tohoto textu již Google zahájil přípravu další podobné události na červen 2012.

Internetová komunita rozhodně netrpí nezájmem o nový protokol. Konference na toto téma se těší notoricky dobré účasti, čile se diskutuje a v současnosti i experimentuje a trochu nasazuje. Jen těm provozním grafům se pořád nechce odlepit se výrazněji ode dna.

### 1.3 Základní principy

Na začátku kapitoly jsem popsal úkoly, které mělo IPv6 vyřešit. Zde se budu ve stručnosti zabývat některými nosnými principy, na kterých je postaveno.

Požadavek na větší rozsah *adresního prostoru* vedl k nemalým debatám o optimální délce adresy. Nakonec byla stanovena na 128 bitů, tedy čtyřnásobek délky použité v IPv4. To znamená, že k dispozici je  $3,4 \cdot 10^{38}$  adres. To je jen těžko představitelné číslo, zkusme je uvést do souvislosti. Povrch zeměkoule činí přibližně půl miliardy kilometrů čtverečních. To znamená, že na jeden čtvereční milimetr zemského povrchu připadá  $667 \cdot 10^{15}$  adres. Ano, řeč je o milionech miliard. V kapitole o adresování uvidíte, že IPv6 velmi plýtvá. Celých 64 bitů věnuje na identifikátor rozhraní, což znamená, že v jedné podsíti lze rozlišit miliardy miliard počítačů. Každá síť má prostor na adresaci 65 tisíc podsítí. A takovýchto sítí je k dispozici bezmála 30 tisíc na každého obyvatele zeměkoule<sup>4</sup>. IPv6 adres je v každém ohledu dost a dost, jak se přesvědčíte v kapitole 3 na straně 55.

*Formát datagramu* byl podroben zásadní revizi. Stručně řečeno: počet položek byl minimalizován a jejich složení upraveno tak, aby základní hlavička datagramu měla konstantní délku. Dřívější volitelné položky byly přesunuty do samostatných hlaviček, které mohou být přidávány k pevnému základu. Pořadí přidávaných hlaviček je zvoleno tak, aby směrovač co nejrychleji mohl zpracovat ty, které jsou určeny pro něj, a zbývající ignorovat.

Popsané změny v záhlaví datagramu mají za cíl usnadnit jeho zpracování a umožnit tak směrování paketů vysokou rychlostí. Dalším aspektem z této oblasti je zavedení koncepce toku (proud souvisejících datagramů se spo-

<sup>3</sup> Mezi jinými servery Google, Facebook, Yahoo! a distribuční sítě Akamai a Limelight Networks.

<sup>4</sup> Počítáno pro deset miliard pozemšťanů.

lečnými parametry), který má opět usnadnit vysokorychlostní směrování. Formát datagramu popisuje kapitola 2 na straně 35.

Z hlediska *automatické konfigurace* se autoři IPv6 snažili, aby byla pokud možno zcela bezpracná. Zavedli dvě alternativy: Stavová konfigurace je staré známé DHCP, ovšem upravené pro IPv6. Jeho podpora je nyní povinná. Bezstavová konfigurace představuje nový princip, kdy si počítač dokáže sám stanovit svou adresu a naučí se směřovat, aniž by jeho správce kdekoli cokoli konfiguroval. Automatickou konfigurací se zabývá kapitola 6 na straně 119.

S bezstavovou konfigurací je poměrně těsně svázáno i *objevování sousedů*. Jeho primárním cílem je nahradit dřívější protokol ARP při hledání fyzických adres sousedních počítačů. Ovšem objevování sousedů má poněkud širší záběr a zahrnuje i mechanismy pro automatickou konfiguraci (objevování směrovačů a parametrů sítě) či testování jednoznačnosti adresy. Vše se dočtete v kapitole 5 na straně 103.

Požadavek na *služby se zaručenou kvalitou* se projevil zavedením tříd provozu a služeb s diferencovanou kvalitou, jejichž prostřednictvím lze zavést různé priority a režimy zpracování datagramů.

Pro zajištění *bezpečnosti* slouží dvě rozšiřující hlavičky: autentizační a šifrovací. Autentizační umožňuje ověřit, zda odesílatelem dat je skutečně ten, kdo to o sobě tvrdí, a zda během přepravy nedošlo ke změně dat. Hlavička pro šifrování dokáže totéž a navíc lze její pomocí zašifrovat celý obsah datagramu. Způsob zabezpečení IPv6 popisuje kapitola 10 na straně 199.

Podpora *mobilních uzlů* staví na domácích agentech. Jedná se o směrovač, který je umístěn v domácí síti mobilního uzlu a „zastupuje jej“ v době nepřítomnosti. Mobilní uzel svému agentovi hlásí aktuální polohu a pokud mu do domácí sítě dorazí nějaká data, domácí agent je přepošle. Následně mobilní uzel oznámí odesílateli, že dočasně změnil svou IP adresu a další komunikace s ním již bude probíhat přímo. Více najdete v kapitole 11 na straně 221.

Pro usnadnění *společné existence IPv6 a IPv4* byla vymyšlena řada nástrojů. Nejjednodušší možností je klasické tunelování, které ponechává oba světy víceméně oddělené a pouze využívá infrastrukturu jednoho k přenosu dat druhého. Kromě něj jsou však k dispozici i rafinovanější metody nabízející překlad datagramů a podobné věci. Zabývá se jimi kapitola 12 na straně 251.

## 1.4 Implementace

Podpora IPv6 ve směrovačích, operačních systémech a aplikacích se začala objevovat poměrně záhy po vydání první sady RFC. V listopadu 1996 se objevilo IPv6 jako experimentální vlastnost jádra Linuxu verze 2.1.8, další systémy na sebe nenechaly dlouho čekat.



Druhou polovinu 90. let lze označit jako experimentální období plné velkých nadějí, většinou nenaplněných. Zavedení producenti operačních systémů a síťových krabic pozorovali novinku s odstupem, jen tu a tam lehce ochutnali. Několik mladých firem a startupů zkusilo rychlou implementací nového protokolu získat dobrou pozici na trhu „Internetu budoucnosti“. Podobně se asijské firmy snažily touto cestou prosadit proti tradičním výrobcům.

Zřejmě i v reakci na tyto snahy začala kolem roku 2000 implementační vlna, kterou bych označil jako marketingovou. Bylo třeba mít v produktovém letáku zaškrtnutou kolonku „podpora IPv6“, na kvalitě skutečné podpory příliš nezáleželo. Typická implementace IPv6 z počátku nového tisíciletí měla jen ty nejdůležitější schopnosti a také výkonem často zaostávala za svým předchůdcem<sup>5</sup>.

Postupem času se ale situace zlepšila. Pozitivní roli rozhodně sehrálo *IPv6 Forum* a jeho program *IPv6 Ready*, k nimž se co nevidět dostanu podrobněji. Přestalo stačit napsat „podporujeme IPv6“. Bylo třeba opatřit si certifikát, čili projít příslušnými testy. Výsledkem je, že nejvýznamnější platformy – operační systémy i hardwarové směrovače – se v současnosti mohou pochlubit podporou IPv6 na velmi slušné úrovni. Chcete-li experimentovat či uvažovat o seriózním nasazení nového protokolu, nemělo by vám z této strany nic zásadního stát v cestě.

Pravda, některé pokročilé prvky – jako je mobilita či zabezpečení – ještě mají své mouchy, obecně ale implementace za posledních několik let udělaly velký krok dopředu a dále se zlepšují. Testy kompatibility a schopností vzájemné spolupráce přispívají k tomu, aby vznikalo reálně použitelné prostředí.

Naopak příliš nedrží krok weby věnované této problematice. Obvykle vzniknou ve velkém nadšení, ale následně nebývají aktualizovány a jejich obsah se postupně rozchází s realitou. Většina výrobců programů a zařízení ale dodržuje konvenci vytvořit na svém webu stránku věnovanou IPv6. Obvykle mívá adresu

**www►** [http://web\\_vyrobcu/ipv6/](http://web_vyrobcu/ipv6/)

a najdete na ní informace o podpoře protokolu v produktech dané společnosti a často i vize dalšího vývoje.

## 1.5 IPv6 Forum a program IPv6 Ready

Stalo se již zvykem, že na podporu nových síťových technologií vznikají společenství organizací a osob usilujících o prosazení novinky do reálného

<sup>5</sup> V počáteční fázi hardwarové směrovače často implementovaly IPv6 softwarově, tedy s výkonem řádově nižším proti IPv4.

života. Jistě nejznámějším příkladem je *Wi-Fi Alliance*, jejíž pozice na poli bezdrátových lokálních sítí je taková, že oficiální název těchto technologií IEEE 802.11 znají jen lidé zasvěcení, zatímco pojem Wi-Fi zlidověl.

**IPv6 Forum** Analogickým sdružením pro podporu nové verze IP je *IPv6 Forum* založené v roce 1999. Jeho cíle sahají od propagace nového protokolu přes sdílení a šíření znalostí a zkušeností až po vývoj technických specifikací a řešení problémů při praktickém nasazení. *IPv6 Forum* původně vzniklo jako centralistická organizace, později ovšem začalo zakládat své národní a regionální pobočky. Na podzim roku 2011 jich existuje kolem šedesáti, jejich seznam najdete na webu

**www►** <http://www.ipv6forum.com/>

Ten se bohužel nachází ve velmi neutěšeném stavu a s výjimkou titulní stránky nestojí za návštěvu. Jednotlivé sekce jsou buď prázdné (dokumenty), nebo nebyly několik let aktualizovány. Na titulní stránce ovšem najdete odkazy na významné konference s tematikou IPv6 a další zajímavé zdroje.

**IPv6 Ready** Nejvýznamnější aktivitou fóra jsou rozhodně certifikační programy, mezi nimiž má prominentní roli nejstarší *IPv6 Ready*. Motivací jeho vzniku byly rané implementace IPv6, jež vykazovaly celou řadu více či méně závažných problémů.

Již v roce 1998 vznikl japonský program *TAHI*, který testoval dodržování specifikací v implementacích IPv6 a jejich vzájemnou interoperabilitu. Rychle získal technické znalosti a zkušenosti i dobré jméno mezi implementátory, neměl však žádný oficiální statut. Po založení IPv6 Fóra se nabízelo spojit síly a vytvořit certifikační program, za nímž budou stát jak odborné kompetence, tak oficiálně respektované jméno. Výsledkem je *IPv6 Ready*:

**www►** <http://www.ipv6ready.org/>

V jeho rámci si každý autor programu či zařízení podporujícího IPv6 může nechat otestovat jeho kompatibilitu se standardy. Pokud uspěje, získá oficiální certifikát a může používat stříbrné či zlaté logo *IPv6 Ready*. Míra kompatibility má totiž různé úrovně, v oficiální terminologii nazývané fáze.

**Fáze 1 (stříbrné logo)** ověřuje nejzákladnější kompatibilitu se specifikacemi IPv6. Konkrétně se testuje, zda zařízení podporuje

- IPv6 adresy
- ICMPv6
- objevování sousedů
- bezstavovou automatickou konfiguraci



**Obrázek 1.2:** Logo *IPv6 Ready*: vlevo fáze 1, vpravo fáze 2

Testuje se pouze povinné chování (v RFC označené jako „must“). Od roku 2003 bylo vydáno bezmála 500 certifikátů. V současné době je fáze 1 považována za překonanou a *IPv6 Forum* doporučuje zaměřit se na pokročilejší fázi 2.

**Fáze 2 (zlaté logo)** je všeobecně komplikovanější. Kromě povinných ověřuje i prvky důrazně doporučené (v RFC označené jako „should“). Především se ale rozpadá do různých kategorií. Povinný je základní test, který představuje rozvinutou fázi 1 doplněnou navíc o objevování MTU cesty. Při testech se zároveň rozlišuje, zda je produkt certifikován jako koncový stroj (hostitel) nebo jako směrovač. K povinné základní certifikaci může získat ještě specializovaný certifikát v některé z následujících kategorií:

- bezpečnost (IPsec)
- IKEv2
- mobilní IPv6
- mobilní síť (NEMO)
- DHCPv6
- SIP
- SNMP
- multicast aneb MLDv2

- uživatelský agent IMS pro mobilní síť (testováno)
- přechodové mechanismy (připravováno)

Na podzim 2011 překročil počet udělených certifikátů fáze 2 číslo 600. Vybrané nejvýznamnější držitele shrnuje v chronologickém pořadí tabulka 1.3. Jejich aktuální přehled i podrobné informace o testovacích procedurách najdete samozřejmě na stránkách programu *IPv6 Ready*.

<i>platforma</i>	<i>kategorie</i>	<i>získáno</i>
FreeBSD (KAME)	hostitel	3/2006
	směrovač	3/2006
Cisco IOS 12.4(9)T	směrovač	4/2006
	hostitel	5/2006
Linux 2.6.15	IPsec konec	5/2006
	směrovač	9/2007
Linux 2.6.20	IPsec brána	10/2007
	hostitel	10/2007
MS Windows Vista	IPsec konec	1/2008
	hostitel	1/2008
MS Windows Server 2008	IPsec konec	3/2008
	hostitel	10/2010
MS Windows 7	hostitel	10/2010

**Tabulka 1.3:** Vybraní držitelé certifikátů *IPv6 Ready* fáze 2

**IPv6 Enabled** Postupem času začalo *IPv6 Forum* svůj certifikační program rozšiřovat. Vzhledem k tomu, že v posledních letech již není pes nejlouběji zakopán v technice, ale spíše v ochotě nový protokol nasadit, nabízí se myšlenka certifikovat služby. Jejím ztělesněním je program *IPv6 Enabled* zahrnující dva podprogramy: pro WWW servery a poskytovatele Internetu.

Webový certifikát *IPv6 Enabled WWW* je dost jednoduchý. Garantuje, že dotyčný web server má v DNS registrovanou IPv6 adresu a je tímto protokolem dosažitelný. Čili klientovi používajícímu IPv6 nebude stát nic v cestě k jeho využívání. Ve veřejně dostupné databázi držitelů certifikátu najdete více než 1300 položek. Do domény *cz* patří 19 z nich, za nejvýznamnější lze považovat *www.nic.cz* a *www.regzone.cz*.

Poskytovatel Internetu získá certifikát *IPv6 Enabled ISP*, jestliže disponuje IPv6 adresami a přiděluje je svým zákazníkům, je dosažitelný z hlediska směrování a trvale nabízí IPv6 služby zákazníkům. V září 2011 počet certifikovaných subjektů převyšoval stovku. Z České republiky se v seznamu nachází šest regionálních poskytovatelů Internetu a jedna housingová firma. Velká jména byste mezi nimi hledali marně<sup>6</sup>.

<sup>6</sup> Jedno je ale zastoupeno nepřímo, protože jedním z držitelů je Losan internet, který dnes patří pod Telefónica O2 Business Solutions.

**IPv6 Education** Vedle techniky a nabídky služeb jsou důležité také znalosti. *IPv6 Forum* se proto pustilo i do této oblasti a zahájilo certifikační program *IPv6 Education*. Opět se člení do několika větví, v nichž lze ověřit vzdělávací kurzy nebo osoby, a to jak pro pozici IPv6 odborníků (Engineer), tak jeho šříitelů (Trainer). Asi nejkurióznější složkou programu jsou metacertifikáty, kdy *IPv6 Forum* certifikuje jiné certifikační programy, jimiž vydávané certifikáty tak získávají na váze.

## 1.6 6bone

Když se začalo experimentovat s prvními implementacemi, vznikla potřeba rozlehlé IPv6 síť, která by posloužila k testování a získávání praktických zkušeností. Tak v roce 1996 vznikla síť *6bone*. Původně propojila jen tři instituce – G6 ve Francii, UNI-C v Dánsku a WIDE v Japonsku. Svého maxima dosáhla v roce 2003, kdy bylo do *6bone* zapojeno kolem tisíce institucí z 50 zemí.

*6bone* byla takzvanou virtuální sítí. To znamená, že neměla vlastní vyhrazenou infrastrukturu, ale využívala existující síť. Skládala se z lokálních IPv6 sítí, navzájem propojených tunely. To znamená, že IPv6 datagramy se bálily jako data do běžného IPv4 a přenášely se standardním Internetem až do cílové síť. Bylo to jednoduché, levné a dala se vytvořit topologie, jaká byla potřeba.

Hlavním cílem *6bone* bylo „hrát si na opravdický IPv6 Internet“ a získat tak praktické zkušenosti s jeho provozem. Proto byla v rámci síť definována směrovací politika, vypracovány procedury na přidělování adres a další potřebné operace. Řadu let byla jedinou IPv6 sítí s globálním dosahem.

Síť měla vyhrazeny vlastní adresy, jež začínaly čtveřicí 3ffe (čili prefixem 3ffe::/16, jak se dočtete později). Organizace, které poskytovaly připojení k *6bone*, dostaly k dispozici určitý rozsah adres, vyjádřený jejich společným prefixem (označovaným jako pTLA). Z něj pak poskytovatel přiděloval části připojeným sítím. Směrovače poskytovatelů disponujících pTLA zároveň tvořily páteř síť *6bone*.

Když po roce 2000 začaly být IPv6 adresy přidělovány standardní cestou a IPv6 začalo postupně pronikat do Internetu, začal klesat i zájem o *6bone*. Svůj účel síť splnila, pomohla získat praktické zkušenosti s provozem IPv6 a doladit řadu jeho prvků. Od samotného počátku byla deklarována jako síť dočasná, což se naplnilo po deseti letech existence.

Síť *6bone* skončila stylově 6. 6. 06 a její prefix 3ffe se vrátil k pozdějšímu využití pro běžné adresy. Odvedla cenné služby a má zajištěno čestné místo v historii IPv6.

## 1.7 Politická podpora a projekty

IPv6 se během své existence dočkalo oficiální podpory z řady míst, včetně těch nejvyšších. Velmi aktivní je Asie, která do kolotoče IPv4 Internetu vstoupila pozdě. V důsledku toho zdejší výrobci hrají spíše druhé housle a některé země (v první řadě Čína) mají citelný nedostatek IPv4 adres.

Nepřekvapí, že japonská vláda již v roce 2000 vyhlásila oficiální podporu IPv6 a následně ji uplatňovala v podobě různých projektů, ale i daňových úlev. V roce 2005 vyhlásila směr IPv6 vláda USA – nejprve ministerstvo obrany, později se přidala celá federální administrativa. V roce 2008 měly všechny vládní sítě v USA podporovat IPv6, následovat měl postupný přechod aplikací.

Nepodařilo se, nicméně vláda USA to nevzdává. V září 2010 vydala memorandum, které požaduje po vedoucích IT oddělení všech orgánů vlády:

- Do konce září 2012 zpřístupnit všechny služby po IPv6<sup>7</sup>.
- Do konce září 2014 plošně nasadit nativní IPv6 ve svých sítích.
- Jmenovat všude manažery pro přechod k IPv6.
- Pořizovat pouze IT vybavení s kvalitní podporou IPv6.

Ke splnění posledního bodu vytvořil NIST testovací program označovaný jako USGv6, který definuje požadavky a způsoby jejich ověřování. Jeho web rozhodně stojí za návštěvu:

**www►** <http://w3.antd.nist.gov/usgv6/>

**Evropa** Aktivní je také Evropská komise. Z února 2002 pochází její *Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6*. Tento dokument stál v pozadí financování několika velkých projektů orientovaných na IPv6 z prostředků evropských rámcových programů. Výzvy ke členským státům v něm obsažené však na příliš úrodnou půdu nepadly.

Z května 2008 pochází akční plán Evropské komise k nasazení IPv6 – *Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe*. Jedná se o dokument místy rozumný, místy bezzubý a místy zcela neuvěřitelný<sup>8</sup>. Mimo jiné požaduje, aby projekty financované ze 7. rámcového programu

<sup>7</sup> Aktuálně využívá řada vládních webů distribuční síť Akamai, která s IPv6 sice experimentuje, ale zatím je nepodporuje. Bude zajímavé pozorovat, jestli se podaří Akamai dotlačit k podpoře IPv6, nebo zda vládní weby změní dodavatele.

<sup>8</sup> Obávám se, že zpřístupnění webů „Europa“ a „CORDIS“ po IPv6 v roce 2010 (které se navíc podařilo jen napůl, *codis.europa.eu* není ani v roce 2011 dostupný po IPv6!) nebyla taková bomba, jak se domnívají autoři dokumentu, když tento bod zařadili jako první akci stimuluji dostupnost obsahu a služeb po IPv6.

používaly ke komunikaci IPv6, pokud to je možné. Také ohlašuje, že při inovaci technického vybavení evropských struktur bude požadována podpora IPv6 a k podobnému kroku vyzývá i vlády členských států.

Evropská komise už v rámci 6. rámcového programu podpořila několik významných projektů rozvíjejících novou verzi IP. Některé z nich byly zaměřeny na vytvoření reálných IPv6 sítí, získání a dokumentaci zkušeností s jejich provozem. Sem patří například *6NET* či *Euro6IX*. Další mířily do oblasti vzdělávání a šíření informací, jako například *6DISS* a jeho nástupce *6DEPLOY*. Mezi podporovanými projekty najdete i tématicky úzce zaměřené výzkumy dílčích oblastí souvisejících s IPv6, třeba projekt *ENABLE* zabývající se mobilitou ve velkých heterogenních IP sítích.

#### Česká republika

Ani Vláda České republiky nezůstala k IPv6 lhostejná. 8. června 2009 přijala usnesení číslo 727, ve kterém uložila ministrům a vedoucím ústředních orgánů státní správy, aby od poloviny roku 2009 při obnově síťových prvků požadovali podporu IPv6 a do konce roku 2010 zajistili přístup ke službám eGovernmentu novým protokolem. Usnesení zároveň doporučuje hejtmanům a pražskému primátorovi postupovat obdobně.

Jak už to s usneseními bývá, v plnění jsou značné rezervy. Na podzim 2011 je dostupná po IPv6 necelá polovina ministerských webů. Nejsmutnější je jeho absence na ministerstvu vnitra, které má v gesci informatiku. eGovernment a jeho Portál veřejné správy jsou k máni stále jen po IPv4.

Mnohé státy se zkrátka snaží různými metodami posouvat rozvoj IPv6 vpřed, protože vnímají blížící se vyčerpání IPv4 adres a další problémy stávajícího protokolu jako ohrožení svého dalšího rozvoje. Bohužel zatím IPv6 pořád není v pozici, kdy by se prosazoval „samospádem“ a kdy by se do něj hrnuli uživatelé i poskytovatelé z toho prostého důvodu, že se jim to okamžitě vyplatí. Snad k jeho prosazení alespoň částečně přispěje i tato kniha.

## 1.8 Webové zdroje

Na webu pochopitelně najdete nepřehledné množství stránek věnovaných IPv6. Podívejme se na ty, které stojí za pozornost. „Oficiálním“ webem odkazovaným ze stránek IPv6 Fóra je *gogoNET*

www► <http://gogonet.gogo6.net/>

Je prezentován jako sociální síť a služby, jež mají profesionálům usnadnit cestu k IPv6. Jedná se o směs informací (dovedně skrytých pod položku *Interact*) a praktických nástrojů, protože pod hlavičku *gogo6* se přestěhovala služba *Freenet6* nabízející volné tunelované připojení k IPv6. Podrobněji se jí budu věnovat v kapitole 13 na straně 291. Z informačního obsahu stojí

určitě za pozornost instruktážní videa, prezentace a občas se objeví cenný text v blogu.

Významným a často odkazovaným zdrojem je také *The IPv6 Portal* na adrese

**WWW►** <http://www.ipv6tf.org/>

Obsahuje řadu informací, orientovaných zejména na evropské aktivity. Jeho jednoznačným kladem je, že zdejší novinky ze světa IPv6 jsou udržovány v aktuálním stavu již řadu let. Jeho autoři bohužel pravděpodobně nikdy neslyšeli o použitelnosti. Některé stránky se jeví jako prázdné, než si všimnete, že vpravo nahoře sídlí decentní podmenu, které vám zpřístupní jednotlivé zdejší sekce.

Trudnomyslným mohu doporučit web specializovaný na vyčerpání IPv4 adres

**WWW►** <http://www.ipv4depletion.com/>

Řadu materiálů (včetně multimediálních) najdete ve výstupech projektu *6DISS*. Postupně zastarávají, protože projekt skončil v září 2007, stále však představují použitelný a ucelený zdroj informací.

**WWW►** <http://www.6diss.org/>

Na domácí půdě to s relevantními informacemi také není nijak oslňující. Pravděpodobně nejlepším informačním zdrojem je web

**WWW►** <http://www.ipv6.cz/>

o jehož obsah se stará několik autorů, pocházejících zejména z pracovní skupiny IPv6 při sdružení CESNET. Pokud máte k dané problematice co říci, rádi Vás uvítáme mezi autory.