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.
Zikova 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

Pavel Satrapa

Internetový protokol verze 6

Třetí vydání

IPv6

Edice CZ.NIC

http://knihy.nic.cz/

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.

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 jím 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 nejpalčivějším je nedostatek adres, který pociťují 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 prázdnotou. 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

1 Úvod **17**
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

I Jak funguje IPv6 **33**

2 Formát datagramu **35**
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

3 Adresy v IPv6 **55**

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 Vícedomovci čili multihoming 88
3.14 Přidělování adres 91

4 ICMPv6 **97**

4.1 Chybové zprávy 99
4.2 Informační zprávy 101
4.3 Bezpečnostní aspekty ICMP 102

5 Objevování sousedů (Neighbor Discovery) **103**

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

6 Automatická konfigurace **119**

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

7 Směrování a směrovací protokoly **139**

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

8 Skupinové radovánky čili multicast **163**

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

9 Domain Name System **189**

9.1 IPv6 adresy v DNS 190

9.2 Obsah domén 193

9.3 Provozní záležitosti 195

10 IPsec čili bezpečné IP **199**

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

11 Mobilita **221**

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

12 Kudy tam **251**

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

II IPv6 v praxi 289

13 IPv6 na vlastní kůži 291
13.1 Lehké oťukávání 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

14 BSD 317
14.1 IPv6 v jádře 317
14.2 Konfigurace rozhraní 318
14.3 Konfigurace směrování 319
14.4 Přechodové mechanismy 320

15 Linux **323**

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

16 Microsoft Windows **331**

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

17 Cisco **345**

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

18 Směrovací programy **355**
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

19 Ohlašování směrovače **371**
19.1 Ohlašování – radvd 371
19.2 Likvidace „pirátských“ ohlášení – ramond 374

20 BIND **377**

21 Server pro DHCPv6 **381**
21.1 Dibbler 381
21.2 ISC DHCP 383
21.3 Určení DUID 387

III Přílohy **389**

A Rezervované adresy a identifikátory **391**
A.1 Skupinové adresy 391
A.2 Skupinové identifikátory 392
A.3 Výběrové adresy 392

B Specifikace IPv6 **393**

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

Literatura **399**

Rejstřík **401**

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 odesilateli)
- 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

vývoj

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

firem 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 beztřídní 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.

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

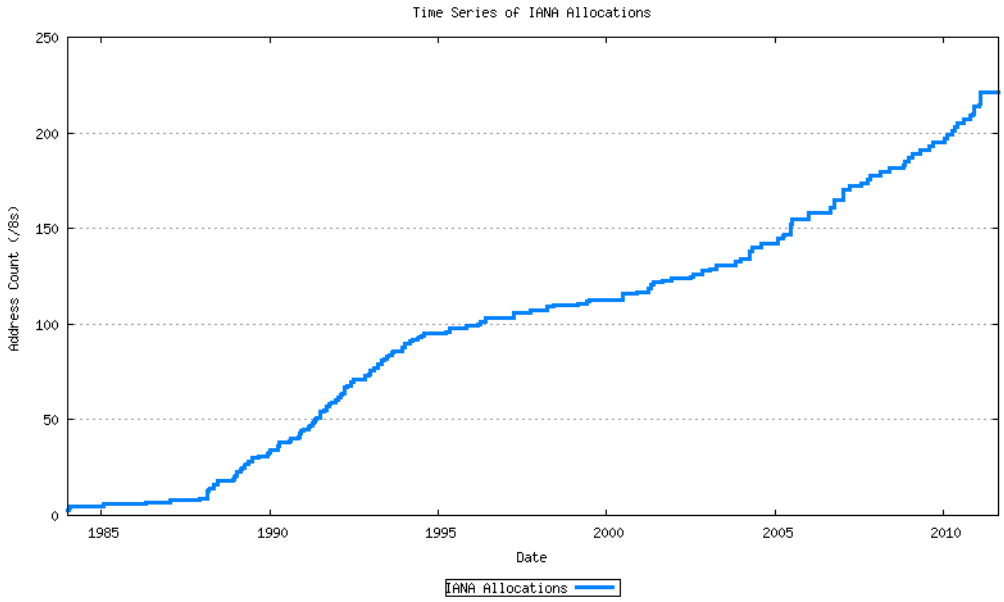
Tabulka 1.1: Pracovní skupiny IETF zapojené do vývoje IPv6

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 vyhlašována 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 *ipv4.potaroo.net* 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 neznamená, 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[1]. 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 nejzákladnější 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 přímočarost 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.

[1] 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 popsaný 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 pozitiva a sociální jistoty. Podívejme se na nejvýznamnější pihy 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 případu 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 dolaďují detaily. Nejisté výnosy[2] v kombinaci s nestabilními specifikacemi jsou silně odrazující pro všechny, kteří by chtěli nový protokol implementovat. Proto jim to šlo jako psovi pastva, 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

[2] 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 nějž 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, prodraží 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 oslňující, 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, jíž 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[3] 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 souvislostí. 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[4]. 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 téže oblasti je zavedení koncepce toku (proud souvisejících datagramů se spo-

[3] Mezi jinými servery Google, Facebook, Yahoo! a distribuční sítě Akamai a Limelight Networks.

[4] 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 směrovat, 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 odesilatelem 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 odesilateli, 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 nejzákladnější schopnosti a také výkonem často zaostávala za svým předchůdcem[5].

Postupem času se ale situace lepšila. 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_výrobce/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

[5] V počáteční fázi hadwarové 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 tématikou 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 sítě (NEMO)
- DHCPv6
- SIP
- SNMP
- multicast aneb MLDv2

- uživatelský agent IMS pro mobilní sítě (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*.

platforma	*kategorie*	*získáno*
FreeBSD (KAME)	hostitel	3/2006
	směrovač	3/2006
Cisco IOS 12.4(9)T	směrovač	4/2006
Linux 2.6.15	hostitel	5/2006
	IPsec konec	5/2006
Linux 2.6.20	směrovač	9/2007
	IPsec brána	10/2007
MS Windows Vista	hostitel	10/2007
	IPsec konec	1/2008
MS Windows Server 2008	hostitel	1/2008
	IPsec konec	3/2008
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 nejhlouběji 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 registrovánu 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[6].

[6] 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 kursy nebo osoby, a to jak pro pozici IPv6 odborníků (Engineer), tak jeho šiřitelů (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 sítě, 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 sítě. Skládala se z lokálních IPv6 sítí, navzájem propojených tunely. To znamená, že IPv6 datagramy se balily jako data do běžného IPv4 a přenášely se standardním Internetem až do cílové sítě. 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 sítě 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 přidělovál části připojeným sítím. Směrovače poskytovatelů disponujících pTLA zároveň tvořily páteř sítě *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[7].
- 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[8]. Mimo jiné požaduje, aby projekty financované ze 7. rámcového programu

[7] 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.

[8] 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 stimulující 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 mání 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 nepřeberné 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.

I

Jak funguje IPv6

2 Formát datagramu

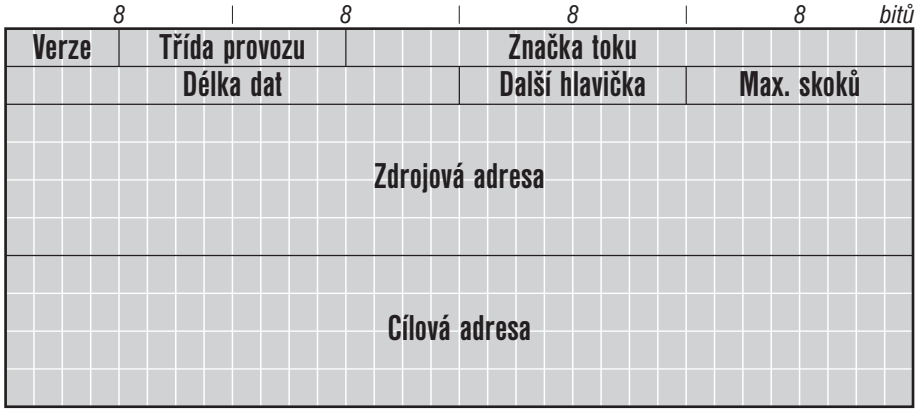
Základním kamenem IPv6 je dokument RFC 2460: *Internet Protocol, Version 6 (IPv6) Specification*, který obsahuje především formát datagramu. Ostatním mechanismům a datovým formátům, které souvisejí s IPv6, jsou věnovány další RFC specifikace.

2.1 Datagram

Datagram má v IPv6 obvyklý základní tvar: začíná hlavičkami, za kterými pak následují nesená data. V porovnání s IPv4 však došlo v hlavičkách ke koncepční změně. Dříve byla jejich délka proměnlivá a jednotliví účastníci komunikace mohli připojovat další nepovinné volby podle potřeby. Hlavička obsahovala kontrolní součet, který bylo třeba znovu vypočítat na každém směrovači, jímž datagram prošel (protože se změnila přinejmenším položka TTL).

IPv6 naproti tomu standardní hlavičku minimalizovalo a omezilo její prvky jen na ty nejnutnější. Tato základní hlavička má konstantní velikost. Veškeré doplňující, nepovinné či příležitostně užívané údaje byly přesunuty do rozšiřujících hlaviček, které v datagramu mohou a nemusí být přítomny. Jejich podobu a zpracování popíši v následující části.

Tvar základní hlavičky vidíte na obrázku 2.1. Přestože se adresy odesilatele a příjemce prodloužily čtyřikrát, celková délka základní hlavičky datagramu vzrostla ve srovnání s IPv4 jen dvojnásobně (z 20 B na 40 B, z toho 32 B zabírají adresy). Minimalismus je patrný na první pohled.



Obrázek 2.1: Základní hlavička datagramu

verze Položka *Verze (Version)* je obvyklým zahájením IP datagramu, které identifikuje verzi protokolu. Zde obsahuje hodnotu 6.

třída provozu Za ní následuje osmibitová *Třída provozu (Traffic class)*, která vyjadřuje prioritu datagramu či jeho zařazení do určité přepravní třídy. Cílem je, aby tato položka umožnila IP poskytovat služby se zaručenou kvalitou. V praxi ale tak daleko nejsme a v nejbližší době ani nebudeme. IP, a to ani ve verzi 6, neumí zaručit dopravní parametry, jako jsou přenosová rychlost, zpoždění či jeho rozptyl. Dovede však poskytovat tak zvané *diferencované služby (differentiated services, diffserv)*. Jejich prostřednictvím mohou mít datagramy různé priority a odlišné způsoby zacházení, které vedou k jejich přednostnímu zpracování či naopak odkládání až po ostatních. Právě diferencované služby využívají pro přenos svých informací položku *Třída provozu*. Ve vlastní definici IPv6 není nijak blíže upřesněna, pouze se zde požaduje, aby implicitní hodnotou byla nula.

značka toku Dalších 20 bitů je věnováno *Značce toku (Flow label)*. Koncepce toku je novinkou v IPv6 a stejně jako třída provozu zatím není přesně definována. V zásadě by jako tok měl být označován proud datagramů se společnými vlastnostmi (odesilatel, adresát, požadavky na vlastnosti spojení). Prostřednictvím identifikátoru (značky) směrovač rychle rozpozná, že datagram je součástí určitého toku, což mu usnadní rozhodování o jeho dalším osudu (bude s ním naloženo stejně, jako s předchozími členy téhož toku). Jak již bylo řečeno, jedná se stále o experimentální půdu a nic moc konkrétního zatím nebylo stanoveno. K tématu se vrátím v části 2.9 na straně 51.

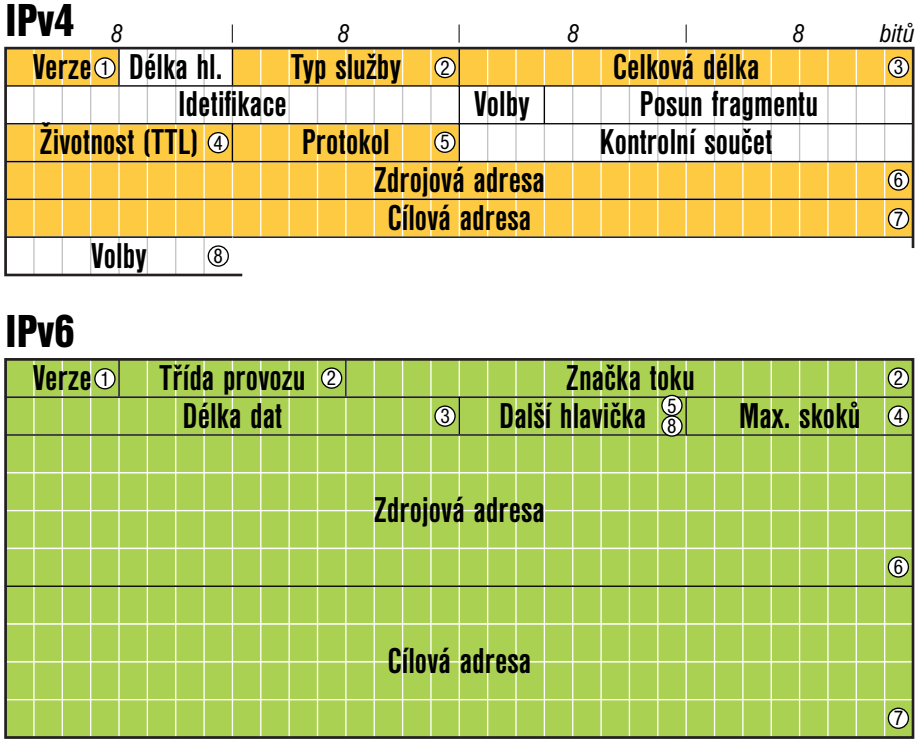
délka dat *Délka dat (Payload length)* nese údaj o délce datagramu. Přesně řečeno počet bajtů následujících za standardní hlavičkou. Z toho plyne, že základní hlavička se do této délky nepočítá, zatímco případné rozšiřující hlavičky ano. Jelikož je položka dvoubajtová, je maximální délkou 64 KB. Pokud je třeba vytvořit delší datagram, lze použít rozšiřující hlavičku *Jumbo obsah* popsanou v části 2.7 na straně 49.

další hlavička *Další hlavička (Next header)* obsahuje identifikaci, jaká hlavička či jaký druh dat následuje za standardní hlavičkou. Podrobněji se jí budu věnovat zanedlouho v části 2.2.

dosah *Maximální počet skoků (Hop limit)* je náhradníkem dřívější životnosti datagramu (TTL). Průchod datagramu jedním směrovačem je považován za jeden skok. Odesilatel v této položce uvede, kolik takových skoků smí datagram maximálně absolvovat. Každý směrovač po cestě pak sníží hodnotu o jedničku. Dojde-li tím k vynulování položky, datagram bude zlikvidován a odesilateli se pošle ICMP zpráva o vypršení maximálního počtu skoků. Smyslem omezení je ochrana proti cyklům při směrování (zacyklený datagram nebude v síti strašit do nekonečna).

adresy Závěrečnými dvěma položkami je dvojice IPv6 adres: *Zdrojová adresa (Source address)* a *Cílová adresa (Destination address)*. Vzhledem k délce

adresy v IPv6 zabírají tyto dvě položky 80 % rozsahu celé hlavičky. Podrobnosti o adresování se dočtete v kapitole 3 na straně 55.



Obrázek 2.2: Porovnání hlaviček IPv4 a IPv6

Při srovnání s IPv4 je nejnápadnější absence tří informací: rozšiřujících voleb, kontrolního součtu a fragmentace. Rozšiřující volby byly nahrazeny obecnějším principem zřetězení doplňkových hlaviček. Obdobně údaje související s fragmentací byly přesunuty do těchto rozšiřujících hlaviček. Zdaleka ne každý paket je totiž fragmentován a lze očekávat, že v IPv6 bude fragmentace ještě vzácnější než v současnosti. IPv6 totiž požaduje, aby infrastruktura pro jeho přenos dovedla přenášet pakety minimálně o délce 1280 B (MTU). Vzhledem k tomu, že drtivá většina koncových zařízení je dnes připojena prostřednictvím různých variant Ethernetu s MTU 1500 B, lze očekávat, že tato maximální velikost paketů se usídlí téměř všude a fragmentace prakticky zmizí ze světa.

Kontrolní součet zmizel bez náhrady. Tuto službu typicky vykonává nižší vrstva síťové architektury (např. zmiňovaný Ethernet), takže na úrovni IP by se jen opakovalo její snažení. Vzhledem k tomu, že hlavička se mění v každém směrovači (klesá dosah datagramu), znamenalo by to zbytečné zpomalování.

Porovnání hlaviček IPv4 a IPv6 názorně představuje obrázek 2.2. V IPv4 datagramu jsou vybarveny položky, které byly (zpravidla v poněkud pozměněné podobě) převzaty do IPv6. Stejná čísla označují položky, které si navzájem odpovídají.

2.2 Zřetězení hlaviček

IP verze 6 používá odlišný způsob reprezentace rozšiřujících hlaviček než jeho předchůdce. Každá hlavička je nyní samostatným blokem a k jejich vzájemnému propojení slouží položka *Další hlavička (Next header)*. Kód v ní obsažený identifikuje, jakého typu je hlavička, která následuje za tou stávající. Každá rozšiřující hlavička začíná položkou *Další hlavička*. Prostřednictvím těchto hodnot lze za sebe zřetězit hlaviček, co hrdlo ráčí.

Poslední z nich obsahuje v položce *Další hlavička* typ dat, která datagram nese. Hodnota položky *Další hlavička* tak zároveň zastupuje dřívější položku *Protokol*. Nejvýznamnější hodnoty shrnuje tabulka 2.1. Aktuální a kompletní specifikaci hodnot pro typy přenášených dat najdete na adrese

www► *http://www.iana.org/assignments/protocol-numbers*

.

Rozšiřující hlavičky	
0	volby pro všechny (hop-by-hop options)
43	směrování (routing)
44	fragmentace (fragment)
50	šifrování obsahu (ESP)
51	autentizace (AH)
59	poslední hlavička (no next header)
60	volby pro cíl (destination options)
135	mobilita (mobility)
Typ nesených dat (protokol)	
6	TCP
8	EGP
9	IGP
17	UDP
46	RSVP
47	GRE
58	ICMP

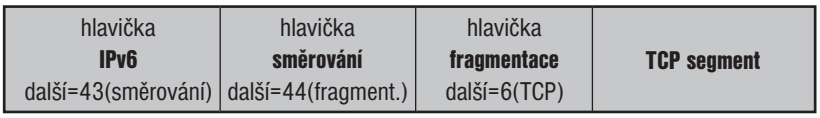
Tabulka 2.1: Vybrané hodnoty položky *Další hlavička*

Pokud tedy datagram neobsahuje žádné rozšířené hlavičky, bude přímo jeho základní IPv6 hlavička obsahovat jako *Další hlavičku* identifikátor typu nesených dat. Tuto situaci ilustruje obrázek 2.3a. Na obrázcích 2.3b

a 2.3c můžete sledovat, jak se změní obsah položek *Další hlavička*, když datagramu přidáme rozšiřující hlavičky *Směrování* a *Fragmentace*.

a) bez rozšiřujících hlaviček

b) s hlavičkou *Směrování*



c) s hlavičkami *Směrování* a *Fragmentace*

Obrázek 2.3: Zřetězení hlaviček datagramu

Hlavními devizami koncepce hlaviček v IPv6 je pružnost a úspornost. Součástí datagramu jsou jen ty průvodní informace, které skutečně potřebuje. Rubem mince je, že zpracování kompletních hlaviček může představovat průchod relativně dlouhým řetězcem. Pokud by se mělo odehrávat v každém směrovači na cestě mezi odesilatelem a příjemcem, mohlo by to vést k nezanedbatelné degradaci výkonu.

pořadí hlaviček

Tento problém řeší IPv6 velmi jednoduše – rozšiřující hlavičky mají předepsáno následující pořadí:

1. základní hlavička IPv6
2. volby pro všechny (hop-by-hop opions)
3. volby pro cíl (destination options) – pro první cílovou adresu datagramu a případné další uvedené v hlavičce *Směrování*
4. směrování (routing)
5. fragmentace (fragment)
6. autentizace (authentication)
7. šifrování obsahu (encapsulating security payload)
8. volby pro cíl (destination options) – pro konečného příjemce datagramu
9. mobilita (mobility)

Jeho cílem je, aby se informace zajímavé pro uzly, kterými datagram prochází, ocitly vpředu a hlavičky určené až pro koncového příjemce následovaly teprve za nimi. Pro průchozí směrovač jsou potenciálně zajímavé jen *Volby pro všechny*, které se smí vyskytnout jen bezprostředně za základní hlavičkou. Ničeho jiného si nemusí všímat. Jakmile vidí v *Další hlavičce* jiný kód než 0 (*Volby pro všechny*), ví, že může s analýzou datagramu skončit.

Ostatní rozšiřující hlavičky jsou zajímavé jen pro adresáta datagramu – ať už průběžného (pocházejícího z hlavičky *Směrování*) či koncového. Průběžného adresáta zajímají jen první tři (volby pro všechny, volby pro cíl a směrování), zatímco koncového se týkají všechny. Podle RFC 2460 adresát musí být schopen se vyrovnat s libovolným pořadím hlaviček, nicméně důrazně se doporučuje dodržovat výše uvedené.

Každá z rozšiřujících hlaviček by se měla objevit nanejvýš jednou. Výjimkou jsou volby pro cíl, které se mohou vyskytnout dvakrát – jednou před *Směrováním* a podruhé před *Mobilitou*.

Speciální význam má, pokud položka *Další hlavička* obsahuje hodnotu 59 (no next header). Ta signalizuje, že se jedná o poslední hlavičku, za kterou již nenásleduje vůbec nic. Pokud datagram podle své délky obsahuje ještě nějaká data, musí být ignorována. Je-li datagram přeposílán dále, musí do něj předávající tato data zkopírovat beze změny.

Podívejme se nyní podrobněji na tvar a význam jednotlivých rozšiřujících hlaviček.

2.3 Volby

Stávající IPv6 zavádí dvě hlavičky obsahující volby: *Volby pro všechny* (*hop-by-hop options*, *Další hlavička* před nimi má hodnotu 0) a *Volby pro cíl* (*destination options*, předcházející *Další hlavička* má hodnotu 60).

Obě hlavičky mají společný tvar, který najdete na obrázku 2.4. Význam položky *Další hlavička* jsem již vysvětlil. *Délka dat* obsahuje délku hlavičky v osmicích bajtů. Do délky se nepočítá prvních 8 bajtů, takže pokud má hodnotu 1, znamená to, že celá hlavička s volbami měří 16 B.

Obrázek 2.4: Rozšiřující hlavičky *volby pro všechny* a *volby pro cíl*

Položka *Volby* pak obsahuje vlastní volby. Ty mohou být zavedeny jako součást jednotlivých konkrétních mechanismů. Například v rámci podpory mobilních počítačů se objevila volba *Domácí adresa*. Samotná definice IPv6

obsahuje jen dvě: *Pad1* a *PadN*. Slouží ke vkládání „vaty“ – volného místa, které má sloužit k lepšímu zarovnání ostatních prvků s přihlédnutím k hranicím čtyřbajtových slov. Jedná se o vycpávky, které nenesou žádnou aktivní informaci. Přehled doposud definovaných voleb najdete v tabulkách 2.2 a 2.3.

Typ	*Význam*	*Strana*
0	Pad1	41
1	PadN	41
5	Upozornění směrovače	42
38	Rychlý start	50
194	Jumbo obsah	49

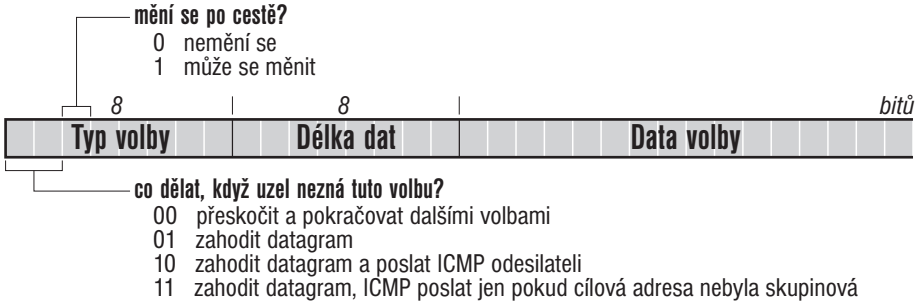
Tabulka 2.2: Volby pro všechny

Typ	*Význam*	*Strana*
0	Pad1	41
1	PadN	41
201	Domácí adresa	237

Tabulka 2.3: Volby pro příjemce

Pad1 *Pad1* vynechává 1 bajt. Tvar této volby je triviální: jedná se o jeden bajt s hodnotou 0, která identifikuje typ volby a zároveň říká, že to je vše.

PadN *PadN* umožňuje vynechat dva a více bajtů. První bajt opět určuje typ volby a má hodnotu 1. Za ním následuje jeden bajt obsahující délku volby, do níž se první dva bajty nepočítají. Následují data uvedené délky, jejichž hodnoty jsou nulové. Chcete-li tedy vynechat celkem 6 bajtů, bude mít *Délka dat* hodnotu 4 a za ní budou následovat čtyři nulové bajty „dat“.



Obrázek 2.5: Tvar voleb pro rozšiřující hlavičky

formát voleb

Všechny volby musí dodržovat jednotný tvar. Odpovídá tomu, který jste viděli u volby *PadN*. První bajt identifikuje, o jakou volbu se jedná. Za ním pak následuje *Délka dat* (do níž se nepočítají první dva bajty) a po ní data. Jejich strukturu musí definovat dokument, který zavede danou volbu.

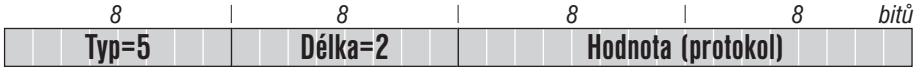
V rámci *Typu volby* byl pevně předepsán význam nejvyšších tří bitů. První dva určují, co se stane s datagramem, pokud zpracovávající uzel dotyčnou volbu nezná. Za nimi následuje bit, který indikuje, zda se volba může měnit během průchodu sítí. Konkrétní hodnoty najdete v obrázku 2.5.

upozornění směrovače

Jednou z „opravdových“ voleb je tak zvané *Upozornění směrovače (router alert)* definované v RFC 2711. Jedná se o volbu pro všechny, která má za cíl upozornit každý směrovač po cestě, že tento paket nese data, která by jej mohla zajímat.

Volba najde uplatnění například v rezervačním protokolu RSVP, který posílá řídicí pakety pro alokaci kapacit po cestě. Tyto pakety jsou určeny všem směrovačům. Právě *Upozornění směrovače* může napovědět, že paket nese zajímavou informaci. Bez něj by směrovač musel prohlížet všechny datagramy a zkoumat, jakému protokolu vyšší vrstvy patří. Když by narazil na RSVP paket, zabýval by se jím podrobněji. V opačném případě by jej poslal dále po cestě k cíli.

Díky *Upozornění směrovače* lze rychle odlišit datagramy potenciálně zajímavé od těch, které se mají prostě předávat dál. Formát volby najdete na obrázku 2.6. Obsahuje vlastně jedinou položku, která slouží k identifikaci protokolu, jehož data nese. Dosud definované hodnoty shrnuje tabulka 2.4.



Obrázek 2.6: Volba *Upozornění směrovače*

Hodnota	*Význam*
0	obsahuje MLD zprávu
1	obsahuje RSVP zprávu
2	obsahuje zprávu *Aktivní sítě*
3	rezervováno
4–35	úroveň vnoření agregovaných rezervací (RFC 3175)
36–67	úroveň agregací QoS NSLP (RFC 5974)
68	NSIS NATFW NSLP (RFC 5973)

Tabulka 2.4: Definované *Hodnoty* pro volbu *Upozornění směrovače*

Aby tato volba přinášela nějaký efekt, musí odpovídající protokol nařizovat její použití. Směrovač má právo ignorovat obsah všech datagramů, které

nejsou adresovány jemu a neobsahují *Upozornění směrovače*. Chce-li určitý protokol získat jeho pozornost, musí k datagramu přihodit tuto volbu.

Upozornění směrovače s sebou nese i určitá bezpečnostní rizika. Jejich rozbor, ale zejména doporučení pro operátory sítí, jak s datagramy nesoucími tuto volbu zacházet, najdete v RFC 6398: *IP Router Alert Considerations and Usage*.

2.4 Směrování

Standardně je datagram směrován podle své cílové adresy. Hlavička *Směrování (Routing)* umožňuje do tohoto procesu zasáhnout a předepsat jeden či několik bodů (IPv6 adres), jimiž musí datagram projít před doručením adresátovi. Motivace pro takové chování jsou různé, jak zanedlouho uvidíte.

IPv6 ponechává prostor pro zavedení různých typů směrovacích hlaviček. K jejich rozlišení slouží hodnota položky *Typ směrování*. Zatím byly definovány dva přesně popsané typy (0 a 2) a dva volné typy (hodnoty 253 a 254) určené pro experimentování se směrovacími mechanismy. Další informace o experimentálních typech najdete v RFC 4727, zde si jimi nebudu zabývat.

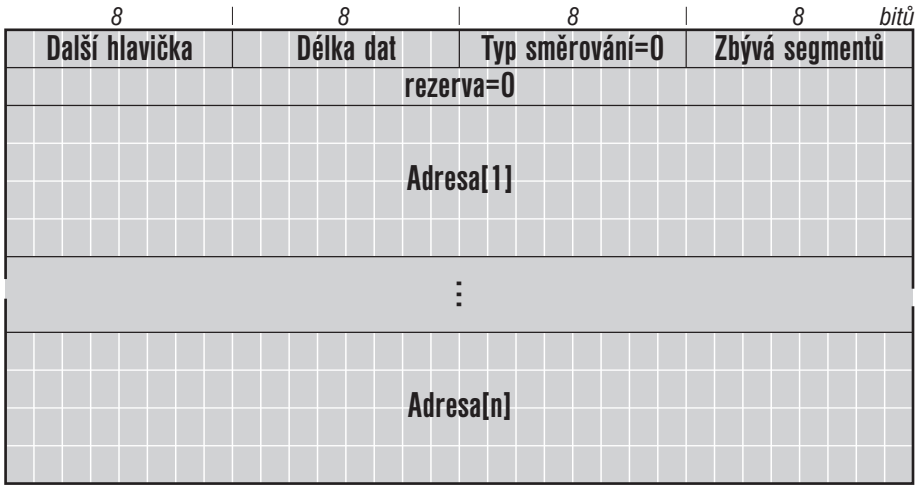
směrování typu 0

Typ 0 je starší, byl zaveden přímo v RFC 2460 jako součást definice jádra IPv6. Umožňuje předepsat datagramu určité body, kterými musí v daném pořadí projít. Zároveň slouží jako záznam, kterými z nich již prošel. Tyto „průchozí body“ nemusí následovat bezprostředně za sebou, mezi každými dvěma může datagram projít libovolným počtem směrovačů. Podobnou rozšiřující volbu nabízí i IPv4.

Formát hlavičky *Směrování* typu 0 představuje obrázek 2.7. Pokud chce odesilatel, aby jeho datagram po cestě k cíli prošel určitými uzly, uvede jako jeho cílovou adresu IP adresu prvního z těchto průchozích uzlů. Do hlavičky *Směrování* pak zapíše postupně adresy zbývajících a na závěr konečný cíl datagramu. V položce *Zbývá segmentů* uvede jejich počet.

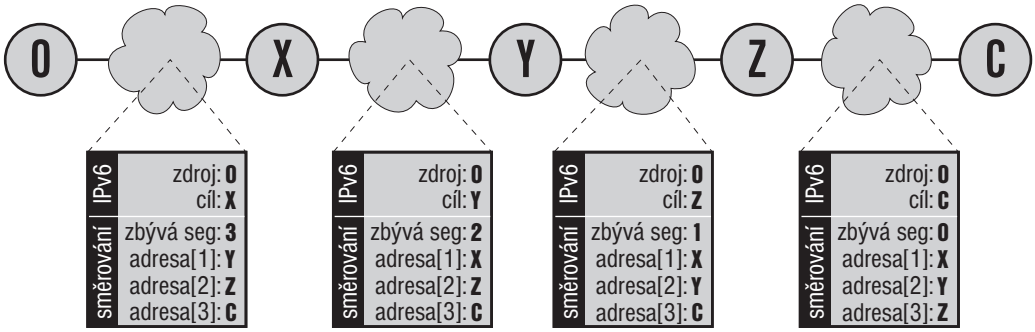
Když datagram dorazí na cílovou adresu uvedenou v základní IPv6 hlavičce a obsahuje hlavičku *Směrování* s nenulovým počtem zbývajících segmentů, vezme počet zbývajících segmentů jako index do tabulky průchozích adres. Určuje, kolikátá od konce je adresa následujícího průchozího bodu. Tuto adresu zapíše jako cílovou do základní hlavičky a dosavadní cílovou (tedy svoji) uloží místo ní do směrovací hlavičky. Následně zmenší počet zbývajících segmentů o jedničku a pošle datagram novému cíli (dalšímu na vytyčené cestě).

Položka *Zbývá segmentů* tedy odděluje, které z uvedených adres již byly navštíveny a kterými datagram ještě musí projít. Je-li nulová, znamená to, že datagram dorazil do svého cíle.



Obrázek 2.7: Rozšiřující hlavička *Směrování* typu 0

Obrázek 2.8 ilustruje vývoj hodnot zajímavých položek při průchodu datagramu sítí. Jeho odesilatelem je *O* a koncovým adresátem *C*. Odesilatel předepsal, že datagram má projít uzly *X*, *Y* a *Z*.



Obrázek 2.8: Změny v hlavičkách datagramu

Směrovací hlavička typu 0 byla zavedena především pro testování dosažitelnosti mezi libovolnými adresami. Můžete v ní předepsat, odkud kam se mají datagramy dopravit a tedy ověřit funkčnost spojení. Mimo jiné jí to dává schopnost projít NATem na neveřejnou adresu – jednoduše lze uvést jako koncový cíl neveřejnou adresu uzlu a jako mezilehlou veřejnou adresu jeho NATu. To může být přínosné pro některé aplikace, zároveň je však

tato vlastnost vnímána jako nebezpečná[1]. Podobně může přispět k ošizení firewallu a proniknutí jeho ochranou.

V roce 2007 byl široce diskutován jiný problém, který nakonec vedl k odmítnutí směrovací hlavičky typu 0. Může totiž posloužit k útokům usilujícím o zahlcení přenosových tras. Útočník díky ní může nechat přepravovat datagramy sítí sem a tam. A když navíc použije několik směrovacích hlaviček napěchovaných po okraj, může se datagram potulovat sítí velmi dlouho. Série takových datagramů dokáže v síti vytvořit datové toky s objemem mnohonásobně převyšujícím kapacitu útočníkova připojení[2], navíc i na velmi dlouhé trase.

Důsledkem bylo RFC 5095: *Deprecation of Type 0 Routing Headers in IPv6*. Podle něj je cílový IPv6 uzel, který obdržel datagram s hlavičkou *Směrování* typu 0, povinen ji ignorovat, pokud je počet zbývajících segmentů nulový. Je-li nenulový, musí datagram zahodit a ohlásit jej odesilateli jako chybný. Kromě toho se zde doporučuje datagramy s tímto typem hlavičky *Směrování* filtrovat na aktivních prvcích.

směrování typu 2

Typ 2 byl definován speciálně pro mobilitu. De facto se jedná o silné zjednodušení obecnějšího typu 0. Když je mobilní uzel na cestách, má kromě své původní pevné adresy i adresu dočasnou, jež se mění podle sítě, ve které se právě nachází. Pokud přechází mezi buňkami, může se dočasná adresa během komunikace měnit. Aby nebyla narušena komunikace běžících programů, používá pro ni svou trvalou, tak zvanou domácí adresu.

Jeho partner pomocí směrovací hlavičky typu 2 stanoví, že koncovou adresou je pevná adresa mobilního uzlu, ale má se nejprve dopravit na jeho dočasnou adresu. Čili datagram je dopraven na aktuální dočasnou adresu, tam se postupem podobným směrování typu 0 nahradí cílová adresa hodnotou ze směrovací hlavičky a vyšším komunikačním vrstvám se data doručí, jako by přišla na trvalou adresu.

Směrovací hlavička typu 2 proto umožňuje uložit jen jedinou adresu (domácí adresu mobilního uzlu, jemuž je datagram určen). To výrazně omezuje její zneužitelnost. Formát této směrovací hlavičky najdete na obrázku 11.16 na straně 237 v kapitole o mobilitě, kde se dočtete i podrobnější informace o jejím fungování.

2.5 Fragmentace

Každá z podřízených technologií, které IPv6 používá pro přepravu svých datagramů, má jistou maximální velikost paketů, které dokáže přenášet. Tato konstanta se označuje zkratkou MTU (Maximum Transmission Unit). Například nejpopulárnější Ethernet má MTU = 1500 B.

[1] Stále se sice zdůrazňuje, že NAT *není* bezpečnostní prvek, ale stejně je tak částečně vnímán.
[2] Prakticky byl předveden 88násobek.

Cílem fragmentace je umožnit IPv6 přepravovat datagramy větší, než je MTU používaných technologií. Základní myšlenka je prostá: odesilatel rozloží datagram do několika dostatečně malých částí a příjemce z nich poskládá původní datagram.

odlišnosti IPv4

Analogickou techniku používal i protokol IPv4, lišil se však v několika důležitých detailech. Zatímco v IPv4 mohl datagram fragmentovat libovolný směrovač po cestě (kdykoli měl být odeslán linkou, jejíž MTU bylo menší než velikost datagramu), *v IPv6 fragmentuje výlučně odesilatel*. Pokud má některý ze směrovačů odeslat datagram linkou s nedostačujícím MTU, zahodí jej a pošle odesilateli ICMP zprávu „příliš velký paket“, jejíž součástí je i MTU, které tento stav způsobilo. Druhou odlišností je, že zatímco IPv4 má všechny podklady pro fragmentaci zařazeny již do standardní hlavičky, IPv6 pro ni používá hlavičku rozšiřující a spíše se snaží, aby k fragmentaci vůbec nedocházelo.

formát hlavičky

Rozšiřující hlavička *Fragmentace (Fragment)* je identifikována kódem 44 v položce *Další hlavička* svého bezprostředního předchůdce. Její tvar vidíte na obrázku 2.9. Velikost je konstantní a kromě obvyklé *Další hlavičky* obsahuje tři informační položky.

Obrázek 2.9: Rozšiřující hlavička *Fragmentace*

Identifikace (Identification) slouží k rozpoznání, které fragmenty patří k sobě. Jedná se o 32bitové celé číslo, které je v rámci dané dvojice odesilatel–příjemce pokud možno jednoznačné (každý další fragmentovaný datagram má číslo o jedničku vyšší než předchozí, po naplnění kapacity čítače se začne znovu od nuly). *Posun fragmentu (Fragment offset)* říká, kam tento fragment patří. Jednotkou jsou osmice bajtů od začátku fragmentovatelné části původního datagramu (viz níže). A konečně příznak *M (More fragments)* signalizuje, zda je tento fragment poslední (hodnota 0) nebo za ním následuje další (hodnota 1).

fragmentovatelná a nefragmentovatelná část

Má-li dojít k fragmentaci, vymezí se v původním datagramu dvě části: na začátku je tak zvaná *nefragmentovatelná část*, kterou tvoří standardní IPv6 hlavička a všechny po ní následující rozšiřující hlavičky až po *Směrování* (včetně). Tedy vše, co v pořadí rozšiřujících hlaviček předchází před fragmentací. Zbytek datagramu je považován za *fragmentovatelnou část* a pouze on je předmětem fragmentace.

postup fragmentace

Tato fragmentovatelná část se rozdělí na úseky, jejichž velikost je násobkem osmi bajtů a je dostatečně malá na to, aby celková velikost výsledných

datagramů nepřekročila požadované MTU. Tím z původního datagramu vznikne několik fragmentů – nových datagramů. Jejich hlavičky jsou sestaveny takto:

- Převezme se nefragmentovatelná část původního datagramu. Jedinými změnami, které se v ní pro jednotlivé fragmenty provedou, je úprava velikosti v základní hlavičce, aby odpovídala skutečné velikosti fragmentu, a změna hodnoty poslední *Další hlavičky* na 44.
- Za ni se přidá rozšiřující hlavička *Fragmentace*, jejíž hodnoty se naplní následovně:
  - vygeneruje se nový *Identifikátor* paketu a tato hodnota se přidělí všem jeho fragmentům
  - hodnota *Další hlavičky* se převezme z poslední *Další hlavičky* nefragmentovatelné části původního datagramu
  - *Posun* každého fragmentu se určí jako počet osmic bajtů, o které je jeho začátek vzdálen od začátku fragmentovatelné části původního datagramu; jelikož všechny fragmenty (kromě posledního) budou mít stejnou délku *x*, bude mít první fragment *Posun* nulový, druhý fragment ponese *Posun*=*x*, třetí *Posun*=2*x* atd.
  - poslednímu fragmentu se příznak *M* nastaví na 0, ostatním na 1
- Na konec se připojí dotyčný fragment (úsek fragmentovatelné části původního datagramu).

původní datagram – 1500 B

základní hlavička (40 B) Délka=1460, Další hl.=17	**data (1460 B)**

po fragmentaci – 1280 a 276 B

základní hlavička (40 B) Délka=1240, Další hl.=44	**fragmentace (8 B)** Další hl.=17, Posun=0, M=1, ID=X	**data 1 (1232 B)**

základní hlavička (40 B) Délka=236, Další hl.=44	**fragmentace (8 B)** Další hl.=17, Posun=1232, M=0, ID=X	**data 2 (228 B)**

Obrázek 2.10: Fragmentace datagramu

Příklad celého postupu vidíte na obrázku 2.10. Odeslání datagramu o velikosti 1500 B skončilo příchodem ICMP zprávy ohlašující překročení MTU s hodnotou 1280 B. Dojde tedy k rozdělení původního paketu do dvou

fragmentů, hodnoty podstatných položek v hlavičkách jsou v obrázku uvedeny.

Vzniklé fragmenty jsou jako samostatné datagramy odeslány adresátovi. Ten je posbírá a z údajů ve fragmentační hlavičce dokáže složit původní datagram: podle *Identifikátoru* pozná, které fragmenty patří k sobě, pomocí *Posunutí* určí správné pořadí a v kombinaci s *Délkou dat* zjistí případné chybějící části a konečně příznak *M* mu prozradí, zda má k dispozici všechny kousky.

Na základě těchto údajů příjemce poskládá původní datagram do podoby, kterou měl před fragmentací (tím zaniknou hlavičky *Fragmentace* jednotlivých částí) a ten pak dále zpracovává bez ohledu na to, že mu přišel po kouskách.

2.6 Velikost datagramů

Fragmentace těsně souvisí s velikostí odesílaných datagramů. Každý datagram navíc přináší určitou (byť malou) zátěž – musí mít své hlavičky, směrovače po cestě se musí rozhodovat, kudy jej poslat, a podobně. Ideálem je, aby datagramy byly pokud možno co největší, aby jich bylo co nejméně a snižovala se tak nadbytečná zátěž. Na druhé straně však datagramy musí být natolik malé, aby nikde po své cestě nepřekročily MTU a nedocházelo tudíž k fragmentaci.

objevování MTU cesty

O dosažení tohoto kompromisu se snaží algoritmus nazvaný objevování MTU cesty. Definuje jej RFC 1981: *Path MTU Discovery for IP version 6*.

Z pohledu teoretika nemá vůbec smysl mluvit o nějakých cestách v souvislosti s protokolem IP. Nabízí službu bez spojení, kdy je každý datagram směrován samostatně a nezávisle na ostatních. To znamená, že každý ze skupiny datagramů tvořících jeden soubor může dorazit k cíli jinou cestou. V praxi se však směrovací tabulky nemění příliš rychle a je vysoce pravděpodobné, že datagramy odeslané v krátkém časovém intervalu ke stejnému cíli budou putovat stejnou trasou. Na tomto pozorování ostatně stojí již letitý program *traceroute*.

Objevování MTU cesty má za cíl najít maximální velikost paketu, který lze poslat danému cíli. Postupuje jednoduše: nejprve pošle datagram, jehož velikost je rovna MTU rozhraní, kterým datagram odesílá. Celkové MTU jistě nemůže být větší. Pokud datagram úspěšně dojde, máme nalezeno MTU cesty.

Jestliže někde narazí na úsek s menším MTU, směrovač na jeho začátku datagram zahodí a pošle odesilateli ICMP zprávu „příliš velký datagram“. Její součástí je i hodnota MTU dotyčné linky. Odesilatel si příslušně zmenší svůj odhad MTU cesty a zkusí štěstí znovu s datagramem této velikosti. Celý proces se opakuje tak dlouho, dokud se datagramy nedostanou až k cíli.

Informace o MTU cesty bývá využívána například v protokolu TCP, který jí přizpůsobí velikost odesílaných segmentů a snaží se tak předcházet jejich fragmentaci.

Pokud komunikace trvá delší dobu, s vysokou pravděpodobností dojde ke změně cesty, případně i několikanásobné. Hledání MTU se snaží s touto skutečností vyrovnat. Pokud MTU cesty poklesne, odesilatel na to přijde hned – obdrží ICMP zprávu o příliš velkém datagramu. O případném zvětšení se však touto cestou nedozví. Proto by měl čas od času zopakovat celý algoritmus hledání MTU, aby zjistil, zda aktuální hodnota není vyšší, než se domnívá. V RFC se požaduje, aby interval mezi těmito zkouškami byl minimálně 5 minut, doporučená hodnota je 10 minut.

Ostatně vzhledem k tomu, že MTU na linkách podporujících IPv6 má být alespoň 1280 B a doporučuje se používat 1500 B nebo více, lze očekávat, že MTU cesty bude zpravidla 1500 B a prakticky se nebude měnit. Klient nesmí zmenšit MTU cesty pod 1280 B. Pokud mu někdo ohlásí nižší hodnotu, musí datagramy fragmentovat.

Objevování MTU cesty lze používat i pro skupinové adresy. V tomto případě může dostat na jeden datagram celou řadu ICMP zpráv. Bude se chovat podle očekávání – použije nejmenší ohlášenou hodnotu.

Implementace popsaného algoritmu je autory IPv6 důrazně doporučena, není však povinná. Jedná-li se o minimalistickou implementaci IPv6 (např. v ROM přenosného zařízení), může používat hodnotu 1280 B, aniž by se pokoušela zjistit, zda skutečné MTU cesty není vyšší.

2.7 Jumbogramy

Jelikož je délka nesených dat v IPv6 datagramu ukládána do 16bitové položky, je maximální dosažitelnou hodnotou 65 535 bajtů. Troufám si tvrdit, že případy, kdy by tento horní limit byl pociťován jako omezení, budou opravdu velmi velmi vzácné. Nicméně i pro ně nabízí IPv6 řešení. Jedná se o volbu *Jumbo obsah (Jumbo payload)*, která umožňuje vytvářet datagramy o délce 65 536 až 4 294 967 295 B. Patří mezi *Volby pro všechny*, takže se jí bude zabývat každý směrovač po trase.

Použití je prosté: *Délka dat* v základní hlavičce se vynuluje a přidá se rozšiřující hlavička s volbami pro všechny obsahující *Jumbo obsah*. Nese položku *Délka jumbo dat (Jumbo payload length)*, která měří 32 bitů a umožňuje proto výše uvedený rozsah přípustných hodnot. Takto velké datagramy jsou označovány jako jumbogramy.

Použití jumbogramů má pochopitelně smysl jen v případě, kdy linková technologie umožňuje přenos takto velkých paketů. Jinými slovy pokud MTU dotyčné linky přesahuje 65 575 (maximální velikost nesených dat plus IPv6

Obrázek 2.11: Volba *Jumbo obsah*

hlavička). Uzly, které nemají tak velké MTU, nemusí jumbogramy podporovat a ani této volbě rozumět.

UDP Příliš velké datagramy ale vadí i protokolům vyšší vrstvy. Například UDP má svou vlastní položku pro délku dat, která je také 16bitová. RFC 2675, které definuje jumbogramy, proto doporučuje, aby na strojích s jejich podporou byl pozměněn kód i ve vyšších vrstvách. Konkrétně pro UDP doporučuje, aby se u jumbogramů uváděla na úrovni UDP nulová délka a aby si kód pro UDP nechal sdělit skutečnou délku od IP vrstvy.

TCP TCP sice nemá ve svých hlavičkách délku, ale definuje volbu *Maximální délka segmentu (Maximum Segment Size, MSS)*, která – jak jinak – používá 16bitovou hodnotu. Doporučenou strategií je prohlásit 65 535 za nekonečno. Pokud jeden z partnerů dostane MSS s touto hodnotou, určí si skutečnou maximální délku segmentu z nalezeného MTU cesty (odečtením 60 B na IPv6 a TCP hlavičky).

Druhým délkovým údajem v TCP je délka urgentních dat. Autoři RFC 2675 považují za nepravděpodobné, že by se urgentní data používala v kombinaci s jumbogramy. Kdyby k tomu však přece jen došlo, doporučují i zde prohlásit 65 535 za nekonečno. Tato hodnota v položce *Urgent pointer* TCP hlavičky znamená „všechna data v tomto datagramu jsou urgentní“. Při odesílání TCP paketu s dlouhou urgentní částí je třeba jej rozdělit na dva tak, aby první obsahoval jen samá urgentní data a ve druhém byla délka urgentní části menší než 65 535, tedy vyjádřitelná šestnáctibitovou délkovou položkou.

Upřímně řečeno považuji jumbogramy spíše za zajímavou teoretickou konstrukci než za prakticky použitelný nástroj. MTU tak velká, aby ji umožňovala použít, se v současném Internetu nevyskytují.

2.8 Rychlý start

Rozšiřující hlavička *Rychlý start (Quickstart)* byla přidána experimentálním RFC 4782: *Quick-Start for TCP and IP*. Jeho cílem je zvýšit propustnost transportních protokolů, především TCP. Stroj zahajující komunikaci přidá do žádosti o navázání TCP spojení tuto hlavičku, v níž vyznačí přenosovou rychlost, jakou by rád používal.

Jedná se o volbu pro všechny, hlavičkou se tedy zabývají všechny směrovače po cestě a pokud některý z nich považuje navrženou přenosovou rychlost za příliš vysokou, sníží hodnotu na akceptovatelnou úroveň. Při příchodu do cílového stroje tedy hlavička obsahuje rychlost přijatelnou pro všechna zařízení na cestě mezi odesilatelem a příjemcem. Během komunikace je pochopitelně tato informace čas od času aktualizována.

Vzhledem k tomu, že dotyčný protokol je experimentální a s vlastním IPv6 souvisí jen volně, nebudu mu zde věnovat větší pozornost.

2.9 Toky

Jedním z nových prvků IPv6 je koncepce toku. Idea je jasná: tok je proud datagramů, které spolu „nějak souvisí“. Často tok odpovídá transportnímu spojení (například TCP spojení mezi WWW klientem a serverem či IP telefonní hovor mohou být dobrými kandidáty pro tok), ale nemusí tomu tak nutně být.

Přestože se termín ve světě IPv4 nepoužívá, analogie toků zde existuje. Obvykle bývají identifikovány pěticí údajů:

- zdrojová IP adresa
- zdrojový port
- cílová IP adresa
- cílový port
- transportní protokol

Pokud jste někdy konfigurovali firewall, jistě vám tahle pětka je důvěrně známá. Typickým příkladem uplatnění de facto toku je stavový firewall, který povolí otevřít TCP spojení jen v jednom směru. Jakmile se tak stane, uloží si pětici uvedených údajů do paměti a po určitou dobu obousměrně propouští datagramy s příslušnými hodnotami, protože je považuje za součást otevřeného spojení (čili toku).

Problém je, že tři z pěti údajů patří do transportní vrstvy a nemusí být snadno dostupné. Dojde-li k fragmentaci datagramu, jsou transportní údaje obsaženy jen v prvním fragmentu. Při utajení pomocí hlavičky ESP se k nim prvky po cestě nedostanou vůbec, protože jsou zašifrovány a z principu věci je dešifrovat umí jen příjemce. Nebo sice jsou dostupné, ale cesta k nim vede dlouhou sekvencí rozšiřujících hlaviček a zbytečně zpracující zařízení zdržuje.

koncept toku

Proto se objevil koncept toků, který má pomoci identifikovat související datagramy snadno a rychle, jen pomocí údajů ze základní IP hlavičky. Výše zmíněnou pětici má nahradit trojice:

- zdrojová IPv6 adresa
- cílová IPv6 adresa
- značka toku

Problematika toků je dosud živá. Původní RFC 2460 ji neřeší vůbec, odkládá definici na později. První krok na cestě k funkčním tokům učinilo RFC 3697: *IPv6 Flow Label Specification*, které definovalo pravidla pro zacházení se značkami toků v datagramech. Postupem času se objevila řada návrhů, k čemu všemu a jak by se dala *Značka toku* ze základní hlavičky využít. Jejich přehled najdete v RFC 6294: *Survey of Proposed Use Cases for the IPv6 Flow Label*. Obvykle však odporují některým pravidlům zavedeným v RFC 3697.

Na podzim 2011 pak vyšla nová generace dokumentů, které se snaží postrčit definici toků zase o něco dál. Zahrnuje RFC 6436: *Rationale for Update to the IPv6 Flow Label Specification* shrnující dosavadní zkušenosti a motivaci nové specifikace. Ta je obsažena v RFC 6437: *IPv6 Flow Label Specification*, jež nahrazuje RFC 3697.

značka toku

Hodnota značky podle RFC 6437 nemá žádnou strukturu ani význam. Slouží čistě jako identifikátor. Pokud odesilatel nechce své datagramy značkovat, vloží do položky *Značka toku* nulu, která signalizuje, že paket není zařazen do žádného toku. Nula je jedinou hodnotou, pro niž specifikace zavádí speciální význam.

Přidělení značky toku má na starosti odesilatel datagramu. Svou vlastní značku typicky dostane každý datový tok se stejnou pěticí základních identifikačních údajů, již jsem zmínil výše. Nicméně není to předepsáno pevně, rozhodnutí je na odesilateli.

Specifikace požaduje, aby hodnoty značek byly rovnoměrně rozděleny v celém dostupném prostoru a aby se nedaly předem odhadnout. Důvodem těchto požadavků je snaha o jejich snadnou použitelnost při hashování a omezení bezpečnostních rizik. Jako vhodné generátory značek dokument zmiňuje hashovací funkci nebo generátor pseudonáhodných čísel. Naopak výslovně nedoporučuje sekvenční přiřazování, kdy každá další značka je o jedničku větší, než poslední použitá.

přeprava

Během přepravy sítí se značka nesmí měnit a musí být příjemci doručena se stejnou hodnotou, jakou jí přidělil odesilatel. Z tohoto obecného pravidle ovšem existují dvě výjimky. První je motivována bezpečností: Pokud by některý ze směrujících strojů dospěl k závěru, že se někdo snaží zneužít značky k vytvoření tajného informačního kanálu, smí do nich zasáhnout. Druhou výjimkou je nulová značka. Jestliže se odesilatel rozhodl datagram

neznačkovat, může to za něj udělat některý ze směrovačů[3]. Jakmile došlo ke vložení nenulové hodnoty, musí už dále zůstat neměnná.

Způsob využití při přepravě není pevně definován. Existují v zásadě dvě cesty: může být bezstavový, kdy si přepravující prvky neukládají žádné informace, jež by při doručování značkovaných datagramů využívaly, či stavový, který se právě o takové informace opírá. Návrh dává přednost bezstavové variantě, zatímco o stavové se zmiňuje jen okrajově.

Podpora toků není povinná. Průchozí zařízení může brát na tok zřetel, nebo nemusí. V tom případě však musí informace související s tokem ignorovat a nijak do nich nezasahovat. Tím je zajištěno, že nic nepokazí strojům, které jsou za ním a věci rozumějí.

Na novou specifikaci toků navazuje RFC 6438: *Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels* s příkladem možného využití *Značky toku* k rozkládání zátěže mezi několik alternativních cest vedoucích ke stejnému cíli.

V praxi se zatím lze se značkováním toků setkat jen zcela ojediněle, valná většina datagramů v Internetu nese nulovou značku. Nová generace dokumentů představuje určitý posun vpřed, ale na reálné používání značek si nepochybně ještě dost dlouho počkáme.

[3] Typickými kandidáty pro takové chování jsou přístupový směrovač koncové sítě nebo vstupní směrovač poskytovatele Internetu.

3 Adresy v IPv6

Rychle se tenčící adresní prostor byl jedním z hlavních hnacích motorů vzniku IPv6. Přestože navržený protokol má i řadu jiných zajímavých vlastností, dodnes je košatost jeho adresního prostoru považována za klíčovou přednost a s krátící se zásobou IPv4 adres nabývá na naléhavosti. Podívejme se na ni podrobněji.

Základním dokumentem pro definici adres je RFC 4291: *IP Version 6 Addressing Architecture* určující jejich délku a podobu, typy adres a další koncepční prvky. Je doplněn několika dalšími dokumenty popisujícími podrobněji vybrané části adresního prostoru.

3.1 Jak se adresuje

V IPv6 – stejně jako u jeho předchůdce – jsou adresy přiřazovány síťovým rozhraním, nikoli počítačům. Má-li váš počítač dvě síťové karty, bude mít každá z nich svou adresu. Přesněji řečeno své adresy. Později uvidíte, že IPv6 s adresami pro rozhraní nikterak neskrblí.

druhy adres

Existují tři druhy adres s odlišným chováním:

Individuální (unicast) jsou staré známé krotké adresy. Každá z nich identifikuje jedno síťové rozhraní a data mají být dopravena právě jemu.

Skupinové (multicast) slouží pro adresování skupin počítačů či jiných zařízení. Pokud někdo odešle data na tuto adresu, musí být doručena všem členům skupiny.

Výběrové (anycast) představují novinku a nejzajímavější přírůstek v IPv6. Také výběrové adresy označují skupinu, data se však doručí jen jedinému jejímu členovi – tomu, který je nejblíže.

Porovnání s IPv4 ukazuje, že zmizely všesměrové (broadcast) adresy. Nejsou potřeba, protože jejich funkce přebírají adresy skupinové. Jsou definovány speciální skupiny, např. pro všechny uzly na dané lince, které umožňují plošnou distribuci zpráv.

adresy rozhraní

IPv6 umožňuje, aby rozhraní mělo libovolný počet adres různých druhů. Ba dokonce přikazuje několik povinných adres, které musí být přiděleny (viz část 3.10 na straně 79). Stejně jako v IPv4 se předpokládá, že všechny počítače v jedné fyzické síti (např. na jednom Ethernetu) budou náležet do stejné podsítě a budou tudíž mít společný prefix podsítě.

3.2 Podoba a zápis adresy

Při rozhodování o velikosti adresy pro IPv6 se autoři řídili heslem „aby nám už nikdy nedošly“. Frustrace způsobená nedostatkem IPv4 adres byla velmi silná. Proto se rozhodli délku prodloužit na čtyřnásobek, adresa v IPv6 tedy měří 128 bitů.

zápis adres

Standardním způsobem jejího zápisu je osm skupin po čtyřech číslicích šestnáctkové soustavy, které vyjadřují hodnoty 16 bitů dlouhých částí adresy. Navzájem se oddělují dvojtečkami. Příkladem IPv6 adresy je

fedc:ba98:7654:3210:fedc:ba98:7654:3210

Upřímně řečeno se očekává, že uživatelé budou striktně používat DNS a ručního psaní uvedených hrůz budou ušetřeni. Černý Petr zbude v rukou správců sítí, kteří se jim při sebevětším úsilí nevyhnou...

zkracování

Jelikož je poměrně častou hodnotou nula, nabízí se dvě možnosti pro zkrácení zápisu. Jednak v každé čtveřici můžete vynechat počáteční nuly. Místo „0000“ tedy lze psát jen „0“. Někdy se dokonce vyskytuje několik nulových skupin za sebou. Ty můžete nahradit zápisem „::“ (dvě dvojtečky). Například adresu

0123:0000:0000:0000:fedc:ba98:7654:3210

můžete zkrátit na

123:0:0:0:fedc:ba98:7654:3210

nebo dokonce jen na

123::fedc:ba98:7654:3210

Koncovou nulu (v poslední čtveřici) pochopitelně vynechat nelze. Kdybyste napsali jen „321“, znamenalo by to „0321“, nikoli „3210“. Úplný extrém představuje nedefinovaná adresa

0000:0000:0000:0000:0000:0000:0000:0000

kterou lze zkrátit až na samotné

::

Konstrukci „::“ můžete v každé adrese použít jen jednou. Jinak by nebylo jednoznačné, jak se má adresa rozvinout do původní podoby. Například adresu

0123:0000:0000:0000:4567:0000:0000:0000

můžete psát jako

123::4567:0:0:0 nebo 123:0:0:0:4567::

nikoli však

123::4567::

kanonický zápis Velká variabilita v zápisu adres komplikuje jejich porovnávání. Výše vidíte několik příkladů výrazně odlišných zápisů stejné adresy, navíc mohou situaci ještě komplikovat malá/velká písmena a pro lidského čtenáře v některých písmech potenciálně zaměnitelné znaky „B“ a „8“ či „D“ a „0“.

RFC 5952: *A Recommendation for IPv6 Address Text Representation* proto definovalo kanonický zápis, jehož cílem je učinit psanou podobu adresy jednoznačnou. Dokument zdůrazňuje, že aplikace musí podporovat všechny přípustné podoby adresy, ale ve svých výstupech, jako jsou výpisy či hodnoty v konfiguračních dialozích, by měly používat kanonický tvar. Pravidla pro jeho vytvoření jsou následující:

- Šestnáctkové číslice reprezentované písmeny se píší vždy malými znaky[1].
- Vynechání počátečních nul ve čtveřici je povinné.
- Konstrukce „::“ musí být použita tak, aby měla největší možný efekt. Musí pohltit všechny vzájemně sousedící nulové skupiny (není povoleno „:0::“ ani „::0:“) a musí být použita pro nejdelší sekvenci nulových skupin v adrese. Má-li shodnou maximální délku několik skupin, použije se „::“ pro první z nich. Není povoleno ji použít pro jedinou nulovou skupinu, ta vždy zůstane jako jednoduchá nula.

Kanonický tvar výše uvedené adresy je 123::4567:0:0:0 a software by ji vždy měl vypisovat v této podobě.

URL Při zápisu adresy do URL bohužel nelze použít stejně přímočarý přístup jako v případě IPv4, kdy se jednoduše místo doménového jména uvede číselná adresa. Dvojtečky jsou v URL používány k oddělení čísla portu od jména či adresy a jejich přítomnost by byla pro interpretující software matoucí. Má-li se v URL vyskytnout IPv6 adresa, musíte ji uzavřít do hranatých závorek. Takže například URL s IPv6 adresou *www.nic.cz* by vypadalo takto:

```
http://[2002:d91f:cd32::1]/
```

Podrobně je vše popsáno v RFC 3986: *Uniform Resource Identifier (URI): Generic Syntax*.

[1] Toto pravidlo bylo nahlášeno jako chybné, protože se tradičně používala velká písmena. O osudu „chyby“ dosud nebylo rozhodnuto, ale nedovedu si představit, že by byla akceptována a pravidlo se změnilo. Argumentace je dost fundamentalistická, opírá se o literaturu starší než 20 let a odporuje současné praxi.

prefixy Příslušnost k určité síti nebo podsíti se vyjadřuje prefixem – všechna rozhraní v jedné síti mají stejný prefix (začátek adresy). Jeho délka může být různá – záleží na tom, s jakou podrobností se na adresy díváte. Může vás zajímat jen prefix poskytovatele Internetu (který bude poměrně krátký) nebo o poznání delší prefix určité konkrétní podsítě.

Tento přístup se používá již v současném Internetu pod názvem *Classless Inter-Domain Routing (CIDR)*. Z něj je také převzat způsob, kterým se prefixy zapisují:

IPv6_adresa/*délka_prefixu*

Délka_prefixu určuje, kolik bitů od začátku adresy je považováno za prefix. Například 60 bitů dlouhý prefix 12ab 0000 0000 cd3 lze zapsat několika možnými způsoby:

12ab:0:0:cd30:0:0:0:0/60
12ab::cd30:0:0:0:0/60
12ab:0:0:cd30::/60

Nejvhodnější je poslední z nich, protože odpovídá kanonickému tvaru a navíc konstrukcí „::“ logicky nahrazuje závěrečnou část adresy, která je z pohledu prefixu nezajímavá. Povšimněte si, že do prefixu nepatří ani závěrečná nula ve skupině cd30, protože při délce 60 bitů do prefixu z této skupiny patří jen 12 bitů, čili první tři šestnáctkové číslice. Tuto nulu však nelze vynechat. Kdybychom to udělali, byla by příslušná skupina interpretována jako 0cd3 a zápisem 12ab:0:0:cd3::/60 bychom ve skutečnosti vyjádřili prefix 12ab 0000 0000 0cd, což je krajně matoucí.

Prefix pochopitelně nemusí končit na hranici šestnáctkových číslic. Například prefix 2000::/3 požaduje, aby první tři bity adresy obsahovaly hodnotu 001 (binárně). Tomu vyhoví všechny IPv6 adresy, jejichž první číslicí je 2 nebo 3.

Ve zkratce lze použít i zápis, který současně oznamuje jak konkrétní adresu rozhraní, tak délku prefixu (a tudíž adresu podsítě):

12ab:0:0:cd30:123:4567:89ab:cdef/64

3.3 Rozdělení aneb typy adres

Obrovský adresní prostor, který má IPv6 k dispozici, byl rozdělen do několika skupin – typů adres. Každý typ sdružuje adresy se společnou charakteristikou. Příslušnost k jednotlivým typům určuje prefix adresy. Dříve se pro tyto určující počáteční bity používal termín *prefix formátu (format prefix, FP)*, novější dokumenty však od tohoto pojmu upouští.

Základní rozdělení uvádí tabulka 3.1. Jak je vidět, drtivou většinu zabírají globální (celosvětově jednoznačné) individuální adresy. Z jejich prostoru

prexif	*význam*
::/128	nedefinovaná adresa
::1/128	smyčka (loopback)
fc00::/7	unikátní individuální lokální (strana 65)
fe80::/10	individuální lokální linkové (strana 64)
ff00::/8	skupinové adresy (strana 68)
ostatní	individuální globální (strana 60)
známé prefixy	
64:ff9b::/96	adresy s vloženým IPv4
2001::/32	Teredo
2001:db8::/32	adresy pro příklady v dokumentech
2002::/16	6to4

Tabulka 3.1: Základní rozvržení adres a vybrané prefixy

je navíc většina prefixů dosud nepřiřazena, zatím se využívá pouze výše zmiňovaný prefix 2000::/3. Ostatní se ponechávají jako rezerva a očekává se, že budoucí RFC jim přiřknou určitý význam a vnitřní strukturu. Aktuální stav jejich přidělení najdete na adrese

WWW► *http://www.iana.org/assignments/ipv6-address-space*

Skupinové adresy jsou snadno identifikovatelné, protože jejich první bajt má v šestnáctkovém zápisu hodnotu ff. Naproti tomu výběrové adresy nemají přiřazeno žádné speciální rozmezí a přidělují se ze stejného prostoru, jako adresy individuální.

Několika menším oblastem adresního prostoru byl přidělen specifický význam. Celý prefix ::/8 byl původně rezervován pro speciální účely. Nyní je deklarován jako nepřiřazený, některé adresy v jeho rámci však přiřazeny byly. Jedná se o individuální adresy ::0 a ::1. První se používá pro nedefinovanou adresu. Říká, že dotyčnému rozhraní dosud nebyla přidělena IPv6 adresa. ::1 je pak adresou lokální smyčky (loopback), kterou počítač-schizofrenik může komunikovat sám se sebou. Spadají sem také prefixy přidělené pro IPv6 adresy obsahující v sobě IPv4 (viz strana 66).

Skupinka prefixů identifikuje adresy s omezeným dosahem. Nejčastěji se setkáte s lokálními linkovými adresami, které jsou jednoznačné vždy jen v rámci jedné linky (jednoho Ethernetu, jedné Wi-Fi buňky,...). Poznáte je podle prefixu fe80::/10 a najdete je u každého rozhraní se zapnutým IPv6. Vedle nich dříve existovaly místní individuální lokální adresy s prefixem fec0::/10 jednoznačné v místní síti. Později však byly zrušeny, proto se jejich prefix v tabulce nevyskytuje. Nahradily je unikátní individuální lokální adresy s prefixem fc00::/7.

Podívejme se nyní podrobněji na jednotlivé kategorie.

3.4 Globální individuální adresy

Tento typ adres je nejdůležitější, protože se jedná o „normální“ adresy – protipól adres současného IPv4. Slůvko globální naznačuje, že identifikují svého nositele v rámci celého Internetu a musí tudíž být celosvětově jednoznačné. Zatím byla definována jen část z nich (prefix 001 binárně), jejíž strukturu definuje RFC 3587: *IPv6 Global Unicast Address Format*.

agregace

Globální adresy jsou přidělovány hierarchicky podle pravidel podobných CIDR ze světa IPv4. To znamená, že poskytovatel Internetu (neboli lokální registr, LIR) obdrží určitý prefix, jehož části v podobě delších prefixů se shodným začátkem pak přiděluje svým zákazníkům. Cílem tohoto přístupu je agregace směrovacích údajů – aby bylo možné při pohledu zvenčí celou poskytovatelovu síť i se všemi zákazníky popsat jediným záznamem ve směrovacích tabulkách, obsahujícím onen společný prefix.

Toto shlukování je velmi důležité, protože významným způsobem zmenšuje velikost směrovacích tabulek. Jemnost členění směrovacích informací přirozeně klesá se vzdáleností od místa určení. Původně se koncept agregace promítal i do struktury adresy, která byla složena z identifikátorů několika úrovní. K praktickému naplnění této vize však nedošlo a reálně používané adresy původní koncept nedodržovaly.

Proto byl opuštěn a RFC 3587 zavedlo maximálně zjednodušený model, v podstatě odpovídající struktuře adresy pro IPv4. Ta má tři části: adresu sítě, podsítě a rozhraní v podsíti. Analogické části má i IPv6 adresa, jen adresa sítě byla přejmenována na globální směrovací prefix. Jejich délky jsou definovány zcela obecně, podle současných pravidel přidělování však globální směrovací prefix měří nejčastěji 48 bitů, adresa podsítě 16 bitů a adresa rozhraní v podsíti 64 bitů. Strukturu globální individuální adresy s nejobvyklejšími délkami jednotlivých částí znázorňuje obrázek 3.1.

Obrázek 3.1: Obvyklá struktura globální individuální adresy

globální směrovací prefix

Globální směrovací prefix identifikuje koncovou síť. Je síti přidělen „zvenčí“ lokálním internetovým registrem, čili zpravidla poskytovatelem Internetu. Proto bývá tato část adresy označována jako „veřejná topologie“. Podrobněji se k problematice přidělování globálního směrovacího prefixu vrátím

v části 3.14 na straně 91. Kromě nejběžnější délky 48 bitů se u malých koncových sítí lze setkat i s prefixy délky 56 či 64 b.

identifikátor podsítě

Identifikátor podsítě slouží k rozlišení jednotlivých podsítí v rámci dané sítě. Tato část adresy je, společně s identifikátorem rozhraní, záležitostí správy koncové sítě a používá se pro ni označení „místní topologie“. Délka identifikátoru rozhraní závisí na délce globálního směrovacího prefixu – dohromady musí měřit 64 bitů. Obvyklými hodnotami jsou 16 a 8 bitů, pokud je ovšem globální směrovací prefix 64bitový, na identifikátor podsítě už nezbývá žádné místo a příslušná síť není dělena na podsítě. Identifikátor rozhraní má totiž konstantní délku 64 bitů.

Pouze v ojedinělých případech, jako jsou například propojovací podsítě na linkách spojujících pouhá dvě zařízení, má smysl uvažovat o dlouhých adresách podsítě a ponechání jen minimálního prostoru pro identifikátor rozhraní. Podrobněji se této problematice věnuji na straně 306, kde jsou rozebrány různé varianty adresování dvoubodových sítí, jejich přednosti a nevýhody.

Nejběžnější délkou identifikátoru podsítě je 16 b, což umožňuje rozlišit 65 536 podsítí. To stačí i pro opravdu velké sítě. Obecně mívá správce sítě k dispozici nebývalé množství adresního prostoru[2] a díky tomu volné ruce při strukturování koncové sítě a návrhu jejího adresního plánu. Problematice se budu věnovat v části 13.5 na straně 304.

identifikátor rozhraní

Závěrečný *identifikátor rozhraní* zabírá celou polovinu adresy, což umožňuje v jedné podsíti rozlišit něco přes $18 \cdot 10^{18}$ různých rozhraní (tedy miliardy miliard). Motivací k takto velkorysému dimenzování podsítě byla snaha o maximální zjednodušení automatické konfigurace počítačů. Nicméně nelze přehlížet, že AppleTalk zvládal automatickou konfiguraci s jediným bajtem[3] a IPv4 stačí čtyři bajty pro celosvětově jednoznačné adresy. Investovat osm bajtů na dosažení jednoznačnosti v jediné podsíti je zkrátka plýtvání.

Přesto RFC 4291 jednoznačně stanoví, že pro všechny individuální adresy (s výjimkou adres s prefixem 0::/3) je vyžadována délka identifikátoru rozhraní 64 bitů a používání identifikátorů ve tvaru modifikovaného EUI-64. Podívejme se na ně podrobněji.

3.5 Identifikátory rozhraní – modifikované EUI-64 a spol.

Základní podoba identifikátoru rozhraní v IPv6 je odvozena z IEEE EUI-64. Jedná se o standard zaměřený na přidělování globálních (celosvětově jed-

[2] Pokud je jeho poskytovatel Internetu skrblík, dostane „jen“ 8 bitů pro 256 podsítí.

[3] Pravda, omezovalo to počet rozhraní v podsíti na 256, což by pro IPv6 jistě bylo neakceptovatelné.