Pavel Satrapa

Čtvrté vydání

IPv6

Internetový protokol verze 6

Edice CZ.NIC

IPv6
Pavel Satrapa

Vydavatel:
CZ.NIC, z. s. p. o.
Milešovská 5, 130 00 Praha 3
Edice CZ.NIC
www.nic.cz

4. aktualizované a rozšířené vydání, Praha 2019
Kniha vyšla jako 22. publikace v Edici CZ.NIC.
ISBN 978-80-88168-46-1

CZ.NIC | SPRÁVCE DOMÉNY CZ

ISBN 978-80-88168-46-1

— Pavel Satrapa

IPv6

Internetový protokol verze 6

— Edice CZ.NIC

Předmluva vydavatele

Vážení čtenáři,

dostává se vám do rukou v pořadí již čtvrté aktualizované vydání knihy o internetovém protokolu IPv6 a jeho širším využití. Aktualizace knihy se nemohl chopit nikdo povolanější než Pavel Satrapa, který svým nenapodobitelným vysoce čtivým způsobem informace o IPv6 protokolu občerstvuje po 8 letech.

První vydání této knihy spatřilo světlo světa již v roce 2002 a od té doby se nasazení protokolu IPv6 v počítačových sítích neustále rozšiřuje. Bohužel ne tak rychle, jak se očekávalo. Sdružení CZ.NIC se již od roku 2010 snaží, ve spolupráci s registrátory a provozovateli webhostingu, o rozšiřování podpory IPv6 protokolu u vybraných internetových služeb. Nasazení IPv6 protokolu tak v rámci české národní domény v roce 2018 překročilo u webových serverů hranici 31 %, u e-mailových serverů 19 % a v případě DNS serverů dokonce 75 %. Současně se sdružení CZ.NIC podílí na prosazování IPv6 ve státní správě, a to jak v rámci evropského projektu GEN6, tak i v úzké spolupráci s Ministerstvem průmyslu a obchodu. Otázkou zůstává, jak moc přispívá k zavádění IPv6 ve veřejné správě usnesení vlády přijaté na konci roku 2013, které vyžaduje zahrnout požadavek na podporu IPv6 do všech relevantních výběrových řízení i jako nedílnou součást požadavků na všechny nově podpořené projekty.

Na kurzu IPv6 pro pokročilé, který pořádá Akademie CZ.NIC a jehož jsem lektorem, se vždy na začátku ptám uchazečů, jaké mají s IPv6 protokolem zkušenosti. Většina z nich přichází na tento pokračovací kurz s tím, že IPv6 již nasadili a používají. Chtějí se dozvědět, jaké jsou další možnosti použití nejen v lokálních sítích a jak co nejvíce přesvědčit uživatele o výhodách nastupujícího protokolu. Právě edukace běžných uživatelů je při jeho rozšiřování nejsložitější disciplínou. Většina z nich v tom nevidí zásadní přínos a neuvědomuje si, že se změny týkají i jich.

Věřím, že při čtení této výborné knihy strávíte příjemné chvíle, získáte nové informace a podaří se vám zase o kousek posunout rozšíření IPv6 protokolu v České republice.

Václav Steiner
Praha, duben 2019

Předmluva

Předmluva

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 mnohem pomaleji a bolestněji, než se původně očekávalo. Poslední dobou se situace konečně obrací k lepšímu – po nasazení velkými hráči (Google, Facebook a další) začal podíl IPv6 na celkovém provozu konečně růst. Současná zhruba čtvrtina má sice ke 100,% daleko, ale protokol už hraje významnou roli.

Cílem této knihy je popsat, jak IPv6 vypadá a jak funguje. Snažil jsem se velmi zevrubně vysvětlit principy a mechanismy, na kterých 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 dlouho drhly.

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.

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*. Od třetího vydání z roku 2011 uplynulo osm let, během nichž se protokol konečně začal prosazovat a používat v praxi.

Vyčerpání IPv4 adres se stalo realitou, jejich nedostatek omezuje poskytovatele připojení i služeb a vynucuje si komplikovaná a křehká řešení. V porovnání s tím pak nasazení IPv6 zhusta vychází jako jednodušší a levnější varianta. Datová centra či páteřní sítě postavené důsledně na IPv6 se z teoretických studií přesouvají do reality.

Nejvýznamnější změnou od minulého vydání je revize základní specifikace IPv6 v RFC 8200. Pro uživatele je viditelnou novinkou algoritmus Happy Eyeballs, který se snaží, aby problémy jednoho protokolu měly minimální dopad. Podstatně se také změnila scéna přechodových mechanismů – od snahy propojovat ojedinělé ostrůvky IPv6 v IPv4 Internetu jsme se přesunuli k odstraňování IPv4 z částí sítě a hledání řešení, jak je dopravit zákazníkům, když páteř podporuje jen IPv6. Celý text jsem důkladně aktualizoval a doplnil.

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. Ke čtvrtému vydání významně přispěli Ondřej Caletka a Radek Zajíc, k těm přechozím zejména Luboš Pavlíček, Pavel Moravec, Petr Adamec, Stanislav Petr a Emanuel Petr.

Pavel Satrapa
Liberec, březen 2019

Obsah

Úvod

1 Úvod

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

1.1 Vlastnosti a vývoj

Jeho kořeny sahají do začátku 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.

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 definicemi základních protokolů a služeb v čele s RFC 2460. 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 … V roce 2017 už bylo různých změn a doplňků tolik, že v RFC 8200 vyšla nová základní definice IPv6.

Navíc – a to je nejdůležitější – se začaly množit a zlepšovat implementace v nejrůznějších operačních systémech. Také řada aplikací dnes již podporuje nový protokol.

Na vývoji IPv6 a jeho komponent se podílela a podílí celá řada pracovních skupin IETF. Přehled těch, které se přímo zabývají IPv6 a jeho součástmi, uvádí tabulka 1.1. Kromě nich ovšem protokol prosakuje i do činnosti celé řady dalších. Přehled pracovních skupin a veškeré jejich dokumenty najdete na adrese:

🔗 https://datatracker.ietf.org/wg/

Priority pro nasazení se časem měnily. Tlak nedostatku adres na určitou dobu polevil a do popředí se začaly drát jiné přednosti IPv6, zejména podpora mobility. Při rychle rostoucím zájmu o nejrůznější přenosná zařízení a jejich zapojení do Internetu se právě jejich podpora, která je v IPv6 výrazně lepší než u jeho předchůdce, zdála být 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 často chyběly, odvedl IPv6 medvědí službu.

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,

aktivní	
6man	údržba a aktualizace specifikací
v6ops	provoz IPv6 sítí
lpwan	IPv6 v nízkonapěťových dálkových sítích
6lo	IPv6 v sítích s omezenými zdroji
6tisch	IPv6 v režimu TCSH sítí IEEE 802.15.4e
uzavřené	
ipv6	(původně *ipng*) vytvořila většinu základních specifikací
mip6	mobilita
mext	rozšíření mobility
multi6	multihoming
shim6	multihoming
6renum	přeadresování IPv6 sítí
6bone	vytvoření sítě *6bone*
6LoWPAN	IPv6 v nízkonapěťových osobních sítích

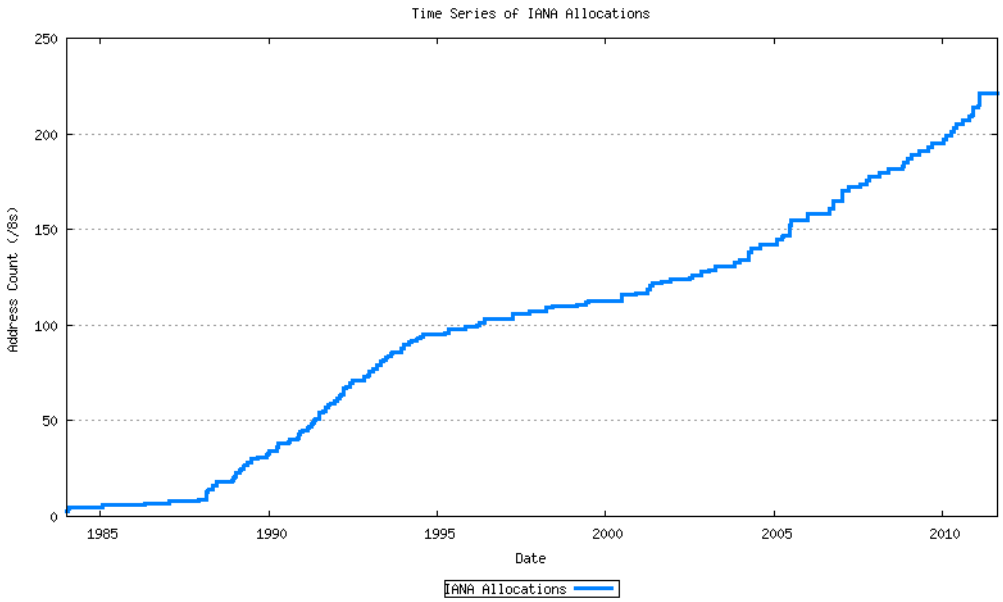
Tabulka 1.1: Pracovní skupiny IETF zapojené do vývoje IPv6

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.

Počátkem roku 2019 se nacházíme v situaci, kdy je vyčerpána centrální zásoba IANA. Regionální registry (RIR) dnes fungují v úsporném režimu, kdy zbývající hrstku adres alokují po velmi malých kouscích. Tabulka 1.2 obsahuje data, kdy jednotlivé registry začaly rozdělovat poslední osmibitový prefix a vstoupily tak do úsporného režimu.

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, například v Evropě lze od RIPE NCC získat maximálně 1024 IPv4 adres. Oficiálně jsou 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



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

IANA	3. února 2011
APNIC	19. dubna 2011
RIPE NCC	14. září 2012
LACNIC	10. června 2014
ARIN	24. září 2015
AFRINIC	16. ledna 2017

Tabulka 1.2: Vyčerpání IPv4 adres

všeobecně rozmáhá 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.

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 (Skype a podobné komunikátory, videokonference, síťové hry, peer-to-peer sítě a další). Potřebují vytvářet přímá spojení mezi komunikujícími zařízeními. 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 286 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 může mít svou vlastní, celosvětově jednoznačnou IP adresu.

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 není moc efektivní.

Své nepochybně vykonal i pomalý vývoj některých specifikací. O nejkřiklavějším případu mobility jsem se již zmínil. Bohužel není jediný, DHCPv6 bylo definováno jen o rok dříve, přestože se jedná o protokol ve světě IPv4 dobře známý a hojně používaný. Standardizace jednotlivých součástí světa IPv6 stále probíhá, i když nyní už se spíše jen doladují detaily. Nejisté výnosy v kombinaci s nestabilními specifikacemi jsou silně odrazující pro všechny, kteří zvažují implementaci nového protokolu. Proto jim to šlo jako psovi pastva, počáteční implementace byly značně nedokonalé a zlepšovaly se jen velmi zvolna.

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

IPv6 se dlouho potácelo v bludném kruhu slepice versus vejce. Uživatelé o něj neměli zájem, protože v něm nebyly dostupné služby. A kdo by převáděl služby pod IPv6, když tam nebyli žádní uživatelé? Svého času byla zřetelná snaha přispět k rozetnutí tohoto kruhu politicky. Vlády vydávaly prohlášení a výzvy podporující přechod na IPv6, financovaly se projekty rozvíjející infrastrukturu a služby.

Nejvýznamnějším zlomem byl *Světový den spuštění IPv6 (World IPv6 Launch Day)* 6. června 2012, kdy IPv6 nativně nasadilo několik velkých poskytovatelů služeb – Google, Facebook, Yahoo, Akamai Technologies a další. Tím vznikl tlak na poskytovatele připojení, aby své případné experimenty s IPv6 dotáhli do funkční podoby, a zároveň se otevřela příležitost využívat nový protokol v širším měřítku. Objem IPv6 provozu začal konečně významněji stoupat.

1.2 Současný stav

IPv6 je zajímavý a nadějný protokol, který je ze strany IETF rozvíjen jako jediná možnost pro budoucnost Internetu. RFC 6540: *IPv6 Support Required for All IP-Capable Nodes* požaduje jeho všeobecnou podporu. Konkrétně:

- Nové implementace IP musí podporovat IPv6.
- Aktualizace stávajících implementací IP by je měly podporovat.
- Kvalita podpory IPv6 musí být přinejmenším srovnatelná s IPv4.
- Implementace by měly podporovat koexistenci obou verzí, ale jejich úplná funkčnost nesmí záviset na IPv4.
- Vyzývá implementátory, aby podporu nového protokolu přidali co nejdříve.

V roce 2016 vydal Internet Architecture Board, který koordinuje technický rozvoj Internetu, *Prohlášení IAB o IPv6* [11]. V něm vyzývá IETF, aby v nových internetových standardech a aktualizacích těch stávajících nepředpokládal existenci IPv4. Měly by být navrženy tak, aby fungovaly v IPv6 síti, tento protokol by měl být považován za výchozí a měl by být používán i v příkladech. Rozhodně by neměly záviset na IPv4. V prohlášení zároveň IAB vyzývá celý obor, aby připravoval strategie pro provoz sítí, kde jediným síťovým protokolem bude IPv6.

Přesto míra jeho nasazení dlouhodobě pokulhává za vizemi a plány. V předchozím vydání jsem na tomto místě psal, že se stále ještě nedá vyloučit, že skončí jako slepá vývojová větev. To už dnes vyloučit můžeme, statistiky nasazení se definitivně odlepily od nuly a pohybují se dnes v řádu desítek procent.

Podle původních očekávání jsme ale už měli být mnohem dál. Touto dobou už měl být Internet dávno kompletně převeden na nový protokol a pouze kdesi na okraji měly vyhasínat poslední zbytky rustikálního IPv4. Místo toho představuje IPv6 podle těch optimističtějších statistik zhru-

ba čtvrtinu provozu. Pravda, už to nejsou desetiny procenta jako před deseti lety, ale k ovládnutí hřiště stále zbývá pořádný kus cesty.

Jak na tom tedy počátkem roku 2019 jsme? Na jednoduchou otázku je složitá odpověď. Existuje řada různých měření a statistik, jejichž výsledky se rozcházejí v závislosti na uživatelské komunitě i metodice měření. Za relevantní bych považoval výsledky APNIC, kde se měření různých veličin pod vedením Geoffa Hustona věnují dlouhodobě a systematicky, vše publikují a konzultují. Jejich statistika na adrese:

https://stats.labs.apnic.net/ipv6

zobrazuje, jaké procento koncových zařízení v jednotlivých zemích dokáže komunikovat po IPv6. Celosvětově se blížíme ke 20 %. Z velkých států si hodně dobře vedou USA a Indie (skoro 50 %), Evropě vévodí Belgie (52 %), následovaná Německem (38 %) a Řeckem (34 %). Česká republika si s necelými deseti procenty nestojí nijak oslnivě. Zatím bohužel výrazně zaostává Čína, země s největší uživatelskou populací a notorickým nedostatkem IPv4 adres. Tento stav ale nejspíš nepotrvá dlouho, protože Čína začala podnikat razantní kroky k nasazení IPv6. Podle měření APNIC od září 2018 do března 2019 vzrostl počet čínských uživatelů s IPv6 patnáctinásobně a stále stoupá …

Jedním z velmi viditelných subjektů na poli IPv6 je Google. Protokolu se soustavně věnuje od roku 2008, přispívá k vývoji specifikací a podílel se na řadě aktivit, směřujících k jeho prosazení. Vede si i své statistiky podle počtu přístupů k jeho službám. Počátkem roku 2019 jich přibližně čtvrtina přichází novým protokolem. Aktuální stav najdete na adrese:

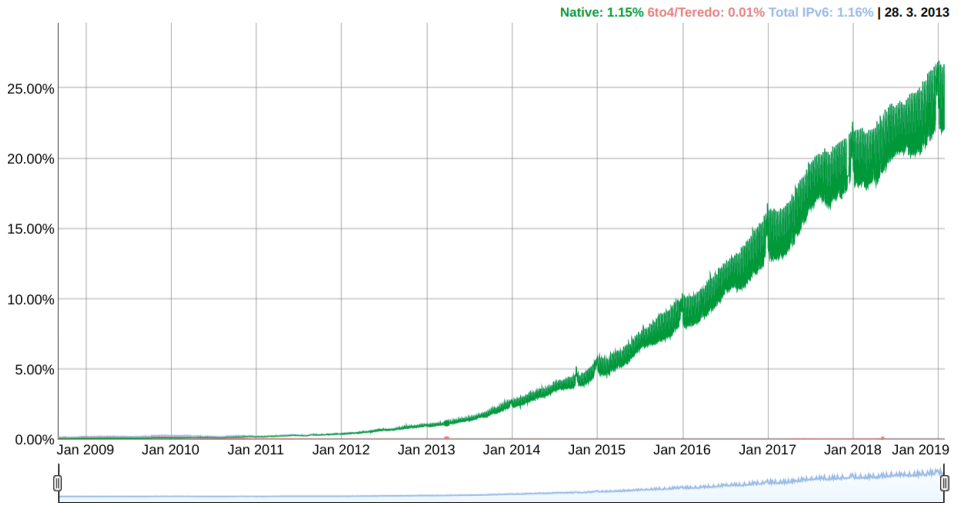
https://www.google.com/intl/en/ipv6/

Zajímavostí je, že během víkendů podíl IPv6 pravidelně stoupá o několik procent. Je vidět, že domácí sítě jsou v jeho nasazení dál, než konzervativnější sítě firemní.

Ani Facebook nespí na vavřínech. Je vidět, že nedostatek IPv4 adres velké poskytovatele služeb pálí a snaží se jej řešit systémově. Jeho statistiky jsou k vidění na:

https://www.facebook.com/ipv6/

a dost se podobají těm od Google, včetně nárůstů ve volných dnech. Také podíl uživatelů přistupujících na Facebook po IPv6 se blíží čtvrtině. Kromě globálních čísel dává Facebook k dispozici i statistiky pro jednotlivé země, které jsou vesměs o něco optimističtější než výše zmiňovaná měření APNIC. Například od nás přichází na Facebook po IPv6 zhruba 11 % uživatelů.



Obrázek 1.2: Podíl IPv6 na přístupech ke službám Google

Velcí hráči nasazují IPv6 nejen vůči koncovým uživatelům, ale i uvnitř svých sítí. Například datová centra Facebooku interně používají pouze IPv6. Pakety přicházející od uživatelů protokolem IPv4 končí na prvcích pro rozkládání zátěže, dále pokračují k vlastním serverům po IPv6. Podobně mají své firemní sítě a datová centra uspořádány i další firmy, jako je Google či Akamai.

Dobrým zdrojem informací o aktuálním stavu IPv6 jsou studie *State of IPv6 Deployment* vydávané Internet Society. V době vzniku této knihy je poslední z roku 2018:

https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

Podle ní se protokol dostává z pionýrských a nadšeneckých dob do fáze rutinního nasazení a má našlápnuto stát se většinovým. Studie uvádí řadu velkých operátorů, kteří IPv6 provozují ve velkém měřítku. Unikátní je indický Reliance Jio, který spouštěl svou mobilní síť v roce 2016 s nedostatkem IPv4 adres. Během 9 měsíců nasadil IPv6 u více než 200 milionů uživatelů, kteří mu generují přes 80 % provozu. Zejména díky němu patří Indie k zemím s nejvyšším podílem IPv6 na světě.

Ani USA ale nestojí stranou, přestože u nich Internet vznikl a jejich firmy často disponují značnými zásobami IPv4 adres z raných dob, kdy pravidla pro jejich přidělování bývala mírná. Řada zdejších velkých operátorů (Comcast, T-Mobile USA, Verizon Wireless) má rozsáhlé IPv6 sítě s desítkami milionů uživatelů. T-Mobile USA už dokonce zahájil proces směřující k odstranění IPv4 z jeho mobilní sítě. Podobné ambice pro svou firemní síť ohlásil Microsoft.

Motivace je u všech zmiňovaných podobná. Nedostatek IPv4 adres vede k masivnímu používání neveřejných adres a NATů. Výsledkem je složitá síťová architektura, křehká a obtížně spravovatelná. IPv6 je pro ně provozně jednodušší a v důsledku i levnější. Navíc z měření Facebooku začíná IPv6 vycházet i jako rychlejší, zjevně z podobných příčin.

Více než čtvrtina z tisíce nejnavštěvovanějších webů podle Alexa je přístupná po IPv6. Protokol podporují všechny kořenové DNS servery a je po něm dostupných více než 98 % domén nejvyšší úrovně. Více než čtvrtina autonomních systémů ohlašuje směrovacím protokolem BGP IPv6 prefixy. Mobilní sítě se stávají segmentem, kde IPv6 převažuje nad svým předchůdcem.

Ve světle těchto čísel už není udržitelná teze, že IPv6 je nepodařený akademický[2] experiment, v praxi nepoužitelný. Protokol zjevně používá významná část internetové populace a je třeba se jím zabývat.

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. Síť standardní velikosti má prostor na adresaci 65 tisíc podsítí. A takovýchto sítí je k dispozici bezmála 30 tisíc na každého obyvatele zeměkoule[3]. IPv6 adres je v každém ohledu dost a dost, jak se přesvědčíte v kapitole 3 na straně 65.

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.

2: Oba autoři RFC 1883 sice pracovali pro komerční firmy, ale kdo by si nechal kazit pěkný příběh nějakými fakty.
3: Počítáno pro deset miliard pozemšťanů.

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 společnými parametry), který má opět usnadnit vysokorychlostní zpracování a směrování. Formát datagramu popisuje kapitola 2 na straně 43.

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. Bezstavová konfigurace představuje nový princip, kdy si počítač dokáže sám stanovit svou adresu a naučí se směrovat, aniž by jeho správce kdekoli cokoli konfiguroval. Podpora bezstavové konfigurace je v implementacích povinná a masivně se využívá. Automatickou konfigurací se zabývá kapitola 6 na straně 135.

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 119.

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 225.

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 247.

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 277.

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[4].

Postupem času se ale situace lepšila. Pozitivní roli rozhodně sehrálo *IPv6 Forum* a jeho program *IPv6 Ready*, k nimž se co nevidět dostanu podrobněji. Už nestačilo 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 – stále 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.

Postupem času se z podpory nového protokolu stala v podstatě samozřejmost. Většina výrobců již zrušila na svých webech sekce věnované IPv6, přesunula informace do standardní produktové dokumentace a považuje IPv6 za běžnou záležitost.

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 života. Jistě nejznámějším příkladem je *Wi-Fi*

4: V počáteční fázi hadwarové směrovače často implementovaly IPv6 softwarově, tedy s výkonem řádově nižším proti IPv4.

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.

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. Informace o něm najdete na webu:

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, nebo nebyly několik let aktualizovány. Na titulní stránce ovšem najdete odkazy na významné konference s tematikou IPv6 a další zajímavé zdroje.

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*:

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) ověřovala nejzákladnější kompatibilitu se specifikacemi IPv6. Konkrétně se testovalo, zda zařízení podporuje:

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

Obrázek 1.3: Logo *IPv6 Ready*: vlevo fáze 1, vpravo fáze 2

Testovalo se pouze povinné chování (v RFC označené jako „must“). Od roku 2003 bylo vydáno bezmála 500 certifikátů. Fáze 1 byla určena především pro rané období implementací a byla již ukončena, v současné době lze požádat jen o certifikaci fáze 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),
- DHCPv6,
- SNMP,
- domácí směrovač (CE Router).

Počátkem roku 2019 bylo vydáno přibližně 1850 certifikátů, z toho valná většina v základní kategorii. Vybrané držitele shrnuje tabulka 1.3. Uvádí celkové počty certifikátů a data získání prvního v jednotlivých kategoriích. Aktuální přehled i podrobné informace o testovacích procedurách najdete samozřejmě na stránkách programu *IPv6 Ready*.

platforma/výrobce	*počet*	*hostitel*	*směrovač*	*IPsec konec*	*IPsec brána*	*domácí směrovač*
Cisco	165	2/2011	4/2006		8/2011	
D-Link	178	6/2006	5/2006	11/2007	11/2007	12/2017
Zyxel	21	7/2005	7/2005	11/2007	11/2007	10/2016
Hewlett-Packard	82	5/2005	7/2008	11/2006		
Dell	51	8/2008	11/2006	11/2012		
MS Windows	10	10/2007		1/2008		
MacOS a iOS	5	12/2010				
Linux	36	5/2006	9/2007	5/2006	10/2007	
FreeBSD	2	3/2006	3/2006			

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

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:

🔗 https://www.ipv6forum.com/ipv6_enabled/

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 2500 položek. Do domény *cz* patří 25 z nich, za nejvýznamnější lze považovat *www.vlada.cz* a *www.nic.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. Počátkem roku 2019 počet certifikovaných subjektů převyšoval dvě stovky. Z České republiky se v seznamu nachází osm regionálních poskytovatelů Internetu a jedna housingová firma. Velká jména byste mezi nimi hledali marně.

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 společným prefixem (označovaným jako pTLA). Z něj pak poskytovatel přiděloval části připojeným sítím. Směrovače poskytovatelů disponujících pTLA zároveň tvořily páteř *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. 2006 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 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 požadovalo po vedoucích IT oddělení všech orgánů vlády:

- Do konce září 2012 zpřístupnit všechny služby po IPv6.
- 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:

https://www.nist.gov/programs-projects/usgv6-program

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[5]. Mimo jiné požaduje, aby projekty financované ze 7. rámcového programu 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 tematicky úzce zaměřené výzkumy dílčích oblastí souvisejících s IPv6, třeba projekt *ENABLE* zabývající se mobilitou ve velkých heterogenních IP sítích.

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

5: Obávám se, že zpřístupnění webů „Europa“ a „CORDIS“ po IPv6 v roce 2010 (které se navíc podařilo jen napůl, *cordis.europa.eu* není ani v roce 2019 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.

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 byla dostupná po IPv6 necelá polovina ministerských webů. V usnesení číslo 695 z 26. srpna 2015 pak vláda nařídila, že lajdáci mají IPv6 už ale doopravdy nasadit do 1. ledna 2016. Možná vás proto překvapí, že počátkem roku 2019 stále ještě pět ministerstev (vnitra, zahraničí, dopravy, zemědělství a pro místní rozvoj) nemá weby přístupné po IPv6. 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. Vládní aktivity ovšem nejsou samospásné. Příkladem budiž Čína, která sice v roce 2003 přijala pětiletý strategický plán *China Next Generation Internet* a v jeho rámci skutečně vybudovala IPv6 páteř, ovšem ještě v roce 2018 se podpora IPv6 v jejích sítích pohybovala v jednotkách procent a představovala největší brzdu mezi velkými zeměmi.

Vypadá to nicméně, že druhý pokus uspěje. V roce 2017 Čína vyhlásila plán masivního nasazení IPv6, který by měl do roku 2020 zpřístupnit nový protokol 500 milionům uživatelů. Na přelomu let 2018 a 2019 začal počet čínských uživatelů IPv6 dramaticky růst a vše nasvědčuje tomu, že nejvýznamnější temné místo na mapě IPv6 zmizí.

IPv6 podle všeho konečně dosáhlo kritického množství a začíná se prosazovat samospádem. Díky tomu vládní aktivity klesají na významu a protokol se nasazuje nikoli kvůli nařízení XY, ale protože to je normální.

1.8 Webové zdroje

Na webu pochopitelně najdete nepřeberné množství stránek věnovaných IPv6. Podívejme se na ty, které stojí za pozornost. Internet Society nabízí „základní informační balíček“ na adrese:

https://www.internetsociety.org/deploy360/ipv6/

Najdete tu základní informace o protokolu a jeho součástech, odpovědi na často kladené dotazy i provozní doporučení postupů, které se v praxi osvědčily. Zajímavý je přehled různých statistik souvisejících s IPv6:

https://www.internetsociety.org/deploy360/ipv6/statistics/

Pokud se týče doporučených postupů, cenným zdrojem je i stránka APNIC, která se zabývá adresováním, přechodovými mechanismy, datovými centry i firemními sítěmi:

https://www.apnic.net/community/ipv6-program/ipv6-bcp/

Trudnomyslným mohu doporučit *IPv4 Address Report*, kde Geoff Huston zkoumá postupné vyčerpání adres a stav IPv4 Internetu:

https://ipv4.potaroo.net/

A za pozornost rozhodně stojí dokumenty o IPv6 evropského správce adresního prostoru RIPE NCC:

https://www.ripe.net/publications/docs/ripe-documents/ipv6-documents

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

https://www.ipv6.cz/

O jeho 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.

Část I

Jak funguje IPv6

2 Formát datagramu

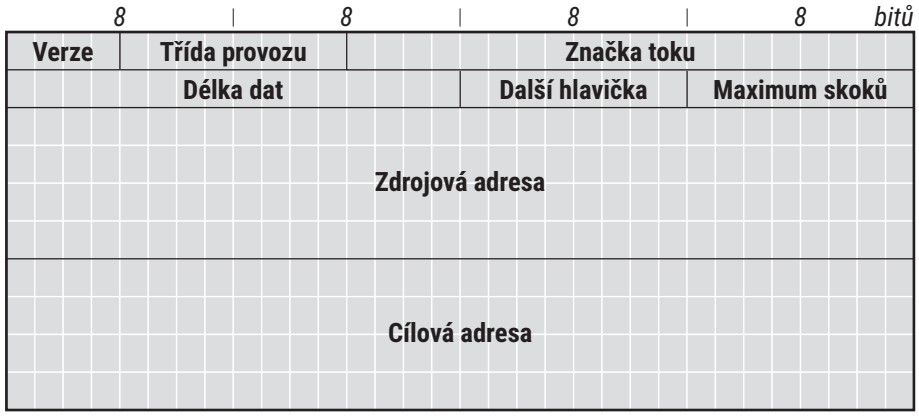
Základním kamenem IPv6 je dokument RFC 8200: *Internet Protocol, Version 6 (IPv6) Specification*, který obsahuje především základní principy a formát datagramu. Ostatním mechanismům a datovým formátům, které souvisejí s IPv6, jsou věnovány další RFC specifikace.

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 části 2.2 na straně 46.

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

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

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.

Dalších 20 bitů je věnováno *Značce toku (Flow label)*. Koncepce toku je novinkou v IPv6 a stále ještě se trochu tápe, k čemu a jak ji využívat. V zásadě by jako tok měl být označován proud datagramů se společnými vlastnostmi (odesilatel, adresát, požadavky na vlastnosti spojení). Prostřednictvím identifikátoru (značky) a dvojice adres 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 pokusy o konkrétní využití teprve vznikají. K tématu se vrátím v části 2.9 na straně 61.

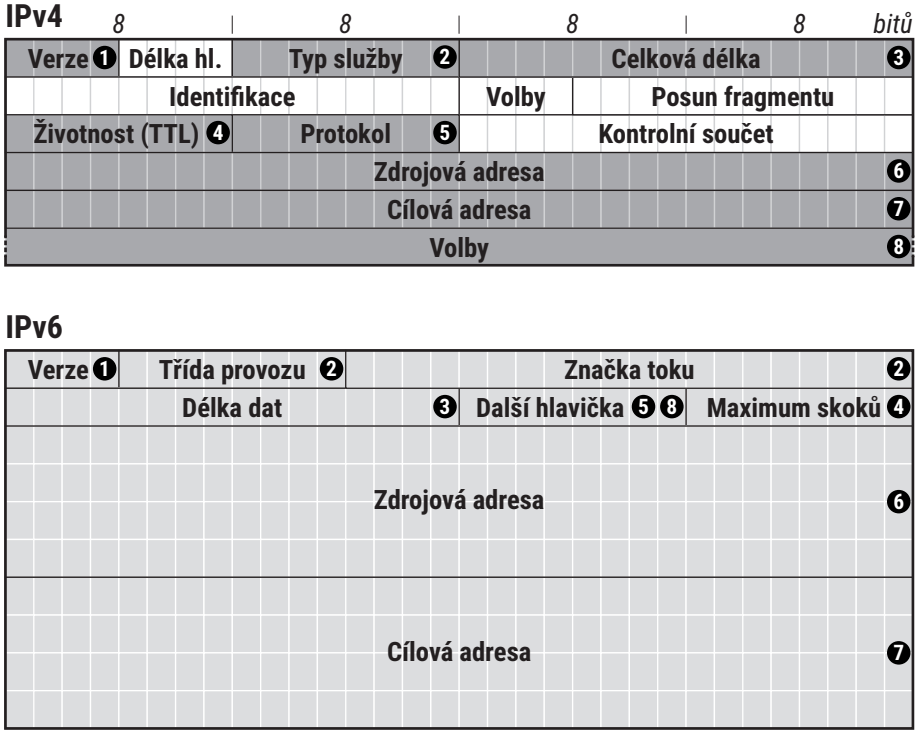
Délka dat (Payload length) nese údaj o délce datagramu. Přesně řečeno počet bajtů následujících za standardní hlavičkou. Z toho plyne, že základní hlavička se do této délky nepočítá, zatímco případné rozšiřující hlavičky ano. Jelikož je položka dvoubajtová, je maximální délkou 64 KB. Pomocí rozšiřující hlavičky *Jumbo obsah* popsané v části 2.7 na straně 60 lze teoreticky vytvářet ještě delší datagramy, reálně je ale nikdo nikdy neviděl.

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.

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).

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 65.

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.



Obrázek 2.2: Porovnání hlaviček IPv4 a IPv6

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 nebo Wi-Fi s MTU alespoň 1500 B, lze očekávat, že tato hodnota 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) a pokud došlo ke zkomolení při přenosu, datagram rovnou zahodí. Na úrovni IP by se jen duplikovala úspěšná kontrola. 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. Zastupuje tak zároveň dřívější položku *Protokol*. Nejvýznamnější hodnoty shrnuje tabulka 2.1. První skupina v ní obsahuje hlavičky, jejichž implementace je podle RFC 8200 povinná. Ve druhé skupině jsou hlavičky nepovinné, následují kódy přiřazené přenášeným protokolům. Aktuální a kompletní seznam hodnot pro typy přenášených dat najdete na adrese:

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

Pokud tedy datagram neobsahuje žádné rozšiřující 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

hlavička **IPv6** další=6 (TCP)	**TCP segment**

b) s hlavičkou *Směrování*

hlavička **IPv6** další=43 (směr.)	hlavička **Směrování** další=6 (TCP)	**TCP segment**

c) s hlavičkami *Směrování* a *Fragmentace*

hlavička **IPv6** další=43 (směr.)	hlavička **Směrování** další=44 (frag.)	hlavička **Fragmentace** další=6 (TCP)	**TCP segment**

Obrázek 2.3: Zřetězení hlaviček datagramu

Rozšiřující hlavičky – povinné	
0	volby pro všechny (hop-by-hop options), str. 51
43	směrování (routing), str. 54
44	fragmentace (fragment), str. 55
50	šifrování obsahu (ESP), str. 232
51	autentizace (AH), str. 231
60	volby pro cíl (destination options), str. 51
Rozšiřující hlavičky – volitelné	
135	mobilita (mobility), str. 249
139	identita (Host Identity Protocol), experimentální
140	Shim6, str. 107
253	pro experimenty a testování
254	pro experimenty a testování
Typ nesených dat (protokol)	
6	TCP
8	EGP
9	IGP
17	UDP
46	RSVP
47	GRE
58	ICMP
59	poslední hlavička (no next header)

Tabulka 2.1: Vybrané hodnoty položky *Další hlavička*

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 ve složitějších případech 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.

Tento problém řeší IPv6 velmi jednoduše – doporučuje pro rozšiřující hlavičky 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.

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*.

RFC 8200 důrazně doporučuje dodržovat výše uvedená omezení, zároveň ale požaduje, aby byl adresát schopen se vyrovnat s libovolným pořadím hlaviček i jejich případným opakováním. Výjimkou z této benevolence jsou *Volby pro všechny* – pokud jsou přítomny, musí být hned na začátku řetězce.

Druhým striktním omezením je, že dojde-li k fragmentaci datagramu, musí být všechny rozšiřující hlavičky obsaženy v prvním fragmentu. Velmi dlouhé řetězce hlaviček komplikovaly situaci firewallům a objevily se i snahy o jejich zneužití. Podrobnější zdůvodnění najdete v RFC 7112: *Implications of Oversized IPv6 Header Chains*.

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. Takový datagram nenese žádná data. Pokud podle své délky obsahuje ještě nějaká data, musí být ignorována. Je-li datagram přeposílán dále, musí do něj předávající tato data zkopírovat beze změny.

Kromě *Voleb pro všechny* zpracovává hlavičky až adresát datagramu. Mezilehlá zařízení rozšiřující hlavičky nezpracovávají a nesmí je měnit. Výjimku představují *Volby pro všechny*, jimiž se naopak zabývá každé zařízení, jímž datagram prochází[1].

Při zpracování se hlavičky procházejí v tom pořadí, ve kterém jsou vloženy do datagramu. Zpracovávající stroj nesmí přeskakovat nebo si vybírat některé přednostně. Tím je zajištěna konzistence v případech, kdy by některá hlavička ovlivňovala ty následující.

Koncept zřetězení rozšiřujících hlaviček se výrazně liší od přístupu IPv4. Bylo s ním proto méně zkušeností a v praktickém provozu se projevily různé problémy. Týkají se například příliš přísně nastavených firewallů, které zahazovaly datagramy s neznámými typy rozšiřujících hlaviček a bohužel neznaly zdaleka všechny. Objevily se také útoky postavené na rozšiřujících hlavičkách, které vedly například k odmítnutí některých variant hlavičky *Směrování*.

IETF se snaží praktické zkušenosti promítat do specifikací a vyjasňovat problematická místa. Zde mám na mysli především RFC 7045: *Transmission and Processing of IPv6 Extension Headers*, které se zabývá zejména přepravou a zpracováním rozšiřujících hlaviček v mezilehlých strojích – směrovačích, firewallech a dalších zařízeních, která nejsou odesilatelem ani adresátem datagramu.

Obecně pro ně platí, že by složení rozšiřujících hlaviček nemělo ovlivňovat přepravu datagramu[2]. Od přepravujících strojů se neočekává, že budou analyzovat celý datagram včetně všech hlaviček. Měly by přezkoumat nezbytné minimum a paket odeslat.

Speciálním případem jsou firewally a další prvky, které naopak datagramy analyzují podrobně, často využívají i informace z protokolu transportní vrstvy, takže musí projít celým řetězcem až k neseným datům. V jejich případě RFC 7045 stanoví následující požadavky:

- Musí podporovat a korektně zpracovávat všechny standardní typy rozšiřujících hlaviček a měly by i typy experimentální.
- Pro standardní typy rozšiřujících hlaviček musí nabídnout individuálně konfigurovatelná pravidla, jak mají být zpracovány. V nich lze stanovit, že datagram lze zahodit na základě přítomnosti konkrétní hlavičky, případně s určitou hodnotou. Implicitně by měly být všechny standardní hlavičky propouštěny.

1: RFC 8200 požaduje, aby zpracování *Voleb pro všechny* bylo možné zapnout/vypnout v konfiguraci.
2: Samozřejmě s výjimkou hlaviček určených pro každý stroj po cestě, které jsou naopak k tomuto účelu určeny.

- Pro experimentální typy rozšiřujících hlaviček jsou požadavky slabší – opět se požadují individuálně nastavitelná pravidla, tentokrát však specifikace připouští jejich zahazování v implicitní konfiguraci.

Firewall samozřejmě může datagram zahodit, pokud vyhodnotí určité jeho rozšiřující hlavičky a hodnoty v nich jako nebezpečné, ale nesmí to v případě standardních hlaviček udělat jen na základě toho, že daný typ nezná.

Pokud se týká hlaviček pro každého, ty by naopak měly být zpracovávány každým zařízením, jímž datagram projde. RFC 7045 ale upozorňuje, že vysokorychlostní směrovače a přepínače to často nedělají a vývojáři by s tím měli počítat.

K usnadnění zpracování rozšiřujících hlaviček přispívá i RFC 6564: *A Uniform Format for IPv6 Extension Headers*, které požaduje, aby nově definované rozšiřující hlavičky dodržovaly jednotný formát: v prvním bajtu *Další hlavička*, ve druhém délka této hlavičky v osmicích bajtů (bez úvodní osmice) a za ní následuje vlastní hodnota, jejíž strukturu a položky stanoví konkrétní specifikace. Jednotné zahájení usnadní a zrychlí zpracování a umožní zařízení jednoduše přeskočit hlavičku, která zde není podporována.

Zároveň je RFC 6564 velmi konzervativní ohledně přidávání typů rozšiřujících hlaviček. Jednoznačně dává přednost předávání doplňkových informací pomocí *Voleb pro cíl*. Vytváření nových typů rozšiřujících hlaviček a nových typů *Voleb pro každého* připouští jen v případě, kdy potřebné informace nelze předávat jiným způsobem. Jejich návrh to musí doložit. Bez výjimky pak zakazuje vytváření nových typů hlaviček, které by vyžadovaly zpracování všemi průchozími zařízeními.

Zajímavá a dost depresivní jsou měření průchodnosti datagramů s rozšiřujícími hlavičkami, která najdete v RFC 7872: *Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World*. Výsledky pocházejí z let 2014 a 2015 a vůbec nejsou lichotivé – přítomnost některé z rozšiřujících hlaviček zvýší pravděpodobnost zahození daného datagramu řádově o desítky procent. Například pakety obsahující fragmentační hlavičku nebyly doručeny zhruba ve třetině případů.

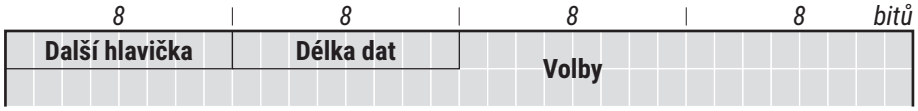
Tyto hodnoty jsou alarmující a je třeba se smířit s tím, že pokud odesilatel vloží do datagramu rozšiřující hlavičku, výrazně tím sníží jeho šanci na úspěšné doručení současným Internetem. Autoři RFC 7872 apelují na zlepšení situace, ale výsledkem může být i to, že programátoři se budou snažit posílání těchto hlaviček vyhýbat.

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

2.3 Volby

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 (Options)* pak obsahuje vlastní volby. Ty mohou být zavedeny jako součást jednotlivých konkrétních mechanismů. Například v rámci podpory mobilních počítačů se objevila volba *Domácí adresa*. Přehled doposud definovaných voleb najdete v tabulkách 2.2 a 2.3. 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.

Typ	*Význam*	*Popis*
0	Pad1	str. 51
1	PadN	str. 52
5	Upozornění směrovače	str. 53
7	CALIPSO	RFC 5570
8	SMF	RFC 6621
38	Rychlý start	str. 61
99	RPL	RFC 6553
109	MPL	RFC 7731
194	Jumbo obsah	str. 60
238	DFF	RFC 6971

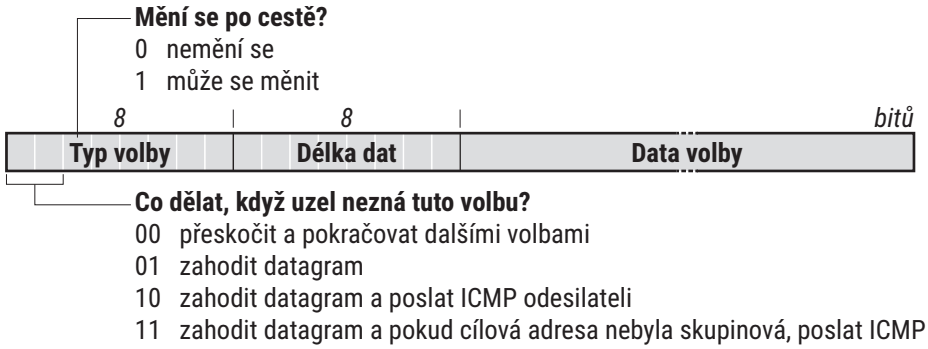
Tabulka 2.2: Volby pro všechny

Typ	*Význam*	*Popis*
0	Pad1	str. 51
1	PadN	str. 52
4	maximální vnoření tunelů	RFC 2473
15	PDM (měření)	str. 54
139	náhodná hodnota pro ILNPv6	RFC 6744
140	LIO (identifikátor linky)	RFC 6788
201	Domácí adresa	str. 263

Tabulka 2.3: Volby pro příjemce

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 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

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.

Jednou z „opravdových" voleb pro všechny je tak zvané *Upozornění směrovače (router alert)* definované v RFC 2711. 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 paket RSVP, 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)
69	MPLS OAM (RFC 7506)

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*.

V RFC 8250: *IPv6 Performance and Diagnostic Metrics (PDM) Destination Option* byla zavedena volba pro příjemce označovaná zkratkou PDM, která je určena pro měření zpoždění a spolehlivosti přenosů. Obsahuje pořadová čísla paketů a časové rozdíly mezi odeslanými a přijatými pakety.

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.

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.

Funguje to tak, že se jako cílová adresa do datagramu vloží první průchozí bod. Když do něj datagram dorazí, přesune se jeho adresa do hlavičky *Směrování* jako hotová a cílem se stane další z průchozích bodů – a tak dál až do skutečného cíle.

Tento mechanismus je bohužel zneužitelný k útokům usilujícím o zahlcení přenosových tras. Útočník 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[3], navíc i na velmi dlouhé trase.

3: Prakticky byl předveden 88násobek.

Důsledkem bylo zrušení směrovací hlavičky typu 0 v 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 konečným cílem celého řetězce. V opačném případě musí datagram zahodit a ohlásit jej odesilateli jako chybný. Kromě toho se zde doporučuje datagramy s tímto typem hlavičky *Směrování* filtrovat na aktivních prvcích.

Typ 2 byl definován speciálně pro mobilitu. De facto se jedná o silné zjednodušení obecnějšího typu 0 s jedinou adresou. 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 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 263 v kapitole o mobilitě, kde se dočtete i podrobnější informace o jejím fungování.

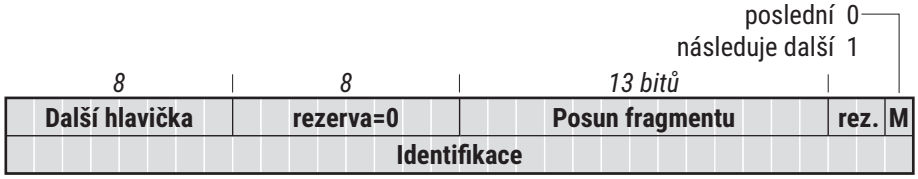
2.5 Fragmentace

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.

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.

Analogickou techniku používá i protokol IPv4, liší se však v několika důležitých detailech. Zatímco v IPv4 může datagram fragmentovat libovolný směrovač po cestě (kdykoli má být odeslán linkou, jejíž MTU je 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.

Rozšiřující hlavička *Fragmentace (Fragment)* je identifikována kódem 44 v položce *Další hlavička* svého bezprostředního předchůdce. Její tvar vidíte na obrázku 2.7. Velikost je konstantní a kromě obvyklé *Další hlavičky* obsahuje tři informační položky.



Obrázek 2.7: 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. Původně se používalo prosté zvětšování jeho hodnoty, jenže se objevily různé druhy útoků, které zneužívaly předvídatelné identifikátory. Proto řada současných implementací dává přednost pseudonáhodným či kryptografickým metodám. Podrobněji se problematice věnuje RFC 7739: *Security Implications of Predictable Fragment Identification Values*.

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).

Hlavičky pro všechny fragmenty	Rozšiřující hlavičky a hlavička vyšší vrstvy	Fragmentovatelná část

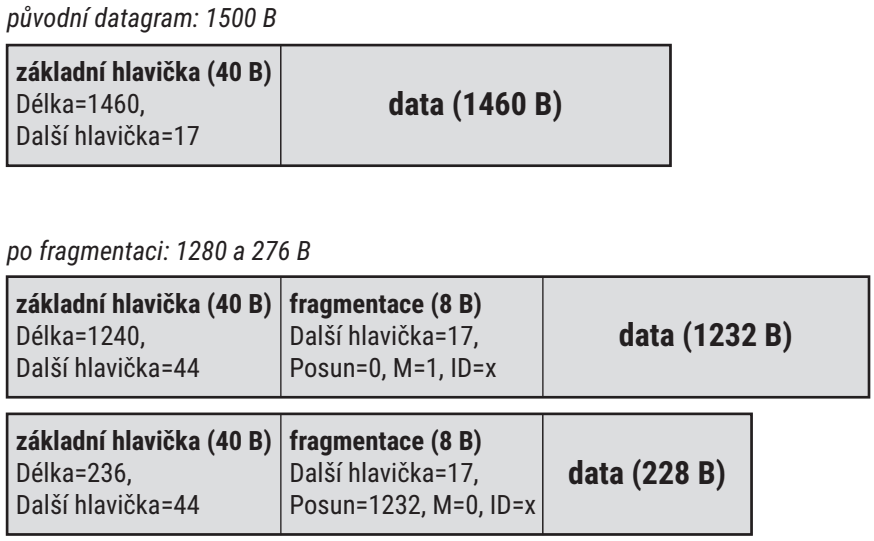
Obrázek 2.8: Části datagramu při fragmentaci

Má-li dojít k fragmentaci, vymezí se v původním datagramu tři části:

- Začátek tvoří hlavičky, které je třeba zopakovat (byť s drobnými změnami) ve všech fragmentech. Patří sem základní hlavička a všechny po ní následující rozšiřující hlavičky až po *Směrování* (včetně).
- Do druhé části patří zbývající rozšiřující hlavičky a hlavička transportní vrstvy, kterou začínají data. Tato část se musí vejít do prvního fragmentu.
- Zbytek datagramu je považován za *fragmentovatelnou část*. Rozdělí se na části tak, aby se výsledné fragmenty vešly do příslušného MTU a délka každého z nich (kromě posledního) byla násobkem osmi.

Datagramy obsahující jednotlivé fragmenty jsou sestaveny následovně:

- Převezmou se hlavičky pro všechny fragmenty z původního datagramu. Jedinými změnami, které se v nich pro jednotlivé fragmenty provedou, je úprava *Délky* v základní hlavičce, aby odpovídala skutečné délce fragmentu, a změna hodnoty poslední *Další hlavičky* na 44.
- Za ně 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 původní poslední *Další hlavičky* společné části hlaviček, která byla přepsána hodnotou 44.
  - *Posun* každého fragmentu se určí jako počet osmic bajtů, o které je jeho začátek vzdálen od začátku fragmentovatelné části původního datagramu. První fragment bude mít *Posun* nulový, u následujících je tvořen součtem délek fragmentů nesených předchozími pakety. Fragmenty se nesmí překrývat.
  - Poslednímu fragmentu se příznak *M* nastaví na 0, ostatním na 1.
- Na konec se připojí dotyčný fragment (úsek fragmentovatelné části původního datagramu).



Obrázek 2.9: Fragmentace datagramu

Příklad celého postupu vidíte na obrázku 2.9. 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 frag-

menty 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.

Fragmentace bohužel způsobuje řadu potíží a významně snižuje pravděpodobnost úspěšného doručení datagramu. Například firewally běžně zkoumají údaje transportního protokolu TCP nebo UDP, protože propouštějí jen povolené porty. Některé jsou nastaveny tak, že pokud datagram neobsahuje hlavičku transportního protokolu, zahodí jej. Ta je ovšem jen v prvním fragmentu. Popsaným typem firewallu projde vždy jen první fragment, zbývající jsou zahozeny a příjemce si původní datagram nikdy nesloží[4].

Další problém způsobuje zahazování ICMP zpráv, které se v Internetu stalo celkem běžným. Odesilatel se díky němu nemusí dozvědět, že paket neprošel a měl by jej rozdělit na menší.

A aby toho nebylo málo, fragmentaci lze zneužít k různým útokům. Řekněme, že v cestě je rozumný firewall, který sice kontroluje hlavičku transportní vrstvy, ale pokud propustí první fragment, povolí i jeho pokračování. Pak lze provozovat různé ošklivé triky, kdy útočník prvnímu fragmentu vloží do transportní hlavičky spořádané údaje, aby jej firewall propustil. Druhý fragment ponese ovšem nulový nebo velmi malý *Posun* a při skládání přepíše transportní hlavičku svého předchůdce nebo její část. Takto lze změnit porty, příznaky TCP, ledacos.

V reakci na triky s překrýváním fragmentů vzniklo RFC 5722: *Handling of Overlapping IPv6 Fragments*, které překrývání zakázalo. Odesilatel musí zajistit, že se fragmenty vzájemně nepřekrývají. A na druhé straně pokud příjemce zjistí, že se fragmenty přicházejícího datagramu překrývají, musí jej celý potichu zahodit.

Obecně je nejlepší se fragmentaci pokud možno vyhnout. Tím se dostáváme k velikosti datagramů.

2.6 Velikost datagramů

Zvolit optimální velikost datagramů je docela tvrdý oříšek. 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

4: Situace je o to lepší, že testovací *ping* projde, protože posílá jen krátké pakety. Spojení se tedy při letmém testu jeví jako funkční, ovšem aplikace, která posílá dlouhé datagramy, po něm nic nepřenese.

a snižovala se tak nadbytečná zátěž. Na druhé straně však musí být natolik malé, aby nikde po své cestě nepřekročily MTU a nedocházelo k fragmentaci.

O dosažení tohoto kompromisu se snaží algoritmus nazvaný objevování MTU cesty. Definuje jej RFC 8201: *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, může dojít 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 by některá technologie nedokázala přepravovat datagramy této velikosti, musí na úrovni linkové vrstvy zajistit kouskování a skládání paketů tak, aby pro IPv6 nabídla alespoň 1280 B.

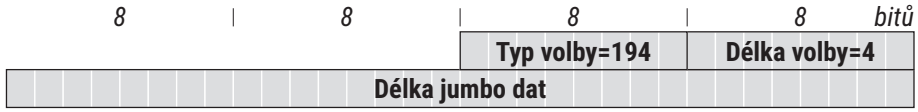
Objevování MTU cesty lze používat i pro skupinové adresy. V tomto případě může dostat na jeden datagram celou řadu ICMP zpráv. Bude se chovat podle očekávání – použije nejmenší ohlášenou hodnotu.

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. Jumbogramy poskytují nástroj, jak přepravovat ještě delší pakety. Nesetkaly se ovšem s reálným nasazením, proto byly z poslední verze požadavků na IPv6 uzel (RFC 8504) odstraněny a lze je považovat za opuštěné.

Jumbogramy zavedlo RFC 2675: *IPv6 Jumbograms*. Jejich základem je volba *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.



Obrázek 2.10: Volba *Jumbo obsah*

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 hlavička). Jumbogramy totiž nesmí být fragmentovány. Uzly, které nemají tak velké MTU, nemusí jumbogramy podporovat a ani této volbě rozumět.

Příliš velké datagramy ale vadí i protokolům vyšší vrstvy. Jak UDP, tak TCP počítá s maximální délkou paketu 65 535 bajtů. RFC 2675 obsahuje návrhy na úpravy kódu transportní vrstvy, které by se s těmito omezeními vypořádaly. Vzhledem k tomu, že jumbogramy byly odsunuty do pozice zajímavé kuriozity, nemá cenu se jim více věnovat.

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 prin-

cipu věci je dešifrovat umí jen příjemce. Nebo sice jsou dostupné, ale cesta k nim vede dlouhou sekvencí rozšiřujících hlaviček a zbytečně zpracující zařízení zdržuje.

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 neřešilo vůbec, odložilo 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.

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 hašování a omezení bezpečnostních rizik. Jako vhodné generátory značek dokument zmiňuje hašovací funkci nebo generátor pseudonáhodných čísel. Naopak výslovně nedoporučuje sekvenční přiřazování, kdy každá další značka je o jedničku větší než poslední použitá.

Během přepravy sítí se značka nesmí měnit a musí být příjemci doručena se stejnou hodnotou, jakou jí přidělil odesilatel. Z tohoto obecného pravidla 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 výjim-

kou je nulová značka. Jestliže se odesilatel rozhodl datagram neznačkovat, může to za něj udělat některý ze směrovačů[5]. 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[6]. 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. RFC 7098: *Using the IPv6 Flow Label for Load Balancing in Server Farms* později přišlo s návrhem využít značky toků k distribuci paketů v rámci serverové farmy.

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.

5: Typickými kandidáty pro takové chování jsou přístupový směrovač koncové sítě nebo vstupní směrovač poskytovatele Internetu.

6: Ale podle RFC 8504 by toky měly být podporovány v každém zařízení implementujícím IPv6.