Česká zemědělská univerzita v Praze

Technická fakulta

Porovnání finanční a materiálové náročnosti návrhu komerční počítačové sítě IPv4 vs. IPv6

Bakalářská práce

Vedoucí práce: Ing. Zdeněk Votruba, Ph.D.

Autor práce: Michal Musil

PRAHA 2020

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Michal Musil

Zemědělské inženýrství
Informační a řídicí technika v agropotravinářském komplexu

Název práce

Porovnání finanční a materiálové náročnosti návrhu komerční počítačové sítě IPv4 vs IPv6.

Název anglicky

Comparison of the financial and material intensity of the proposal commercial network IPv4 vs. IPv6.

Cíle práce

Na základě literární rešerše, informací od poskytovatele služeb i na základě vlastních zjištění definovat možný přechod od IPv4 na IPv6 pro běžnou komerční firmu. Navrhnout vhodnou koncepci přechodu z pohledu minimalizace výpadků služeb, finanční náročnosti a organizačních změn. Porovnat tyto náklady s případným ziskem, který tato změna přinese.
Na několika modelových situacích (malá firma, bytový komplex,...) ukázat rozdíl v návrzích sítí s podporou IPv4 a IPv6 ready. Zpracovat a porovnat cenové kalkulace.
Uvedený proces zobecnit a formulovat obecně platné závěry.

Metodika

1. Úvod
2. Cíl práce
3. Metodika
4. Varianty technického řešení a jejich porovnání
5. Definice kritických míst jednotlivých řešení
6. Návrh konkrétního řešení
7. Vyjádření finanční, organizační náročnosti ve vztahu k přínosu řešení
8. Závěr a hodnocení

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

IPv6, počítačová síť, QoS, ekonomická rozvaha

Doporučené zdroje informací

internetové zdroje, zvláště pak: https://www.cesnet.cz/sluzby/pripojeni/ipv6/

PAVEL SATRAPA: IPv6 – třetí vydání, NIC.CZ, https://knihy.nic.cz/files/edice/ipv6_2012.pdf

PODERMAŃSKI Tomáš. IPv6 Mýty a skutečnost, díl I. – Jak jsme na tom. Lupa.cz. Praha: Internet Info s.r.o, 2011, roč. 2011, č. 1, s. 9. ISSN 1213-0702.

Shannon McFarland, Muninder Sambi, Nikhil Sharma, Sanjay Hooda: IPv6 Kompletní průvodce nasazením v podnikových sítích, COMPUTER PRESS, 2011

Předběžný termín obhajoby

2019/2020 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 18. 1. 2017

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 1. 2017

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 08. 03. 2020

Čestné prohlášení:

„Prohlašuji, že jsem práci Porovnání finanční a materiálové náročnosti návrhu komerční počítačové sítě IPv4 vs IPv6 vypracoval samostatně a použil jen prameny, které cituji a uvádím v seznamu použitých zdrojů. Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby. Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí. Jsem si vědom, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

V Praze dne 26. 3. 2019 ……

Michal Musil

Na tomto místě bych rád poděkoval vedoucímu mé bakalářské práce, Ing. Zdeňku Votrubovi, Ph.D. za cenné rady, informace, připomínky, za ochotu a čas při konzultacích, a především za nezměrnou trpělivost.

Abstrakt: Práce porovnává protokoly IPv4 a IPv6 především z hlediska rozdílností prvků v počítačové síti a finanční náročnosti jejich implementace do sítě. První část práce se věnuje vývoji, rozdílnosti protokolů a jejich nárokům na hardware. Zároveň předkládá zhodnocení současného stavu použití obou protokolů v počítačových sítích. Druhá část poté pracuje s návrhy počítačových sítí pro malou firmu a bytový komplex a porovnává jejich rozdíly ve výbavě a ceně při použití jednotlivých protokolů. Závěrem je shrnuje výsledky a subjektivní představu autora práce o budoucím vývoji ohledně implementace protokolů v počítačových sítích.

Klíčová slova: IPv4; IPv6; síťový protokol; počítačová síť

Comparison of the financial and material intensity of the proposal commercial network IPv4 vs. IPv6

Abstract: The thesis compares the IPv4 and IPv6 protocols and focuses on the differences between the elements of the two protocols in a computer network and the financial costs of implementing the protocols in a network. The first part of the thesis discusses the development of the protocols, the differences between them, and their hardware requirements. It also provides an assessment of the current state of the utilization of both of the protocols in computer networks. The second part reviews proposals for computer networks for a small company and for an apartment complex and notes the differences between the two proposals as to equipment and price when utilizing the two protocols. The thesis summarizes the results and presents the author’s prediction of the future development of the implementation of the protocols in computer networks.

Key words: IPv4; IPv6; network protocol; computer network

Obsah

1 Úvod

Internet, obrovská celosvětová síť propojených počítačů, tabletů, mobilních telefonů a mnoha dalších zařízení. Za světové populace 7,75 miliard lidí (2019) využívá nějakým způsobem internet více než polovina – 53,6 %. V tzv. rozvinutých zemích je toto číslo dokonce mnohem větší – 86,6 %. V České republice pak podle statistik ČSÚ v roce 2019 internet využívalo cca 80 % obyvatel. 4 z 5 je velké číslo, na druhou stranu podle stejné statistiky žije v ČR stále 1,3 milionu lidí, kteří internet nikdy k ničemu nevyužili. Není ovšem pochyb, že počet uživatelů internetu bude v dohledné celosvětově pouze přibývat. Internet obrovskému množství vzájemně propojených uživatelů poskytuje téměř neomezené a nevyčíslitelné možnosti. Nejen jako nástroj pro sdílení a získávání informací, ale i jako zdroj zábavy, práce, výdělku a v dnešní době také jako prostředek k sociálnímu vyžití.

Je nemyslitelné, že v šedesátých letech 20. století při vývoji experimentální sítě Arpanet, kterou obecně považujeme za zárodek toho, čemu dnes říkáme internet, si někdo dokázal představit, jakých rozměrů celosvětová síť dosáhne. Zároveň je nemožné, aby všechno, co bylo navrženo původně pro 4 propojené počítačové uzly fungovalo stejně dobře pro 3,9 miliardy uživatelů. Samozřejmě tomu tak ani nebylo a jednotlivé mechanismy propojení uživatelů si v průběhu let prošly vývojem. Tímto vývojem si prošel i IP protokol bez kterého by jakékoli propojení počítačů bylo dnes nemyslitelné. Jako u spousty věcí v životě jsme i přes veškerou snahu narazili na hranici jeho další použitelnosti. Nová verze IP protokolu, která řeší všechny limity a nedostatky se ale od protokolu původního příliš liší, a nejen to částečně brzdí jeho rozšíření.

2 Cíl práce

Cílem práce je porovnat protokoly IPv4 a IPv6 z hlediska materiálové a finanční náročnosti při jejich implementaci v počítačové síti. Tedy porovnání protokolu IPv4, který je užíván celosvětově již léta, a jeho inovované verze IPv6, která řeší nedostatky v protokolu původním. Toto porovnání je provedeno na modelových příkladech menší firmy a bytového komplexu, které autor práce považuje za dva sektory, kam se, vzhledem k současnému stavu, bude třeba ubírat v implementaci protokolu IPv6.

Zároveň autor předkládá informace o stručné historii obou protokolů a jejich rozdílech a současném stavu implementace protokolu IPv6 a jeho podílu na přenosu informací prostřednictvím počítačové sítě v ČR a ve světě.

3 Metodika

Základem pro vytvoření práce byla hloubková rešerše a důkladné prostudování dostupných zdrojů. Kvůli charakteru popisované problematiky, značnou část tvoří internetové zdroje. Výběrem informací relevantních pro popisovanou problematiku a jejich syntézou vznikl text, který je dělen do několika částí. Úvodní část práce za pomoci získaných informací analyzuje přenosové protokoly IPv4 a IPv6 z hlediska vzniku a vývoje. Řeší problematiku a míru implementace jednotlivých přenosových protokolů v rámci dnes již neodmyslitelného a denně používaného přenosového media, označovaného jako internet. Dále pak porovnává protokoly na dvou příkladech jejich možné implementace. A to do sítě menší firmy a do sítě obytného komplexu. Následuje zhodnocení výsledků a výhled do budoucnosti implementace IPv6 v počítačových sítích.

4 Protokol TCP/IP

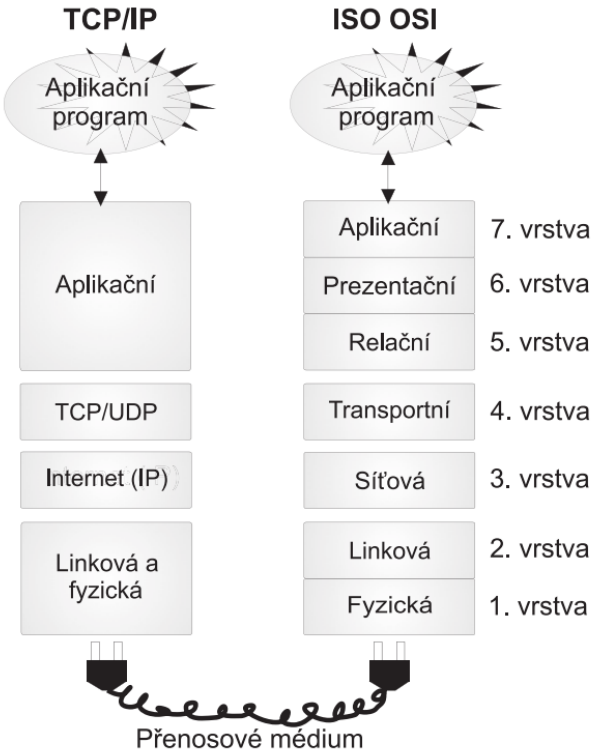
4.1 Potřeba komunikačního protokolu

Již v druhé polovině 20. století, ještě před příchodem mikroprocesorů, kdy měly počítače velmi daleko k tomu, abychom je nazývali „osobní“ (Personal Computer), začala být, mezi tehdejším stále se zvyšujícím počtem strojů, čím dál zřetelnější potřeba nějakým způsobem data sdílet. Řešení tohoto problému se ujímají vědecká centra ve Velké Británii, Spojených státech, ale také ve Francii. Tou dobou spolu počítače komunikují pomocí přidělených linek vedoucích od jednoho k druhému. Tedy tak, jak se tehdy řešil i obyčejný telefonní hovor. Nicméně je to až zakázka amerického ministerstva obrany z konce 60. let, která přichází s řešením tzv. přepínání paketů, kdy spolu na stejné síti může komunikovat zároveň více dvojic. Aby bylo možno v síti rozlišit, od koho která data pochází a komu jsou určena, bylo nutno implementovat jednotný komunikační protokol. Vytvořené řešení je původní IP (Internet Protocol).

4.2 Adresace IPv4

Rodina protokolů TCP/IP je bezesporu dominantní při komunikaci v současném internetu (zásluhou například propracovaného adresního schématu směrování pro velké sítě).

Za zmínku ještě minimálně jeden protokol vyvinutý pro stejné účely, a to ISO/OSI, který byl vyvinut jako referenční model pro vytvoření normy v propojování systémů. Jednu dobu se i zdálo, že upozadí rodinu TCP/IP. Model ISO/OSI na rozdíl od modelu TCP/IP, který má čtyři nebo pět vrstev, sedmivrstvý a natolik odlišný (obr. 2), že je s TCP/IP neporovnatelný. Nicméně na vrstvě linkové a na vrstvě síťové jsou si velmi podobné. TCP/IP navíc neřeší (až na výjimky) linkovou a fyzickou vrstvu. V současném internetu se tedy setkáme se směsicí TCP/IP, ISO/OSI a ITU (dříve standard pro hlasové hovory, vychází z něj například GSM). ISO/OSI a ITU najdeme téměř výhradně pouze na spodních dvou vrstvách, linkové a fyzické. [2]



Obr. 1 Porovnání TCP/IP a ISO/OSI. [2]

4.2.1 Historie

V roce 1974 vydává IEEE (Institute of Electrical and Electronics Engineers) článek nazvaný „A Protocol for Packet Network Intercommunication“. Autory jsou Vint Cerf a Bob Kahn [1]

Během následujících let prochází IP, stále ještě jako experimentální, dalším vývojem ve snaze ho zdokonalit a zrychlit. Je vytvořen a následně zdokonalován návrh hlavičky, část starající se o přenos se vyčleňuje ven jako samostatný protokol TCP (Transmission Control Protocol), UDP (User Datagram Protocol) se usazuje na transportní vrstvě atp. Dílčí verze jsou značeny jako IPv0 až IPv3.

V červnu roku 1978 přichází nová verze mimo jiné s opět přepracovanou hlavičkou a označením IPv4. V září stejného roku je IPv4 standardizován v RFC 760.

4.2.2 Popis protokolu

Jak již bylo zmíněno, TCP/IP je model sestávající se z více vrstev. Komunikují spolu vždy dvě stejné vrstvy dvou různých systémů za pomoci vrstev nižších. Tento návrh umožňuje komunikaci protokolů jedné vrstvy bez dopadu na vrstvy ostatní. Struktura a funkce jednotlivých vrstev je analyzována v následujících bodech.

4.2.3 Fyzická vrstva

Zabývá se signály používanými v komunikaci mezi bezprostředními komunikačními sousedy (např. elektromagnetickými, elektrickými či optickými). Fyzická vrstva zároveň specifikuje i tvary konektorů a vlastnosti nejrůznějšího příslušenství k propojování (např. maximální délka kabelu). [2]

Fyzická vrstva specifikuje například:

- typ média (kroucená dvoulinka, optické vlákno atp.),
- tvar konektorů (RS485, RJ45, …),
- elektrické specifikace signálu a impedanci (+1 V, -1 V),
- přenosovou rychlost,
- IR (např. šířka pásma) a bezdrátovou komunikaci,
- Kódování,
- synchronizaci, zdroj hodin atp.

4.2.4 Linková vrstva

Zajišťuje výměnu dat mezi sousedními počítači a v rámci lokální sítě. Základní přenosovou jednotkou na linkové vrstvě je tzv. linkový rámec, který sestává ze záhlaví (header), přenášených dat (payload) a zápatí (trailer). V záhlaví rámce nalezneme podstatné řídicí informace včetně linkové adresy odesílatele a linkové adresy příjemce. Zápatí obsahuje především kontrolní součet (CRC) vytvořený z přenášených dat a sloužící ke kontrole, zda nedošlo k porušení dat, či jejich ztrátě. Samotnými daty přenášenými v rámci linkového rámce pak bývají IP datagramy, případně ARP pakety. Linková vrstva tedy přebírá data od vrstev vyšších, aby je opatřila fyzickou adresou (MAC) a následně v podobě linkového rámce předala fyzické vrstvě k odeslání. [2]

4.2.5 IP vrstva

Realizuje přenos dat mezi vzdálenými počítači (síť WAN, internet). Jednotku přenosu na IP vrstvě nazýváme IP datagram, který se pak dále „balí“, jak již bylo zmíněno v 4.2.2.2. IP datagram se skládá z pole IP záhlaví a pole Data. [3]

Z hlediska počtu směrovačů v síti můžeme říci, že počítače v síti spolu mohou komunikovat dvěma způsoby:

- Lokálně (v rámci sítě LAN), mezi zdrojovým a cílovým počítačem se nenachází žádný směrovač.
- V rámci sítě WAN, komunikace probíhá přes alespoň jeden směrovač.

Směrovač každý přijatý paket nejdříve vybalí z datového rámce na linkové vrstvě a následně ho před odesláním dál znovu zapouzdří do nového datového rámce s jiným linkovým protokolem. Pro komunikaci na IP vrstvě je toto však jedno. IP vrstva totiž vůbec nevidí zařízení pracující na linkové a fyzické vrstvě (opakovače, přepínače atp.). Síťovým rozhraním na IP vrstvě je síťová karta, případně jiný komunikační port. Toto síťové rozhraní má vlastní a v síti jedinečnou IP adresu. Každý IP datagram pak ve svém záhlaví nese IP adresy příjemce a odesílatele, což je kompletní informace pro směrování v rámci sítě. Síť tedy může

přenášet každý datagram samostatně, což může vést k tomu, že datagramy dorazí na místo určení v jiném pořadí, než odešly od odesílatele. [2]

4.2.6 TCP/UDP vrstva

Protože mezi dvěma počítači může komunikovat prostřednictvím sítě více aplikací najednou, je třeba roztřídit a rozlišit, která data, které konkrétní aplikaci patří. O toto se stará TCP/UDP vrstva. Ta přichází do adresace s tzv. porty. Příjemce tak není určen pouze unikátní IP adresou, ale i portem aplikace a zároveň použitým protokolem na této vrstvě. Ty jsou zde k dispozici dva:

- Protokol TCP, spojovaná služba, kdy příjemce potvrzuje přijetí dat, a v případě jejich ztráty nebo poškození žádá o opakování přenosu.
- Protokol UDP nevyžaduje potvrzení, prostě data odešle a už ho nezajímá, zdali byl doručen.

Podle použitého protokolu tak sítí kolují buď TCP segmenty nebo UDP datagramy. IP vrstva zároveň předpokládá, že veškerá komunikace na nižších vrstvách probíhá, a spojení mezi počítači je tedy zajištěno. Věnuje se pouze rozdělování dat na jednotlivých portech. [3], [4]

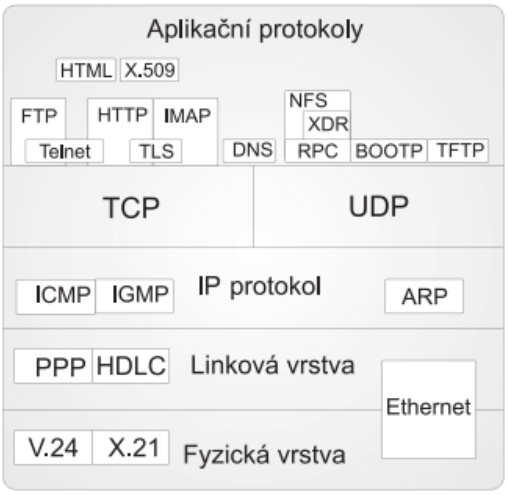
4.2.7 Aplikační vrstva

Stejně jako vrstva TCP/UDP a IP vrstva, tak i aplikační vrstva prostě spoléhá na správnou funkci nižších vrstev. Aplikační vrstva komunikuje pomocí datových toků, které vytváří vrstva nižší (TCP/IP). Protože datové toky fungují oboustranně, aplikační vrstva do nich buď vkládá data aplikací, nebo je z nich bere a distribuuje mezi aplikace. Řídí tedy komunikaci mezi aplikacemi, a to tak že mj.:

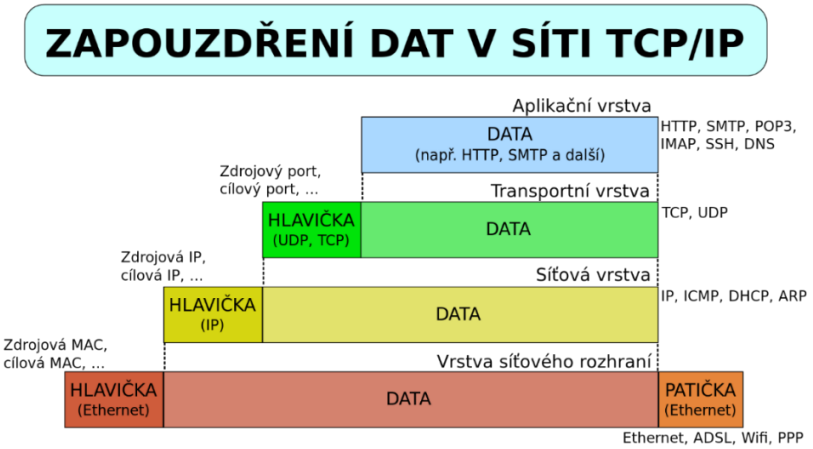
- Předepisuje dialog mezi aplikacemi.
- Předepisuje formát dat, které se předávají mezi aplikacemi.

- Zabezpečuje spojení proti případným útočníkům.

Na aplikační vrstvě se můžeme setkat s velkým množstvím protokolů. Ať už to jsou služební protokoly, sloužící k zajištění správné funkce internetu (např. směrovací tabulky, SNMP), nebo uživatelské protokoly, které jsou využívány přímo (SMTP, FTP, http atp.). Na obrázcích můžeme vidět výčet některých protokolů používaných na internetu (obr. 2) a schematické znázornění zapouzdření na jednotlivých vrstvách v síti TCP/IP (obr. 3). [3], [4]



Obr. 2 Některé protokoly na Internetu. [2]



Obr. 3 Zapouzdření dat v síti TCP/IP. [5]

4.2.8 IP adresa

Jak vyplívá ze struktury protokolu TCP/IP, IP adresa je tím identifikátorem, kterým se rozlišují počítače v síti. Pro správnou funkci sítě je nutné, aby každé zařízení připojené do sítě mělo unikátní IP adresu a nedocházelo tak k nejednoznačnosti při adresování.

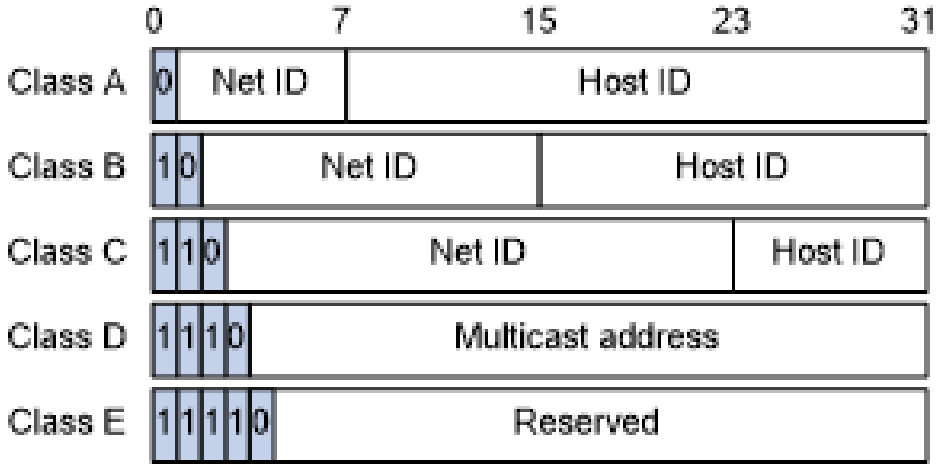
IPv4 protokol zavedl IP adresu jako 32bitové číslo zapsané dekadicky po jednotlivých oktetech (tedy osmicích bitů). Jako příklad může posloužit IP adresa serveru seznam.cz, která je: 77.75.79.53. Adresní prostor, tedy rozsah všech použitelných adres lze spočítat jednoduše jako 2^{32}, to jest 4 294 967 296 adres. Skutečná velikost adresního prostoru však bude mnohem menší, protože některé části nemohou být použity, ať už proto, že jsou vyhrazeny pro jiné potřeby protokolu, nebo proto, že z praktických důvodů jsou některé IP adresy shlukovány do větších celků a tyto jsou pak tzv. privátní a nedají se v internetu použít. Návrh také počítá s rozdělením adresy na část síťovou a část lokální (obr. 4). Prvních osm bitů tedy určuje síť a zbytek konkrétní zařízení uvnitř sítě. Sítí tak mohlo být celkem 256, ale v každé z nich se mohlo nacházet více než 16 milionů počítačů.

Obr. 4 Struktura IP adresy [2]

S tím, jak se zvyšoval počet lokálních sítí, tento návrh přestal být použitelný. Bylo tudíž přijato řešení v podobě rozdělení IP adres do tříd.

- Třída A, pro menší počet velkých sítí,
- Třída B, pro střední počet středně velkých sítí,
- Třída C, pro velký počet malých sítí,
- Třída D, pro skupinové vysílání (multicast),
- Třída E, jako rezerva.

Přidělovala se tedy vždy adresa z konkrétní třídy, takže vlastník adresy měl pro své využití celý adresní prostor dané podsítě. Třídní (classful) rozdělení se nachází na Obr.5.



Obr. 5 Třídní rozdělení IP adres [9]

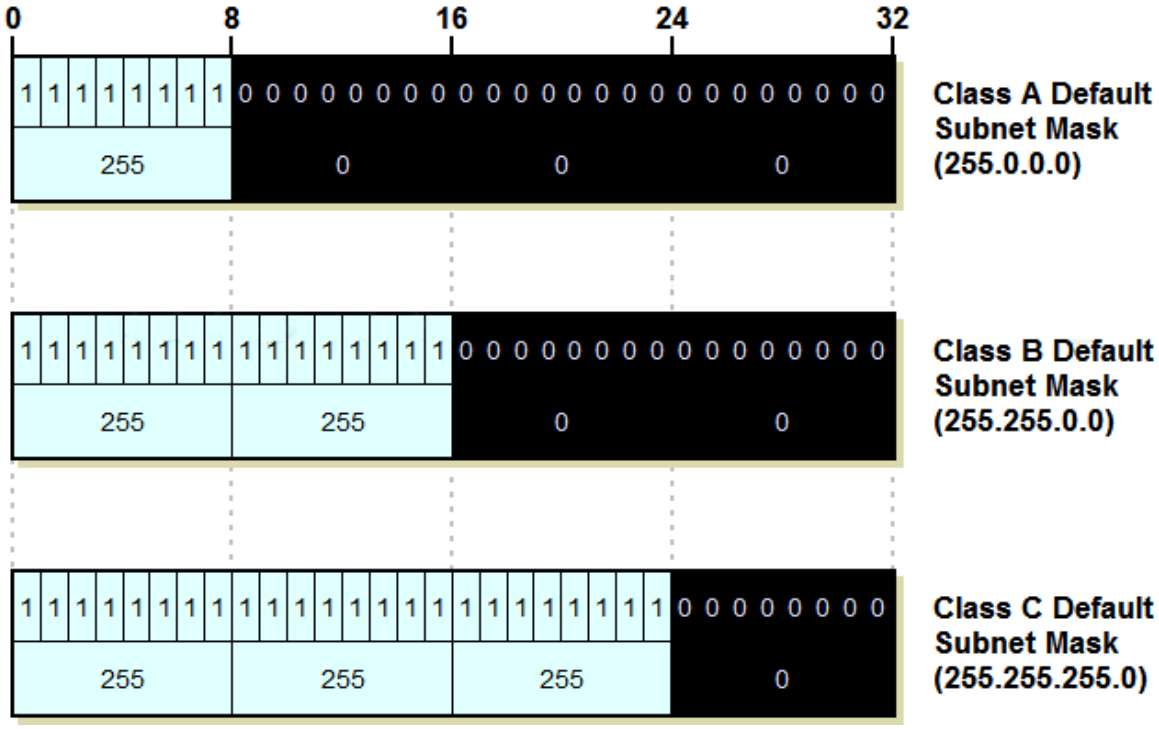
4.2.9 Nedostatek adres IPv4

Adresní prostor téměř 4 miliard adres se zdál v osmdesátých letech jako nevyčerpatelný. Nicméně, jak se začal zvyšovat počet zařízení připojených k internetu, začalo být stále jasnější, že opak je pravdou. Velkorysost a nedostatečný cit při přidělování IP adres způsobil značné plýtvání adresami. IP adresy třídy A, kterých bylo nejméně, se prakticky musely přestat přidělovat. Místo přidělení jedné adresy třídy B se přidělilo více adres třídy C atp. Tím se sice žadateli zmenšil adresní prostor v podsítích, ale aspoň se zpomalil úbytek IP adres pro přidělení. Zároveň se ale tvořily stále větší směrovací tabulky a hrozilo vyčerpání kapacity operační paměti směrovačů (což je věc, která by se stejně časem nevyhnutelně projevila s přidělením více a více adres). To vše by nicméně nezajistilo, aby adresy nedošly v budoucnu. Bylo tedy nutné najít jiný způsob. Řešení se našlo postupně několik. [8]

4.2.10 Subnetting a supernetting

Třídní rozdělení přestalo dostačovat a jeho nedostatkem bylo především to, že nebylo možné libovolně měnit polohu vymezující hranici mezi logickými částmi adresy. Tedy tou,

která rozděluje adresu sítě, a adresu počítače v ní. Ačkoli by stačil nějaký číselný údaj o poloze hranice, byla zavedena tzv. maska sítě. Maska sítě je 32bitový řetězec (stejně jako IP adresa), který obsahuje logickou 1 v bitech odpovídajících adrese sítě a logickou 0 v těch bitech, které odpovídají adrese zařízení v dané podsíti (Obr. 6). [8]



Obr. 6 Základní masky sítě jednotlivých tříd IP adres [10]

S použitím masky sítě se dá dosáhnout dvou efektů:

- spojení několika adres do jedné (spojované adresy musí být „sousední“ – tzv. supernetting,
- rozdělení jedné adresy na několik adres menších – subnetting.

Subnettingem lze tedy dosáhnout vytvoření několika podsítí posouváním „dělící čáry“ doprava. Všechny takto vytvořené podsítě ale musí mít právě jeden společný vstupní bod do zbytku internetu, protože zvenčí chybí informace o posunutí hranice a rozdělení sítě na podsítě. Tzn. rozdělení pomocí aplikace různých masek má platnost pouze lokální, nikoli globální. [8], [4]

Supernetting je přesným opakem. Pokud vlastník několika „sousedních“ adres (tzn. těch, které se shodují v určitém počtu vyšších bitů) z nějakého důvodu potřebuje vytvořit podsíť větší, než mu jednotlivé adresy dovolují, může je posunutím hranice směrem doleva spojit v jednu síť velkou. Stejně jako u subnettingu má informace o spojení platnost lokální.

4.2.11 CIDR (Classless Inter Domain Routing)

CIDR, nebo také beztřídní směrování, umožnilo jemnější dělení adres na podsítě. V třídním rozdělení byla maska sítě příslušná k jednotlivým třídám IP adres (třída A, B nebo C). Tedy maska je v třídním rozdělení dána třídou použité veřejné adresy. CIDR tuto příslušnost ruší a dovoluje dělení adresy po jednotlivých bitech místo po oktetech, jak tomu bylo v třídním rozdělení. CIDR zároveň zavádí zápis masky jako číslo, vyjadřující počet „jedničkových“ bitů, za lomítkem v zápisu IP adresy. Stejný způsob zápisu masky je používán i v novějším IPv6. Zároveň bylo nutné vyřešit to, že se stále zvětšující směrovací tabulky. Což bylo způsobené „bezhlavým“ přidělováním adres. CIDR zavedl jasně definovaná pravidla a hierarchii v přidělování adres. Adresy přidělují tzv. LIR (Local Internet Registry), tedy lokální registrátoři, kteří garantují dodržování stanovených pravidel. Agregují adresy a řeší velikosti přidělovaných prefixů. Díky prefixům se také zjednodušilo směrování mezi sítěmi. LIRům adresy ke správě dávají tzv. regionální registrátoři (Regional Internet Registry, RIR), kteří zároveň vytváří adresní politiku pro oblast ve své správě. Regionální registrátor pak dostává bloky adres od ICANN (Internet Corporation for Assigned Names and Numbers) prostřednictvím organizace IANA (Internet Assigned Numbers Authority). Dnes je tedy internet rozdělen mezi pět regionálních registrátorů, jimiž jsou: [2], [8]

- AfriNIC (Afrika)
- APNIC (Pacifická oblast – Austrálie a Asie)
- ARIN (Severní Amerika)
- LACNIC (Jižní Amerika)

- RIPE NCC (Evropa)

4.2.12 NAT (Network Address Translation)

Ačkoli byl CIDR opatřením úspěšným a výrazně zabránil v plýtvání a s ním souvisejících problémů, stále pouze oddaloval nevyhnutelné vyčerpání IP adres jako takových. V důsledku blížícího se vyčerpání adres se krom vývoje komunikačního protokolu nové generace (IPng) sáhlo k řešení v podobě překladu síťových adres (NAT). Z důvodu nedostatku IP adres tedy nemůže mít každý uživatel internetu svou unikátní veřejnou adresu. NAT toto řeší způsobem, kdy může vlastník veřejné adresy za tuto adresu „skrýt“ celou vnitřní síť a ta pak vůči okolí působí jako jedna stanice. Toto je možné bez ohledu na rozsah sítě. NAT pro úpravu provozu je implementován jako funkce v zařízení, přes které potom probíhá obousměrně komunikace mezi vnitřní sítí a okolím. Takovou bránou (Gateway) může být router, ale například i počítač. [9]

Zjednodušeně tak komunikace při použití NAT probíhá následovně:

- klientský počítač vyšle požadavek k bráně vnitřní sítě (routeru),
- router pakety přebere, změní jejich IP adresu (vnitřní sítě) na svou vnější IP adresu,
- router označí pakety a odešle je z náhodného TCP portu,
- router si zapíše do tabulky, který port pro odeslání paketů zvolil a který klient k němu patří,
- po přijetí odpovědi provede router akci opačnou a pakety vrátí klientskému počítači.

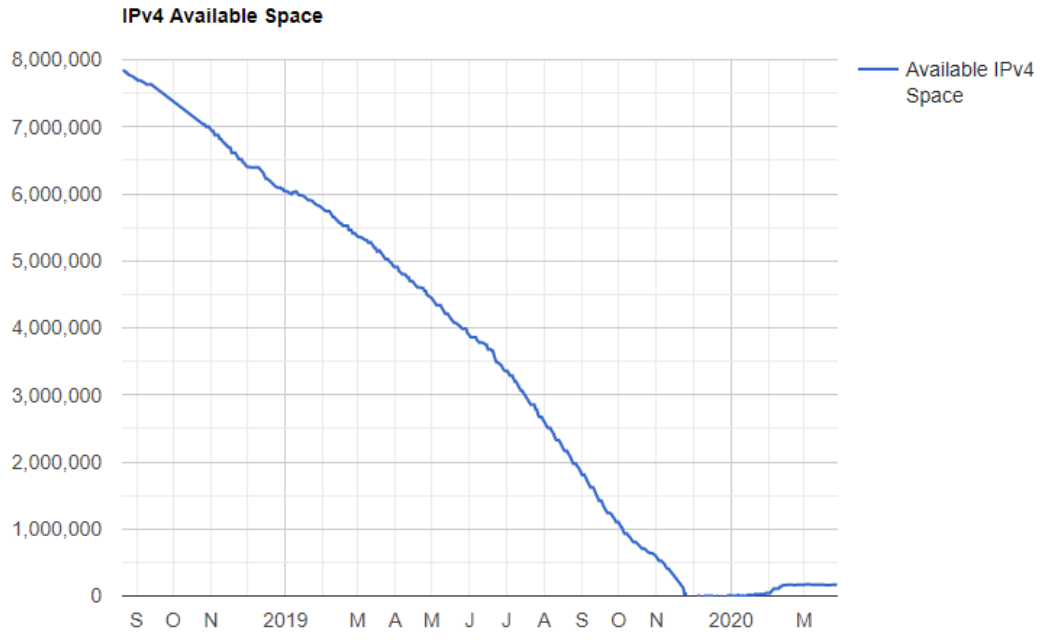
Klient tedy při komunikaci s použitím NAT, až na výjimky, proces nijak neovlivňuje a komunikace je pro něj naprosto transparentní. Druhá strana neví, že je klient „schován“ ve vnitřní síti a bez problému komunikuje s překladačem. NAT tedy nedovoluje se spojit přímo

s počítačem ve vnitřní síti. Bez dalších úprav tedy nejsme schopni provozovat ve vnitřní síti například vlastní server. Tato nevýhoda ovšem většině uživatelů vůbec nevadí, a naopak kvituje bezpečnostní stránku věci. Princip funkce NAT má tedy jakýsi pasivní vliv na bezpečnost sítě. Druhotným důsledkem pak je překrytí veškeré komunikace se světem. Případný útočník tak nemá ponětí o struktuře sítě, může odpovídat pouze na výzvy zevnitř a nemůže se přímo spojit s konkrétním počítačem. Spousta uživatelů, ale například i poskytovatelů připojení, a dokonce i výrobců hardwaru, tedy nabírá falešný pocit bezpečí v sítích používajících NAT a nemají potřebu používat firewall. Dokonce jejich funkce a názvy chybně zaměňují. Toto je z hlediska bezpečnosti velmi chybné. [9]

4.2.13 Vyčerpání adresního prostoru IPv4

Jak již bylo popsáno výše, NAT nedovoluje bez dalších výraznějších úprav sítě (port forwarding, SSH tunneling atp.) tedy provozovat přístupnou službu (např. server). K tomu je stále zapotřebí vlastnit veřejnou IP adresu. Zavedení NAT do struktury sítí tedy opět pouze zpomalilo problém s vyčerpáním adresního prostoru IPv4. Některé adresy se sice vrací zpět do oběhu (např. po ukončení smlouvy s poskytovatelem připojení), to ale velikost poptávky nemohlo pokrýt. Při sledování vývoje čerpání adres bylo datum vyčerpání vcelku přesně odhadnuto na rok 2011. Toto se i potvrdilo 3.2.2011, kdy IANA rozdala poslední své adresy regionálním registrátorům a tím se vyčerpala celosvětová zásoba IPv4 adres. Každý z regionálních registrátorů si pak stanovil hranici vyčerpání. Při dosažení této hranice pak RIR hlásí faktické vyčerpání zásob, ačkoli si fakticky nechává zlomek adres jako poslední nutnou rezervu. APNIC dosažení této hranice ohlásil již 19.4.2011. RIPE NCC pak 14.9.2012. LACNIC ohlásil vyčerpání 10.6.2014. APNIC si za hranici vyčerpání stanovil absolutní nulu, které dosáhl 24.9.2015. V současné době tedy z regionálních registrátorů (RIR) disponuje adresami pouze AfriNIC, u kterého se obecně odhaduje vyčerpání na rok 2020. Nedostatek adres v ostatních regionech ale spustil vlnu migrace hostingových poskytovatelů do afrického regionu z důvodu větší šance na přidělení většího prefixu adres, což čerpání zásoby AfriNIC bezesporu urychlí. V ostatních regionech, krom oné rezervy u RIR, jsou již IPv4 adresy pouze v rukou lokálních registrátorů, případně se žadatelé zapisují na čekací listinu a adresy se jim přidělují až po tom,

co se dostanou zpět do oběhu. Éra IPv4 je tedy podle všeho u konce. Vývoj počtu volných IPv4 adres od roku 2018 do dnes pro RIPE NCC je dobře patrný z Obr. 7. [23]



Obr. 7 vývoj počtu volných adres v RIPE NCC [28]

4.3 Adresace IPv6

V souvislosti s přechodem IPv4 na IPV6 asi nejednoho člověka napadlo, proč se jedna verze protokolu IP někam poděla. IPv5 je označení pro Internet Stream Protocol (ST). Šlo o experimentální protokol pro přenášení hlasu, videa a distribuovaných simulací. IPv5 byl definován už roku 1979 a zapsán jako RFC 1190 ve své verzi ST-II. Stejně jako IPv4 používal k přenosu pakety, a dokonce garantoval QoS (Quality of Service). K jeho použití mimo experimentální sítě a masovému nasazení však nikdy nedošlo. [7]

Zkraje devadesátých let 20. století bylo již zřejmé, že beztřídní směrování (CIDR) neodvrátí vyčerpání zásob adres IPv4 a protokol bude minimálně nutné upravit. V roce 1992 přichází komise IETF (Internet Engineering Task Force) s požadavkem na vytvoření IP protokolu nové generace (IPng). [6]

Pro návrh IPv6 byly zformovány následující požadavky:

- Dostatečné velký adresní prostor. Tak, aby se situace s nedostatkem adres již nikdy neopakovala
- Podpora služeb QoS (Quality of Service)
- Implementace bezpečnostních mechanismů přímo do IP
- Návrh odpovídající nové generaci vysokorychlostních sítí
- Podpora pro mobilní zařízení
- Automatická konfigurace
- Co nejhladší přechod z IPv4, ideálně možnost souběžného fungování obou

V roce 1995 byla tedy vydána sada RFC, která definuje základ nového internetového protokolu. Stěžejní je především RFC 1883: Internet protocol, version 6 (IPv6). Od této chvíle již nehovoříme o IPng, ale o IPv6. [13]

4.3.1 Adresa a adresní prostor IPv6

Jedním z hlavních požadavků na IPv6 byl velký adresní prostor. Tak, aby se situace s docházejícími adresami už nemusela v budoucnu řešit. Při návrhu byla zvolena varianta, kdy adresa IPv6 je 128bitový řetězec hexadecimálních číslic. Dosáhlo se tedy adresního prostoru o velikosti 2^{128} adres. Toto číslo je tak obrovské, že je pro člověka obtížně představitelné. Jen pro pořádek: je to 340 282 366 920 938 463 463 374 607 431 768 211 456 adres. O málo lepším příkladem bude představit si, že na každého člověka na planetě Zemi vychází několik triliónů adres. Nebo ještě jinak: kdyby byla každou jednu vteřinu přidělena jedna síť s prefixem /48, tedy 48 bitů, vystačil by nám adresní prostor IPv6 cca 35 000 let. Z tohoto můžeme odvodit, že adres IPv6 je tedy dostatek (což se mimochodem ve své době domnívali i autoři IPv4). [14]

128 bitů IPv6 adresy je rozděleno do osmi skupin po čtyřech číslicích šestnáctkové soustavy, vyjadřujících hodnoty šestnáct bitů dlouhých částí. Tyto skupiny se oddělují dvojtečkami. Například:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Očekává se, že uživatelé budou používat DNS (viz. kapitola 4.3.1.1) a vypisování jednotlivých adres nebude nutné. Při správě sítě nicméně bude nutno adresy ručně vypsat. Protože jsou v adrese poměrně často přítomny nuly, je možno její zápis zkracovat podle určitých pravidel. Je možno vynechat v každé čtveřici počáteční nuly, tedy místo „0000“ zapsat pouze „0“. Dále pokud se vyskytuje více nulových skupin za sebou, lze je nahradit konstrukcí „::“. Použitím obou pravidel se z výše uvedené adresy dostane její zkrácená verze:

2001:db8:85a3::8a2e:370:7334

Konstrukci „::“ lze v každé adrese použít pouze jednou, protože by nebylo jednoznačně jasné, jak vypadá nezkrácená varianta adresy. Toto a další pravidla pro tzv. kanonický zápis adresy bylo popsáno v dokumentu RFC 5952: A Recommendation for IPv6 Address Text Representation. Ten mimo jiné ukládá že:

- vynechání počátečních nul ve čtveřicích je povinné,
- písmena reprezentující číslice v šestnáctkové soustavě jsou vždy psána malými znaky,
- nahrazení více nulových skupin konstrukcí „::“ musí být použito pro nejdelší řetězec nulových čtveřic v adrese, pokud je víc řetězců stejné délky, musí být použito pro první z nich. [6]

4.3.2 DNS (Domain Name System)

Již u adresace IPv4 bylo pro použití mezi širokou veřejnost téměř nemožné chtít po lidech, aby vypisovali kompletní zápis IP adresy. Toto řeší systém DNS realizovaný DNS servery, který „překládá“ textový zápis doménové adresy, jež je pro člověka k použití a zapamatování mnohem příjemnější, na IP adresu ve standartním číselném zápisu, jak bylo popsáno v kapitole 4.3.2.

U IPv6 je představa vypisování adresy, i ve zkrácené podobě (za předpokladu, že konkrétní adresu je možné podle pravidel nějak zkrátit), pro běžné použití naprosto nereálná. S delšími adresami se hůř pracuje a jejich zapamatovatelnost je prakticky nereálná. Zde se opět nabízí řešení v podobě systému DNS, který ale bylo třeba upravit pro potřeby IPv6 (hovoříme o DNSv6), ale samozřejmě při zachování funkce pro komunikaci skrze IPv4. Do DNS bylo nutné přidat podporu pro adresy IPv6. Zároveň bylo zapotřebí vyřešit komunikaci při dotazování systému DNS při použití IPv6. Toto řeší vydané RFC 3596: DNS Extensions to Support IP Version 6. Přidání adres IPv6 do DNS samozřejmě zvyšuje, a do budoucna navyšovat bude, nároky na paměť DNS serverů - což ale dnes už není problém. [6], [15]

Původní návrh DNS a bohužel ani DNSv6 nepočítal se situací, kdy se za DNS server může vydávat útočník, případně může nějakým způsobem napadnout komunikaci mezi DNS serverem a uživatelským počítačem nebo mezi dvěma DNS servery. Toto pak vyústí v překlad doménové adresy na jinou IP adresu, než k doméně patří. Tato bezpečnostní hrozba vedla k vývoji DNSSEC (Domain Name System Security Extensions), které má těmto případům bránit. DNSSEC je rozšíření pro systém DNS zvyšující jeho bezpečnost. Má uživateli zaručit, že informace, kterou požaduje po systému DNS přišla od důvěryhodného zdroje a její integrita nebyla během přenosu nijak narušena. DNSSEC vyžívá asymetrické šifrování pomocí dvou klíčů (jeden k zašifrování a druhý k rozšifrování). Držitel domény tedy svým privátním klíčem podepíše údaje o své doméně, které do systému DNS vkládá. Pomocí veřejného klíče, který je uložen u nadřazené autority jeho domény, je pak možno pravost podpisu ověřit. I na úrovni TLD (Top-level doména, např. .cz) jsou data v DNS podepisována a klíč je předán opět vyšší autoritě. Ukládáním druhého klíče u nadřazené autority dochází k vytvoření hierarchické struktury, která zajišťuje důvěryhodnost. Pokud tedy není tato struktura nijak narušena, všechny klíče v ní souhlasí. Registrátor domény tedy musí chtít systém DNSSEC použít a nikdo

ho k tomu nenutí. A zde se dostavuje liknavost tohoto lidského faktoru, jak je vidět dále. Mezi průkopníky v používání DNSSEC patří mimo Brazílii, Bulharsko a Švédsko i Česká Republika. Tyto země začali používat jako první DNSSEC pro své TLD. V roce 2013 přijala dokonce vláda ČR usnesení podle něhož od 1.7.2015 musí všechny orgány veřejné správy používat DNSSEC pro všechny domény, které spravují. Tím se ČR stala nejspíše první zemí na světě, která zavedla povinné zabezpečení domén veřejné správy. Toto je až na pár málo výjimek (celnisprava.cz, některé domény MŠMT, MV atp.) dodnes pravda. [24], [25]

4.3.3 Objevování sousedů

Další, v čem se IPv6 od svého předchůdce diametrálně odlišuje je zjišťování linkové adresy partnera, se kterým chce komunikovat. Počítač tedy o partnerovi ví, zná jeho IP adresu, ví tedy, že spolu jsou v jedné lokální síti, ale ke komunikaci potřebuje znát adresu jeho linkového rozhraní. IPv4 k řešení této situace využívá samostatný protokol ARP (Address Resolution Protocol). Pomocí něho vyšle všem strojům v síti, tedy na všesměrovou adresu 255.255.255.255, dotaz ohledně vlastnictví dotazované IP adresy a vlastník odpoví a přikládá k odpovědi svou adresu linkového rozhraní (v případě ethernetu je to MAC adresa). Tazatel si údaj zapíše do tzv. ARP tabulky a má všechny potřebné údaje k odeslání datagramu. [6]

U IPv6 je mechanismus řešící tuto problematiku definován jako základní součást IP a jmenuje se objevování sousedů (Neighbor Discovery, ND). ND je daleko obecnější nástroj a má na starosti mnohem více věcí než jenom zjišťování linkové adresy komunikačního partnera. Nástroj objevování sousedů slouží k následujícím účelům: [6]

- Zjišťování linkových adres uzlů v lokální síti
- Zjišťování změn v linkových adresách, ověřování platnosti položek
- Přesměrování
- Hledání směrovačů
- Detekce duplicity v adresách

- Ověřování dosažitelnosti sousedů
- Zjišťování parametrů sítě pro automatickou konfiguraci

4.3.4 Automatická konfigurace

Významnou vlastností IPv6 v nakládání s adresami je automatická konfigurace. Ta funguje na principu minimální potřebné počáteční konfigurace a svojí funkcí připomíná technologii Plug and Play. Pokud tedy připojíme nějaké zařízení (např. počítač, mobilní telefon atp.) k síti, toto zařízení si samo na příslušných místech obstará všechny parametry, které jsou potřebné k fungování v dané síti a samo si parametry nastaví včetně vygenerování příslušné IPv6 adresy. IPv6 nabízí k použití dokonce dva typy automatické konfigurace: stavovou a bezstavovou. [6], [13]

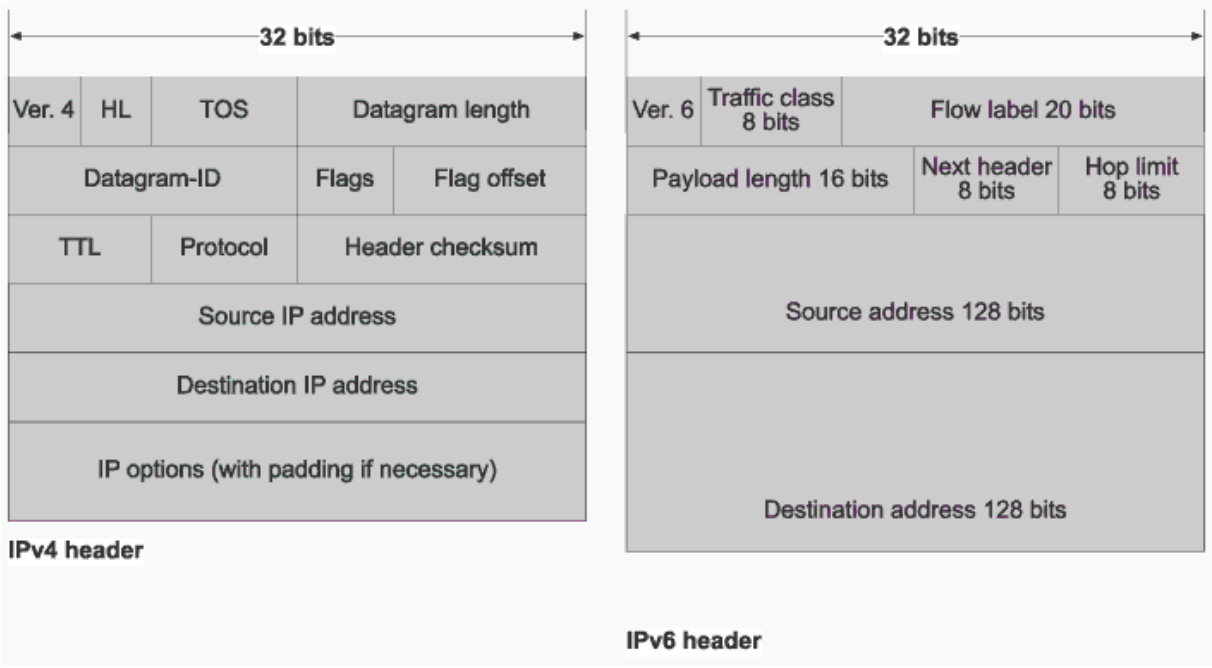
Stavová konfigurace, nazývaná rovněž DHCPv6 je jednoduše jenom evolucí stejného nástroje, tedy DHCP, známého z IPv4. Rozdíl je především v použití IPv6 adres oproti IPv4. Základem je služba spuštěná na síti (DHCPv6 server), která se stará o přidělování parametrů každému zařízení, které se chce stát součástí dané sítě. V praxi tedy nové zařízení vyšle dotaz do sítě ohledně konfiguračních parametrů pro danou síť, na nějž mu zasláním příslušných parametrů odpoví DHCP server. Ty obvykle zahrnují základní informace pro připojení do sítě: IP adresu, prefix sítě, adresy DNS a NTP serverů atp. [6]

Bezstavová konfigurace neboli SLAAC (Stateless Address Autoconfiguration) je v IPv6 prezentována jako součást nástroje objevování sousedů a představuje opravdu nový prvek na rozdíl od „vylepšeného“ DHCP. Bezstavová konfigurace pracuje s předpokladem, že v každé síti se nachází hlavní směrovač, který zná všechny parametry potřebné pro komunikaci s ostatními sítěmi. Tento hlavní směrovač pak pomocí nástroje ohlášení směrovače (router advertisement) v nahodilých intervalech tyto parametry vysílá do sítě. Nové zařízení tak má dvě možnosti. Buď dostatečně dlouho naslouchat, než hlavní směrovač vyšle potřebné údaje. Nebo pomocí nástroje výzva směrovači (router solicitation) toto ohlášení vynutit. Použitím bezstavovou konfigurace odpadá potřeba konfigurace a údržba DHCP serveru. Nevýhodou je

pak fakt, že je do sítě v intervalech vysílána informace, jaké DNS servery má klientské zařízení použít.

4.3.5 Datagram IPv6

Základním stavebním kamenem IPv6 protokolu je přepracovaný datagram. Ten vychází z datagramu známého z IPv4. Tzn. první část datagramu tvoří hlavičky, ty pak následuje část datagramu obsahující přenášená data. Již hlavičky však doznaly mnohých změn. Hlavička IPv4 datagramu měla proměnlivou délku a obsahovala kontrolní součet hlavičky (header checksum). Takže při každé změně provedené v hlavičce, například pouhým průchodem přes směrovač v síti, bylo nutné souběžně s přepsáním hlavičky vytvořit nový kontrolní součet, což by obohacené o adresní prostor IPv6 představovalo nežádoucí zátěž pro prvky v síti. Kontrolní součet byl tedy odstraněn a hlavička přepracována tak, aby nebyl nutný. Počet prvků v hlavičce se pak redukoval pouze na ty nejnutnější, čímž došlo k maximálnímu zjednodušení struktury a vznikla tzv. základní hlavička. Všechny ostatní informace byly vymístěny do hlaviček dalších (tzv. rozšiřujících). Ty jsou uvozeny částí (next header) datagramu, která poskytuje informaci o tom, který typ rozšiřující hlavičky má následovat. Tímto skládáním za sebe se dá použít libovolný počet rozšiřujících hlaviček. Při porovnání hlaviček datagramů (Obr.8) IPv4 a IPv6 zjistíme, že hlavička datagramu IPv6 má velikost pouze dvojnásobnou, tedy 40 bajtů (a to 32 z oněch 40 tvoří adresy odesílatele a příjemce). [6]



Obr. 8 Porovnání hlaviček datagramů IPv4 a IPv6 [21]

Další změna v návrhu datagramu se týká části, která obsahuje přenášená data. Technologií, které využívá IPv6 k přepravě datagramů, je spousta a každá z nich má jinou maximální velikost paketů, kterou dokáže přenést (MTU, Maximum Transmission Unit). IPv4 toto řešil tzv. fragmentací. Když datagram IPv4 při průchodu sítí narazil na linku, na jejíž MTU byl příliš velký, mohl jej směrovač před linkou s nižším MTU fragmentovat. V praxi to znamená rozdělit ho na několik menších částí a přidat o tom záznam do hlavičky. Příjemce pak z údajů v hlavičkách datagramů vytvořil datagram původní. V případě IPv6 fragmentaci již nemůže provést libovolný směrovač po cestě, ale může fragmentovat pouze odesílatel. Pro záznam o fragmentaci se pak použije nová rozšiřující hlavička. V případě, že datagram narazí na linku s nižším MTU, směrovač ho prostě zahodí a odesílateli odešle zprávu s důvodem zahození (vč. velikosti MTU). Odesílatel tak může datagram, pokud je to nutné, fragmentovat. Fragmentování datagramů nicméně znamená zvýšení jejich počtu a tím pádem větší zátěž na směrovače. Pokud pošleme například datagram o velikosti 1600 a narazí na rozhraní s MTU 1500, router z každého datagramu udělá dva, což v praxi znamená zdvojnásobení počtu všech datagramů pro dané vysílání. Je tedy nutné najít ideální kompromis mezi velikostí datagramů a jejich množstvím. Ideálně co nejmenší počet datagramů co největších, ale zároveň dost malých, aby nenarazily na menší MTU. IPv6 se snaží proto fragmentaci datagramů, pokud možno zabránit. Využívá k tomu algoritmu objevování MTU cesty a vychází z předpokladu, že

se směrování v síti v praxi příliš často nemění a datagramy odeslané v relativně krátké době za sebou budou putovat stejnou cestou sítí. Zjistí tak MTU na rozhraní, ze kterého vysílá, a pošle zkušební datagram o maximální možné velikosti tohoto rozhraní. Vychází z logiky, že větší datagramy, než je velikost prvního MTU, stejně vyslat nejdou. Pokud datagram dojde, je vše v pořádku a lze odvysílat celou skupinu datagramů. Pokud datagram na cestě narazí na menší MTU, je zahozen a IPv6 přizpůsobí velikost testovacího datagramu tomuto MTU. Celý proces se opakuje tak dlouho, dokud se systémem pokus-omyl nenalezne správná maximální velikost datagramu pro průchod sítí. [6]

4.3.6 QoS (Quality of Service)

Dojde-li z nějakého důvodu (velký objem dat, ale také např. malá přenosová kapacity linky) k zaplnění přenosové kapacity linky, snaží se aktivní síťové prvky vyřešit toto krátkodobé zahlcení linky uložením dat do vlastní vyrovnávací paměti (bufferu). Ve vyrovnávací paměti pak datagramy čekají ve frontě a do cíle dorážejí se zpožděním (latence). Síťové služby pracující s daty v reálném čase (VoIP, stream atp.), fungují s vyšší latencí velmi špatně. Dochází k výpadkům, zpožděním a celkově trpí kvalita těchto služeb. IPv4 k tomu využívá především dvě metody, policing (rate limiting) a shaping. Obě metody dělají totožné věci, ale každá svým vlastním způsobem. Policing omezuje provoz tak, že pakety, které by jinak překročili pásmo prostě zahodí, případně přeznačkuje. Výhodou je, že takto se dá omezovat pásmo přímo na vstupu/výstupu příslušného interface. Shaping oproti tomu příslušné pakety primárně nezahazuje, ale zařadí je do fronty a jejich odeslání rozloží do delšího časového úseku. Při tom vychází z předpokladu, že datový tok je nárazový. Nespornou výhodou je zamezení ztráty paketů. [2], [29]

Zatímco IPv4 tedy funguje spíše na modelu best-effort, v návrhu IPv6 se počítalo se zaručením určité kvality služby. V podstatě jde o mechanismus, jak některé pakety doručovat rychleji než jiné. Ke každému IPv6 datagramu je tedy možné přiřadit jeho prioritu a určit druh dat. O to se starají v síti směrovače, které pak řídí provoz paketů tak, aby pakety s vyšší prioritou byly odeslány před pakety s prioritou nižší. Mimo to má IPv6 ještě možnost efektivního směrování uvnitř podsítě jasně definovanou cestou. V lokální síti nicméně potřeba

QoS odpadá, protože kapacita přenosu v lokální síti bývá zpravidla vyšší než skutečný síťový provoz. QoS se tedy uplatní především za hranicí lokální sítě.

4.3.7 Podpora mobilních zařízení

Současnost v technologiích je více než čímkoli jiným nejvýraznější nastupujícím Internetem věcí (Internet of Things, IoT). Nejběžnějším příkladem je samozřejmě mobilní telefon (podle Googlu se 75 % lidí mladších 25 let připojuje na Internet z mobilu stejně nebo více často, jak z počítače). Tato zařízení charakterizuje ona mobilita, která znamená pohyblivost z hlediska geografického, ale s ním souvisí i pohyb z hlediska toho ve které síti se zařízení momentálně nachází. Zařízení tedy tím, jak putuje mezi sítěmi, mění svou IP adresu. To nepředstavuje problém, pokud spojení navazuje zařízení. Pak prostě jenom použije svou momentální IP adresu a spojení proběhne bez problémů. Pokud se ovšem chce někdo spojit s cestujícím zařízením, nastává problém, protože k tomu potřebuje znát jeho momentální adresu. IPv4 se toto zařízení pokouší vždy najít, což je pomalé a z hlediska QoS naprosto nepoužitelné. IPv6 toto řeší pomocí tzv. domácího agenta. Každé zařízení má nějakou domovskou síť a v té má svojí IP adresu, ta je zanesena do systému DNS a jí také použije kdokoli se bude s tímto zařízením chtít spojit. V nepřítomnosti zařízení v domovské síti jej zastupuje domácí agent, tuto roli hraje jeden ze směrovačů. IPv6 zahrnuje i způsob jeho automatické konfigurace. Role domácího agenta spočívá především v tom mít přehled o aktuální IP adrese cestujícího zařízení (to samo na novou adresu při její změně agenta upozorní) a zprostředkování požadavků na spojení na tuto adresu. Komunikace přes domácího agenta pak zjednodušeně probíhá takto: [26]

- Externí počítač vyšle paket s žádostí o spojení na domovskou adresu mobilního zařízení
- Domácí agent zprávu přijme a tunelem ji zašle mobilnímu zařízení na jeho momentální IP adresu
- Mobilní zařízení odpoví a zároveň započne proces optimalizace cesty, jehož účelem je informovat žadatele o svojí aktuální adrese.

- Když se žadatel dozví aktuální IP adresu, komunikace již probíhá přímo mezi ním a sdělenou IP adresou

5 Problematika přechodu

Teď již je jasné, v čem a jak moc se IPv6 od IPv4 odlišuje. IPv6 tedy řeší nedostatky v návrhu IPv4. Má prakticky neomezený adresní prostor, lépe nakládá s datagramy, má integrované bezpečnostní mechanismy, nabízí větší pořádek při hierarchickém uspořádání adres atp. Ale zároveň kvůli všem těmto vylepšením a změnám není s IPv4 zpětně kompatibilní. Logicky tedy existovaly dvě možnosti. Všichni přejdou okamžitě na IPv6, nebo je třeba vyřešit, jak zabezpečit souběžný chod obou a vzájemnou spolupráci s výhledem na postupné a přirozené nahrazení jednoho druhým. První možnost byla samozřejmě nereálná z mnoha důvodů. Spousta zařízení nebyla připravená na IPv6, bylo by potřeba napsat a nainstalovat nové firmwary, spousta směrovačů neměla operační paměť dost velkou, aby změnu na IPv6 zvládla. Síťové karty nebyly na implementaci stavěny. Pro starší verze operačních systémů by se musely psát záplaty (pokud by systém vůbec změnu zvládl bez zásahu do jádra). Při nemožnosti některých části internetu přejít by se fakticky vytvořily v síti díry. Problematika přechodu měla a stále má dvě roviny:

- technickou rovinu – Jak tedy zařídit souběžné fungování IPv4 a IPv6 a připravit všechna zařízení v síti na implementaci IPv6 a postupný přechod,

- morální rovinu – Jak přesvědčit uživatele a správce sítí, aby implementovali IPv6 i když to bude všechny něco stát.

S tím, jak šel vývoj technologií dopředu problematika přechodu se po této stránce vyřešila prakticky sama. Protokol IPv6 byl dostatečně dobře znám a technologické firmy měly dostatek času na jeho implementaci do svých produktů. Již pár let není k dostání síťový prvek, který by IPv6 nepodporoval.

Druhou stranou mince je pak podpora operačních systémů. Někteří výrobci operačních systémů poměrně dlouho otáleli s podporou IPv6 a čekali, zdali z něj nebude jenom další slepá ulička (jako např. model ISO/OSI), nicméně postupem času téměř všichni (LG WebOS nemá

podporu IPv6) nabízí nativní podporu IPv6 ve svém operačním systému. Zde jsou uvedeny ty nejrozšířenější: [22]

- Microsoft Windows – již verze XP s možností instalace protokolu IPv6, od verze Vista již nativně.
- MacOS – od verze 10.7 (Lion) podporuje IPv6, ale až do verze 10.10 vždy priorizuje IPv4 při dostupnosti obou. Od verze 10.11 již používá primárně IPv6, pokud je dostupné.
- Android – Od verze 5.0 (Lollipop) nativní podpora. Dosud bohužel nepodporuje DHCPv6.
- iOS – Od verze 4.1 podpora IPv6 vč. DHCPv6.

5.1 Přechodové mechanismy

Protože uživatel, který by přešel na IPv6, by se prostřednictvím IPv6 dostal v síti pouze tak daleko, dokud by v síti byla podpora IPv6, a zároveň uživatel, který nepřešel, by se prostřednictvím IPv4 nemohl spojit s částmi sítě, které by už měly přechod na IPv6 za sebou, bylo třeba zajistit, aby se toto nestalo. Přechodové mechanismy jsou odpovědí na otázku, jak zaručit vzájemné fungování IPv4 a IPv6.

5.1.1 Dvojí zásobník (Dual stack)

Dvojí zásobník je asi nejčastěji používanou variantou. Zařízení pracující v režimu dvojího zásobníku musí podporovat oba protokoly (IPv4 i IPv6) a na svém rozhraní získat dvě IP adresy, od každé jednu. K získání IPv4 adresy se používá většinou ruční konfigurace nebo DHCP, u IPv6 adresy je to pak krom ruční konfigurace a DHCPv6 ještě bezstavová automatická konfigurace. Lokální DNS server zároveň musí mít znalost obou verzí. Zařízení podporující jak IPv4, tak IPv6 jsou pak označována jako IPv4/IPv6 uzly.

5.1.2 Tunelování (Tunneling)

Tunelování je metoda, která umožňuje přenést data mezi zařízeními komunikujícími stejným protokolem skrze síť, která tento protokol nepodporuje. Nejčastější variantou je přenos IPv6 paketů za pomoci IPv4 sítě. Datagram IPv6 se pak prakticky zabalí do datagramu IPv4, který už může být přes síť přenesen. Existují dva typy tunelů: explicitně konfigurované a automaticky vytvářené. Konfigurovaný tunel se vytvoří mezi zařízeními s podporou tzv. tunelového serveru (nabízí vytvoření tunelu všem zájemcům o IPv6). Mezi servery nabízející tunelování patří například: Tunnel broker, TSP, Hurricane Electric, SixXS. Automatické tunely se tvoří pomocí tunelovacího mechanismu bez zásahu nějaké osoby. Každý tunelovací mechanismus se trochu jinak stará o použití jedné veřejné IP adresy k vytvoření tunelu až do cílové sítě. Tunelovací mechanismy jsou např.: 6to4, 6over4, 6rd, ISATAP, Teredo

5.1.3 Translátory

Tunelování i dvojí zásobník řeší případ komunikace dvou zařízení se stejnou verzí protokolu. Je však možné, že se zařízení komunikující skrze IPv6 bude chtít spojit se zařízením komunikujícím pouze skrze IPv4. Tato situace může nastat například mezi mobilními sítěmi třetí a čtvrté generace. Právě v těchto případech se používají translátory neboli překladače. Translátor umožňuje převod datagramů IPv6 na datagramy IPv4 a obráceně a tím přímou komunikaci.

5.2 Motivace k přechodu

Při připravenosti síťových prvků, softwaru a služeb na IPv6 by se zdálo, že pokročení v přechodu z IPv4 na IPv6 tedy nic nebrání. Opak je však pravdou. Běžní uživatelé Internetu nemají potřebu požadovat IPv6. Nemají důvod požadovat veřejnou IP adresu a za NATem je jim dobře. Zároveň netuší nic o QoS, šířce pásma, bezpečnostních mechanismech atp. Ze zkušeností z mého okolí vím, že nejdůležitější pro běžného uživatele je spojit se s cílovým serverem (obvykle facebook.com) a už neřeší, jak se spojení realizuje. Případné snížení kvality

služeb způsobené zahlcením linky uživatel prostě přetrpí, popřípadě se přihlásí do jiné sítě. Ale po běžném uživateli nikdo nechce, aby aktivně implementoval IPv6. To je záležitost vlastníků a správců sítí, a především poskytovatelů připojení. Ti by se měli starat o hladký přechod. Bohužel v infrastruktuře sítí se na některých místech nacházejí aktivní prvky, které by si s provozem skrz IPv6 buď částečně, nebo vůbec neporadili. Zároveň se jedná o nemalé množství hodin práce při nastavování síťových prvků a konfigurace firewallů a serverů všeho druhu. A tady vzniká zásadní problém. Uživatelé aktivně nepožadují IPv6, což nenutí providery implementovat a poskytovat IPv6. A zároveň: proč by měl provider nabízet IPv6, když po něm není poptávka?

Obvyklým řešení takových zacyklených problémů bývá situace, kdy se problému chopí politická autorita a vydá ohledně problematiky nějaké nařízení. A to se stalo také v případě přechodu na IPv6. Různé úrovně politických garnitur, které si byly vědomy závažnosti problému, zaujaly různé postoje a vypracovaly plány, které měly zajistit hladký a brzký přechod. Zde je uvedeno pár příkladů plánů zavedení IPv6:

- USA: Transition Planning for Internet Protocol Version 6 (IPv6), to set the US Federal Agencies a hard deadline for compliance to IPv6 on their core IP networks
- Austrálie: Preparation Jan 2008 – Dec 2009, Transition Jan 2010 – Dec 2012, Implementation Jan 2013 – Dec 2015
- Čína: China Next Generation Internet (CNGI) sets out a 5 year plan (2006–2010) for the early adoption of IPv6 [27]

Pro nás je zajímavé především počínání Evropské unie. V červnu 2008 byl přijat Evropskou komisí akční plán pro nasazení IPv6. Ten požadoval, aby do konce roku 2010 bylo uživatelů s přístupem k IPv6 minimálně 25 %. Akce k dosažení tohoto cíle byly rozděleny do čtyřech oblastí:

1. Stimulace obsahu a služeb – dostupnost veřejných služeb skrze IPv6, vyzvání komerčních subjektů k jeho podpoře, použití IPv6 v projektech 7. rámcového programu pro vědu a výzkum EU.

2. Vytvoření poptávky ve veřejných dodávkách – požadována podpora IPv6 všech členských států v dalším inovačním cyklu síťových zařízení.

3. Včasná připravenost – Cílené kampaně zaměřené na informovanost. Konkrétní podpůrné akce. Zařazení IPv6 do výuky na školách.

4. Řešení bezpečnosti a soukromí – soubor doporučených postupů a monitoring dopadů IPv6 na soukromí uživatelů.

Toto počínání EU bohužel nezajistilo zmíněných 25 % uživatelů s IPv6 konektivitou do roku 2010. Reálně mělo IPv6 konektivitu v polovině roku 2011 něco málo přes 6 % uživatelů z EU. [27]

V návaznosti na počínání EU přijala 8.6.2009 vláda ČR usnesení č. 727. V něm ukládá zajistit kompatibilitu síťových prvků státní správy s IPv6 a zajištění přístupu ke stránkám eGovermentu skrze IPv6. Zároveň doporučuje tento postup všem složkám místní samosprávy. To vše do 31.12.2010. Dodržování nařízení vlády č. 727 bylo revidováno počátkem roku 2012 a bylo zjištěno, že tuto povinnost nesplnilo více než polovina ministerstev a 50 % ústředních orgánů státní správy. V době dokončování této práce (březen 2019) nemá stále webové stránky dostupné přes IPv6 5 ze 14 ministerstev ČR. [20]

Obr. 9 Dostupnost webu MKČR přes IPv6 [30]

6 Současný stav

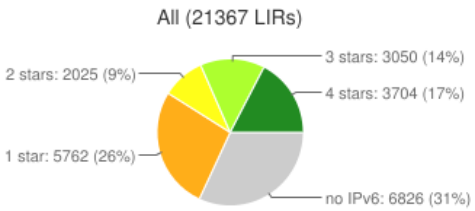
IPv6 je v současné době tedy jediným nástupcem IPv4. IEFT (Internet Engineering Task Force) ani nikdo jiný v oboru nepracuje na žádné jiné alternativě a největším konkurentem IPv6 je jeho předchozí verze, tedy IPv4. Budoucnost ve formě IPv6 je poměrně jasná. IPv4 adresy došly. Technologické problémy byly prakticky vyřešeny. Téměř každý má doma nebo v ruce zařízení „IPv6 ready“, a přechod tak závisí výhradně na vlastnících a provozovatelích sítí a serverů. V následujícím textu je popsán současný stav. [6]

V dnešní době jsou servery rozprostřené prakticky po celém povrchu Země. Nadnárodní korporace mívají lokální varianty serverů ať už pro jednotlivé regiony, nebo přímo pro jednotlivé státy. Firma z ČR si může pronajmout webhosting na druhé straně planety. Dokonce se mluvilo o zavěšení serverů Thepiratebay.org na balóny umístěné na nízké oběžné dráze Země, aby unikly spravedlnosti. Zkrátka moderní člověk konzumující obsah na internetu dnes každý den navštěvuje elektronicky spoustu míst po celé Zemi a ani si toho vlastně nevšímá. Jako příklad stačí prosté dotazování na konkrétní IP adresu DNS serveru. Z těchto důvodů by se mohlo zdát srovnávání implementace a připravenosti na IPv6 podle jednotlivých zemí světa zavádějící. To by však byl omyl. Tyto údaje nám souhrnně nastíní, jak je to vlastně u každého státu s přístupem k IPv6. Kdyby byla po IPv6 poptávka, vznikla by jistě i nabídka. Například při touze obyvatel po veřejných IP adresách. Kdyby se třeba vláda některého státu uvolila přechod na IPv6 nějakým způsobem podpořit, těžko si představit, že by dané podpory žádný z provozovatelů sítí nevyužil a svou síť neinovoval, případně nepostavil novou. Technologie jsou přeci běžně dostupné a infrastruktura již existuje (pomineme-li problematiku v zemích třetího světa a rozvojových státech).

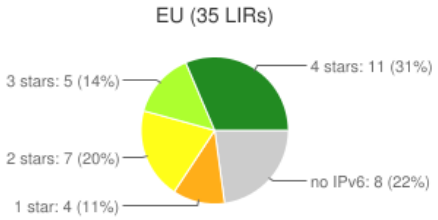
Zdrojů dat by se našlo nespočet a při porovnání výsledků se budou lišit. Je to dáno tím, že každý subjekt, který statistiku tvoří, používá jiné způsoby měření a skládání dat a jiná kritéria hodnocení. Pravda tedy bude „někde mezi“. Jednotlivé zdroje nicméně uvádějí čísla hodně podobná.

RIPE NCC ve své statistice IPv6 RIPEness například používá systém hodnocení spočívající v přidělování hvězdiček. Každému lokálnímu registrátorovi (LIR) přidělí 1-4 hvězdy (od roku 2013 se majitelé 4 hvězd kvalifikují jako uchazeči o hvězdu pátou) podle jeho připravenosti. 1.

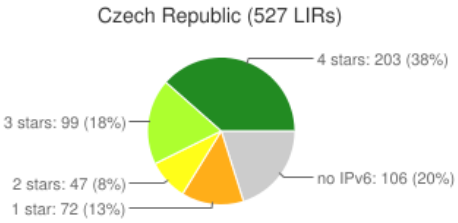
hvězda za přidělený adresní prostor IPv6, 2. hvězda za route6 objekt (záznam ve směrovacím registru IPv6) atp. Registrátory pak vyjádří procentuálně podle počtu hvězd. Ze souhrnné statistiky (Obr. 10) vidíme především zajímavý údaj v části koláče „no IPv6“, a to 31 %. Téměř třetina všech lokálních registrátorů tedy nemá z různých důvodů možnost přidělovat IPv6 adresy a jejich klienti jsou tak v síti svého LIR bez IPV6. Koláčový graf stavu Evropské unie (Obr. 11) je lehce zavádějící, protože jenom 35 LIR je zapsáno jako registrátoři pro EU. Pro informaci je přiložen stav podle RIPEness v ČR (Obr. 12) a na Slovensku (Obr. 13). [16]



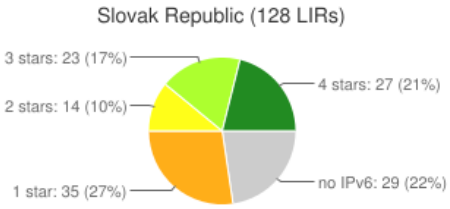
Obr. 10 RIPEness hodnocení všech LIR [16]



Obr. 11 RIPEness hodnocení LIR v EU [16]



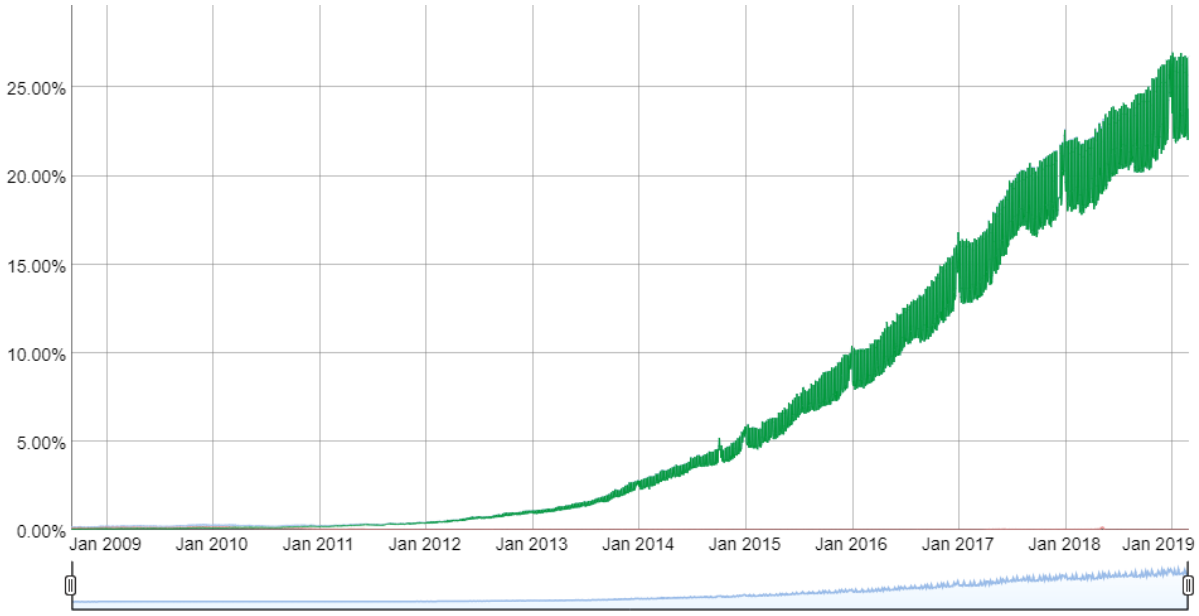
Obr. 12 RIPEness hodnocení LIR v ČR [16]



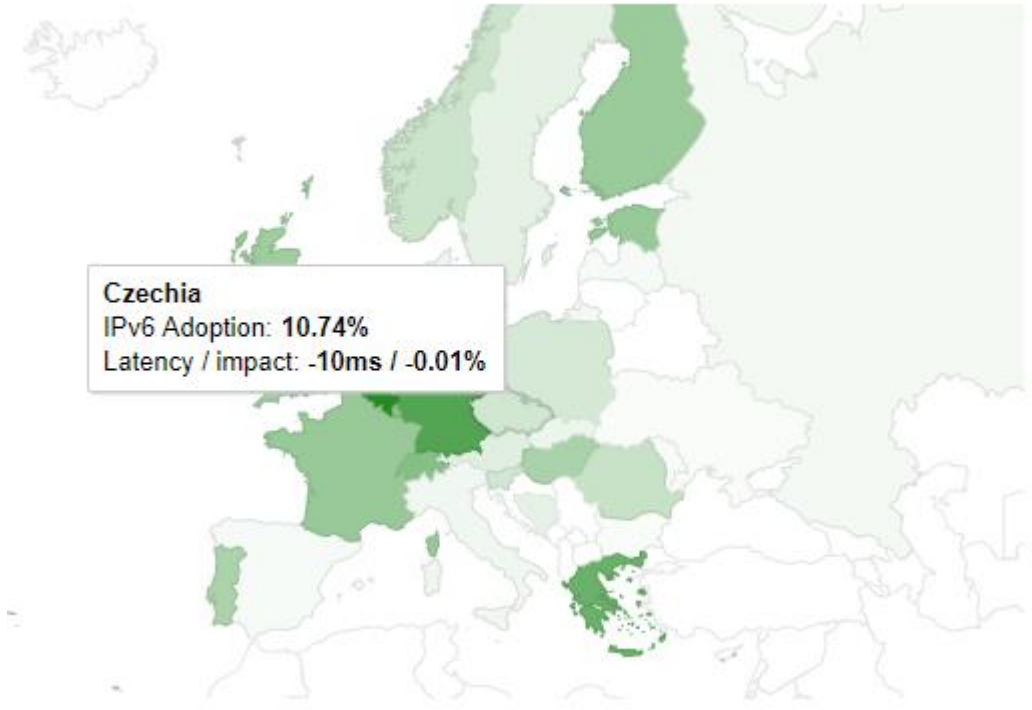
Obr. 13 RIPEness hodnocení Slovenských LIR [16]

Google a Cloudflare pak zjišťuje funkčnost IPv6 konektivity uživatelů, kteří přistupují k jejich službám. Google tak zjistil, že více než 10 % jeho uživatelů mělo funkční IPv6 konektivitu již 1.1.2016. Od té doby měl vývoj stoupající tendenci a dnes (březen 2019) je to již více než 25 % uživatelů (Obr. 14). Nejvíce procent uživatelů Googlu skrze IPv6 najdeme v Belgii (53 %), Německu (41,3 %) a Řecku (35,4 %). Zajímavé jsou údaje pro Uruguay (34,9 %) Vietnam (31,9 %) a Indii (33,5 %, ale většina IPv6 komunikace vzniká přes operátora Reliance Jio, který síť buduje od počátku jako IPv6). Naopak procento uživatelů s IPv6 konektivitou z Afriky se blíží nule. Česká republika je v pomyslném průměru 10,7 % (Obr. 15). [17], [18]

Téměř totožná čísla jako Google pak uvádí APNIC. [19]



Obr. 14 Vývoj IPv6 konektivity uživatelů služeb Google [18]



Obr. 15 Procento uživatelů Google s IPv6 konektivitou z ČR [18]

7 Modelové situace

7.1 Menší firma

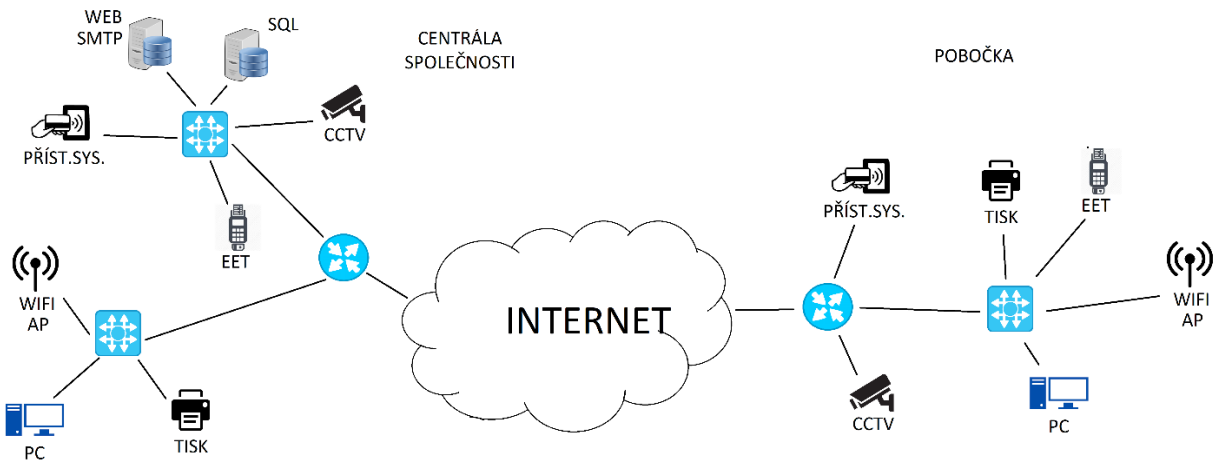
Jako jeden z příkladů je předkládáno prostředí menší firmy (Obr. 16). Příklad firmy poslouží jako dobrá demonstrace finančně náročnější varianty přechodu, zahrnující nutnou výměnu síťových prvků.

Firma má své sídlo, které slouží zároveň jako centrála firmy, a jednu pobočku, která je od centrály geograficky vzdálená. Centrála firmy a pobočka mají z důvodu výrazně jiného umístění každá jiného poskytovatele připojení k internetu. Přechod na IPv6 není pro firmu nutností, protože momentálně pro většinu jejích potřeb funguje dostatečně dobře překlad adres (NAT). Nicméně s vývojem technologií v současném světě, nástupem IoT (Internet of Things) a postupem digitalizace firemních řešení si začíná uvědomovat postupnou nutnost posunu k IPv6. Navíc pohodlnost vzdáleného přístupu (kamerový systém, přístupový systém atd.) usnadní adresní prostor IPv6. Zároveň nechce být ničím překvapena ve vývoji věcí a nechce riskovat případnou nevýhodu v konkurenčním prostředí. V našem příkladu centrála – pobočka se jedná o dvě oddělené lokální sítě, které ale mezi sebou musí komunikovat prostřednictvím internetu. Použití přechodového mechanismu typu dvojitý zásobník (dual stack) je tedy více než nasnadě.

Firma v rámci běžné činnosti hodlá provozovat následující:

- firma má vlastní WEB, SMTP a SQL server umístěný na centrále,
- mezi centrálou a pobočkou běží jeden sdílený přístupový a docházkový systém,
- firma na obou místech provozuje kamerový systém,
- zaměstnanci k práci používají stolní počítače (MS Windows),
- zaměstnanci a návštěvy se dále k bezdrátové síti připojují z přenosných počítačů (MS Windows, MacOS) a mobilních telefonů (Android, iOS),
- v rámci firmy běží na serveru vnitropodnikový systém,

- centrála i pobočka provozují platební terminál a registrační pokladnu,
- centrála i pobočka provozuje síťové tiskárny.



Obr. 16 Síťové prostředí menší firmy [vlastní]

7.1.1 Náklady

Největším finančním nákladem přechodu firmy na IPv6 bude nákup nových síťových prvků z důvodu nekompatibility prvků současných s IPv6. Nové prvky ve struktuře sítě nahradí prvky staré (2x směrovač a 3x switch). Doporučuje se nákup těchto prvků:

- 2x router TP-LINK TL-ER6120
- 3x switch TP-LINK JetStream T1700G-28TQ

Klientské počítače a jiná síťová zařízení buď IPv6 podporují, nebo budou modernizovány jindy. Z důvodu použití stávajících síťových rozvodů zůstane topologie sítí stejná. Jediným dalším nákladem na přechod tak bude finanční odměna technikovi, který provede nutná nastavení na centrále i pobočce. Nutné bude nastavit především:

- konfigurace webového serveru, serveru pošty a databázového serveru,
- nastavení výchozích bran (pro klientské uzly se použije dynamická konfigurace)
- konfigurace DNS v rámci IPv6,
- konfigurace bezdrátových přístupových bodů.

Zařízení běžící na síti (servery, NVR atp.) dostanou přidělenu adresu veřejnou. Běžná klientská zařízení pak dostanou dynamicky přidělenou adresu z rozsahu fc00::/7. Předpokladem je pak zpřístupnění nativní konektivity IPv6 od místních poskytovatelů připojení.

7.1.2 Porovnání

Současný stav síťového prostředí ve firmě je brán jako fungující síť běžící především s použitím IPv4. Zůstatkovou cenu nahrazovaných síťových prvků je možno zanedbat. Vyčíslení nákladů tedy bude finanční náročností firemní sítě IPv6. Vyčíslení je provedeno v následující tabulce.

položka	jednotka	počet	MOC bez DPH (Kč)	celkem bez DPH (Kč)	celkem s DPH (Kč)
TP-LINK TL-ER6120	Ks	2	5 529,-	11 058,-	13 380,-
TP-LINK JetStream T1700G-28TQ	Ks	3	5 777,-	17 331,-	20 970,-
konfigurace prvků technikem (odhad)	hod	20	372,- Kč/hod	7 440,-	9 002,-
celkem				35 829,-	43 352,-

Tabulka 1 Finanční zhodnocení nákladů modernizace sítě firmy a implementace IPv6 [vlastní]

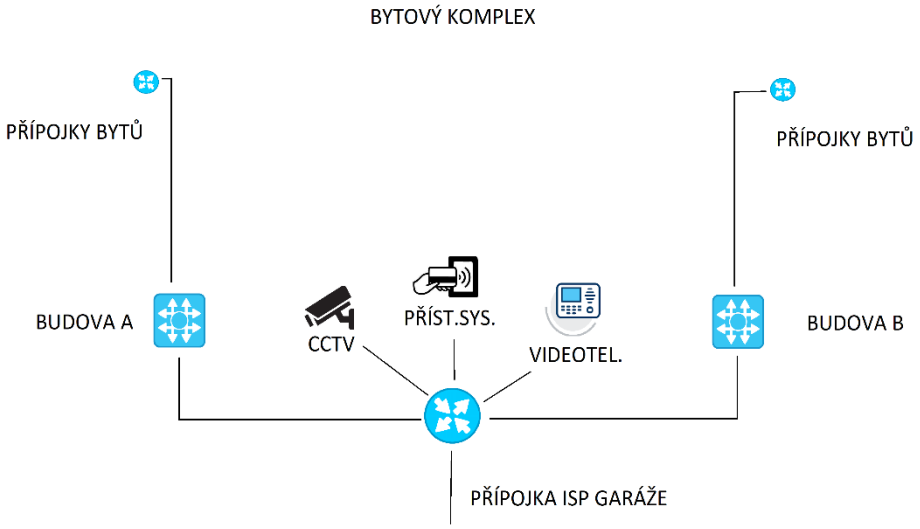
Celkové náklady implementace IPv6 do firemní sítě jsou tedy 43 352,- Kč. Částka není nikterak vysoká s přihlédnutím k tomu, že bylo potřeba vyměnit všechny základní síťové prvky a při výběru prvků nových se zohledňovala jejich kvalita před cenovou úsporou.

7.1.3 VPN

Centrála firmy s pobočkou je spojena pomocí VPN (Virtual Private Network). Při použití IPv4 toto znamená spojení dvou oddělených vnitřních sítí za pomocí virtuálního routeru, který zajistí šifrovanou komunikaci. V případě IPv6 mají všichni klienti v obou sítích veřejnou IP adresu. Použití firewallu mezi internetem a jednotlivými vnitřními sítěmi je tedy nutností. Nastavením striktních pravidel pro provoz na vnitřních sítích v kombinaci s firewallem se dosáhne dostatečné bezpečnosti. Absence NATu navíc dovolí pravidla zjednodušit a předejít chybám v jejich nastavování. Díky veřejným IP adresám se obě sítě bez problémů vidí. Pro zajištění komunikace mezi centrálou a pobočkou stačí v pravidlech firewallu povolit provoz mezi sítěmi. V tuto chvíli ale bude onen provoz nezabezpečen a kdokoli na internetu může nejenom zjistit IP adresy počítačů a s tím i strukturu sítě, ale i číst obsah paketů a tím pádem neinvazivně získávat firemní informace. Proto bych zde navrhl použití IPsecu mezi sítěmi. IPsec je bezpečnostní rozšíření přímo podporované v IPv6 a zajistí šifrované spojení mezi centrálou firmy a pobočkou. Každý paket procházející routerem se zapnutým IPsecem je porovnán s tabulkou politik, která je nastavitelná. V případě centrály firmy se například nastaví, že všechny pakety odcházející na pobočku je třeba zašifrovat a zároveň všechny pakety přicházející z pobočky na centrálu jsou zašifrované a je třeba je rozšifrovat. Na pobočce firmy se pak nastaví totéž (samozřejmě se záměnou termínů pobočka a centrála) a bezpečnost komunikace je zajištěna.

7.2 Obytný komplex

Druhý příklad popisuje menší bytový komplex (Obr. 17) o dvou budovách bytové výstavby. Obě budovy spojuje společná podzemní garáž, ve které se nachází přípojka poskytovatele internetu. Všechny bytové jednotky v komplexu tedy mají stejného poskytovatele pevného internetu. Rozvod sítě je veden od přípojky skrze garáže do racku v 1PP každé z budov a následně pak stoupacím vedením do bytových jednotek. V rámci komplexu je instalován kamerový systém a obyvatelé ke vstupu a ovládání výtahu používají čipový systém. Dále je v bytech instalován systém videotelefonů se vzdáleným přístupem z mobilní aplikace. Logická topologie sítě obytného komplexu je jasně patrná z obrázku 16.



Obr. 17 Topologie sítě obytného komplexu [vlastní]

7.2.1 Náklady

Protože je obytný komplex nedávno dostavěný, všechny aktivní prvky v síti plně podporují IPv6 a konektivita klientských uzlů je zároveň předpokládána. Jedinými náklady na implementaci tedy budou náklady na zpřístupnění nativní IPv6 konektivity ze strany lokálního poskytovatele internetového přepojení a finanční odměna správce sítě při konfiguraci firewallu, nastavení výchozí brány sítě a přidělení adres. Síť komplexu bude po přechodu v režimu dual stack a pro přidělení adres klientských uzlů se použije DHCPv6. Adresy síťových prvků přístupového a kamerového systému budou nastaveny staticky, stejně tak adresa bran pro systém domovních videotelefonů.

Náklady poskytovatele internetu na zpřístupnění nativní IPv6 konektivity nelze dostatečně dobře odhadnou. Oslovení poskytovatelé (byli osloveni tři z menších poskytovatelů internetového připojení z okolí Prahy) nebyli ochotní poskytnout informace ohledně náročnosti změn v jejich infrastruktuře směrem zajištění plné IPv6 konektivity. To pravděpodobně z kombinace důvodů, že se nejedná o reálnou zakázku a zároveň nechtějí sdělit informace o stavu jejich infrastruktury a její připravenosti podporovat plně IPv6. Zástupce jednoho z poskytovatelů dokonce vyjádřil podiv nad požadavkem na IPv6 konektivitu a označil jej za zbytečný. Zároveň se vyjádřili dostatečně jasně, že si nepřejí, aby v této práci byla jejich jména zmíněna.

7.2.2 Porovnání

Výchozí stav síťového prostředí se tedy opět dá považovat za plně funkční z hlediska IPv4. Porovnáním tohoto beznákladového stavu a stavu po provedení nutných úprav se započtením nákladů se dosáhne vyčíslení finanční náročnosti přechodu sítě obytného komplexu na IPv6 (Tab. 2).

položka	jednotka	počet	cena/jednotka	cena celkem
Náklady poskytovatele na poskytnutí nativní IPv6 konektivity	nelze odhadnout			
Konfigurace prvků technikem	Hod	10	450 Kč/hod	4 500,-Kč
celkem				4 500,- Kč

Tabulka 2 Vyčíslení nákladů na implementaci IPv6 do sítě bytového komplexu [vlastní]

Náklady na implementaci IPv6 tedy činí 4 500,- Kč. Tato částka je poměrně nízká především kvůli tomu, že není nutné kupovat žádný nový hardware. Zároveň však neodráží náklady poskytovatele, které nelze dostatečně dobře odhadnout.

8 Diskuze a výhled do budoucnosti

IPv6 by tedy potřeboval nějaký impuls k širšímu rozšíření. Otázkou je, co by tím impulsem mohlo být. Nabízí se úvaha, že by to mohlo být naprosté vyčerpání všech IPv4 adres. To by ale mohlo být již dost pozdě. Bylo by pravděpodobně lepší zvolit nějakou formu podpory ze strany politiků. A to nejen formou nařízení a doporučení. Ta se totiž zatím neukázala jako

účinná. Řešení by mohlo být například formou poskytnutí úlevy na dani poskytovatelům, kteří budou budovat infrastrukturu se zajištěnou IPv6 konektivitou. Podobná úleva funguje v Portugalsku pro veškeré investice realizované zahraničními subjekty. Zároveň by bylo potřeba zvýšit informovanost nejen veřejnosti, ale především správců a vlastníků síťových prostředí směrem k tomu, aby IPv6 implementovali a požadovali nativní konektivitu.

Nastupující internet věcí si změnu ve velmi krátké době vynutí sice sám, ale pokud nebude infrastruktura, budou uživatelé odříznuti od využití všech jeho možností. Zároveň pokud nebude informovanost všech, kterých se to týká na dostatečné úrovni, bude se následně nutná implementace tzv. „šít horkou jehlou“, což by mohlo mít potenciálně za následek vážné ohrožení bezpečnosti na síti.

9 Závěr

V textu této práce bylo několikrát jasně naznačeno, že hromadný přechod na IPv6 je nevyhnutelný a nutný. Nejen protože IPv4 adresy došly, ale především proto, že nároky dnešní doby, jako jsou masivní konzumace internetového obsahu, vymísťování dat do cloudu a internet věcí, jsou den ode dne větší a přestárlé IPv4 je nedokáže dlouhodobě uspokojit.

Bohužel je přístup k IPv6 ze všech zúčastněných stran velice laxní. Přijatá nařízení se nedodržují, memoranda k IPv6 přechodu nejvíce vystihuje rčení: „Papír toho snese hodně“. Argumentace správců sítě, že přechod by byl záležitost finančně náročná už je mnoho let naprosto lichá. Všechna moderní zařízení jsou již dávno kompatibilní a i tam, kde by byla nutná výměna nějakého hardware, jsou náklady relativně nízké. Většinový podíl nákladu tak tvoří náklady na lidskou práci a ochota zúčastněných. A především ochota je v souvislosti s touto problematikou nedostatková. Poskytovatelé připojení se povětšinou o IPv6 bavit vůbec nechtějí a na otázky ohledně stavu jejich sítě v souvislosti s poskytnutím nativní podpory IPv6 buďto mlčí, nebo užitečnost IPv6 dokonce rozporují. Není výjimkou, především u menších poskytovatelů internetu, mít klidně i celé části sítě (vsi, osady atp.) za NATem a jejich připravenost na IPv6 konektivitu je prakticky nulová.

Budoucnost rozhodně patří internetu. A dnes to platí více než kdy jindy. Z doby internetu pro lidi se pomalu ale jistě přesouváme do doby internetu pro věci. Ještě nedávno to bylo nepředstavitelné, dnes se jedná o běžnou realitu. Nejen ovládání věcí na dálku, ale vzdálená odpověď od věci, a dokonce i vzdálená akce iniciovaná věcí samotnou. To vše se dnes běžně děje. Věci mohou i komunikovat vzájemně mezi sebou a na základě požadavků pak situaci vyhodnocovat a konat akce. Současný trend v digitalizaci a automatizaci výroby, známý též jako Průmysl 4.0, počítá s využitím kyberneticko-fyzikálních systémů, které budou vykonávat především opakující se a jednoduché činnosti, aby tato práce již nemusela být obsluhována lidmi. Produkty i stroje mají dostat každý vlastní identifikaci na základě které budou moci vzájemně komunikovat a bude je možno vzdáleně kontrolovat a řídit. Inteligentní domácnosti, inteligentní systémy, inteligentní a „smart“ řešení, to je dnes obsah reklamních poutačů. Svého uživatele si najde dokonce i lahev na pití, která vede statistiku o množství vypité tekutiny. A spousta z nás by chtěla, aby nás na konci pracovního dne vyzvedl před prací

náš samořídící vůz a odvezl nás na večeři do restaurace, kde nám rezervaci zajistil náš chytrý domácí asistent a podle naší aktuální diety nám zúžil výběr z místního menu. Nic z toho ale nebude možné bez unikátní identifikace jednotlivých prvků v síti. IPv6 je naše nutná budoucnost. Jinou alternativu totiž nemáme.

10 Použité zdroje

[1] Vinton G. Cerf, Robert E. Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. 22, No. 5, May 1974 pp. 637–648.

[2] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[3] DOYLE, Jeff a Jennifer DeHaven CARROLL. *Routing TCP/IP*. 2nd ed. Indianapolis, Ind.: Cisco Press, 2006. ISBN 15-870-5202-4.

[4] CASAD, Joe. *Sams teach yourself TCP/IP in 24 hours*. 4th ed. Indianapolis, Ind.: Sams, c2009. ISBN 978-0-672-32996-8.

[5] MUDRÁK, David. *Zapouzdření dat v síti TCP/IP* [online]. In: [cit. 2019-02-10]. Dostupné z: https://commons.wikimedia.org/wiki/File:Tcpip_zapouzdreni.svg#/media/File:Tcpip_zapouzdreni.svg

[6] SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011. CZ.NIC. ISBN 978-80-904248-4-5.

[7] *IPv5* [online]. [cit. 2019-02-10]. Dostupné z: http://www.jiribrejcha.net/2008/01/jak-je-to-s-ipv5-existoval-vubec-nekdy/

[8] Subnetting, supernetting a CIDR [online]. [cit. 2019-02-23]. Dostupné z: http://www.earchiv.cz/anovinky/ai1681.php3

[9] Proč není NAT totéž, co firewall [online]. [cit. 2019-02-26]. Dostupné z: https://www.root.cz/clanky/proc-neni-nat-totez-co-firewall/

[10] *IP address representation and classes* [online]. In: [cit. 2019-02-23]. Dostupné z: http://h22208.www2.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3942_l3-ip-svcs_cg/content/images/image8.png

[11] *Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied* [online]. [cit. 2019-02-26]. Dostupné z: https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf

[12] *IPv4 Address Report* [online]. [cit. 2019-02-26]. Dostupné z: http://ipv4.potaroo.net/

[13] DEERING Stephen, HINDEN Robert. Internet Protocol, Version 6 (IPv6) Specification. http://www.ietf.org/. [Online] The Internet Engineering Task Force (IETF), December 1995. [cit. 2019-02-27].https://tools.ietf.org/html/rfc1883

[14] PODERMAŃSKI, Tomáš. *IPv6 Mýty a skutečnost, díl II. - Adresový prostor* [online]. [cit. 2019-02-28]. Dostupné z: https://www.lupa.cz/clanky/ipv6-myty-a-skutecnost-dil-ii-adresovy-prostor/

[15] THOMSON Susan, HUITEMA Christian, KSIANT Vladimir, SOUISSI Mohsen. DNS Extensions to Support IP Version 6. http://www.ietf.org/. [Online] The Internet Engineering Task Force (IETF), October 2003. [cit. 2019-02-28]. https://tools.ietf.org/html/rfc3596

[16] *RIPE NCC RIPEness* [online]. [cit. 2019-03-03]. Dostupné z: http://ripeness.ripe.net/

[17] *Čtvrtina uživatelů Google má k dispozici IPv6* [online]. In: [cit. 2019-03-03]. Dostupné z: https://www.root.cz/zpravicky/ctvrtina-uzivatelu-google-ma-k-dispozici-ipv6/

[18] *IPv6 adoption* [online]. [cit. 2019-03-03]. Dostupné z: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption

[19] IPv6 Capable Rate by country (%) [online]. [cit. 2019-03-03]. Dostupné z: https://stats.labs.apnic.net/ipv6/

[20] https://www.lupa.cz/clanky/jak-jsou-na-tom-weby-ceskych-uradu-s-dnssec-a-ipv6/

[21] *IPv4 and IPv6 Header Differences* [online]. [cit. 2019-03-03]. Dostupné z: https://www.juniper.net/documentation/en_US/junose15.1/information-products/topic-collections/swconfig-ip-ipv6/index.html?topic-64529.html

[22] Comparison of IPv6 support in operating systems. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-03]. Dostupné z: https://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems

[23] Už i v Africe docházejí IPv4 adresy. *Root.cz* [online]. [cit. 2019-03-17]. Dostupné z: https://www.root.cz/clanky/uz-i-v-africe-dochazeji-ipv4-adresy/

[24] *DNSSEC* [online]. [cit. 2019-03-17]. Dostupné z: https://www.dnssec.cz/

[25] [online]. [cit. 2019-03-17]. Dostupné z: https://www.lupa.cz/clanky/jak-jsou-na-tom-weby-ceskych-uradu-s-dnssec-a-ipv6/

[26] *Podpora mobilních zařízení* [online]. [cit. 2019-03-18]. Dostupné z: https://www.ipv6.cz/Podpora_mobiln%C3%ADch_za%C5%99%C3%ADzen%C3%AD

[27] PODERMAŃSKI, Tomáš. IPv6 Mýty a skutečnost, díl I. - Jak jsme na tom. *Lupa.cz* [online]. 2011 [cit. 2019-03-20]. Dostupné z: https://www.lupa.cz/clanky/ipv6-myty-a-skutecnost-dil-i-jak-jsme-na-tom/

[28] [online]. [cit. 2020-03-28]. Dostupné z: http://opendata.labs.lacnic.net/ipv4stats/graphs/ipv4avail.html

[29] *Samuraj* [online]. [cit. 2020-03-28]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-qos-3-omezovani-rychlosti-policing-shaping/

[30] IPv6 test [online]. [cit. 2019-03-03]. Dostupné z: https://ipv6-test.com/validate.php

11 Seznam obrázků

12 Seznam tabulek

13 Seznam použitých zkratek

ARP - Address Resolution Protocol

CIDR - Classless Inter-Domain Routing

CNGI - China Next Generation Internet

CRC - Cyclic Redundancy Check

ČSÚ – Český Statistický Úřad

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

DNSSEC- Domain Name System Security Extensions

FTP- File Transfer Protocol

GSM – Groupe Spécial Mobile

IANA – Internet Assigned Numbers Authority

ICANN – Internet Corporation for Assigned Names and Numbers

IEEE – Institute of Electrical and Electronics Engineers

IP – Internet Protocol

IPng – Internet Protocol next generation

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

IoT – Internet of Things

ISO/OSI - International Organization for Standardization/ Open Systems Interconnection

ITU - International Telecommunication Union

LAN – Local Area Network

LIR – Local Internet Registrator

MAC - Media Access Control

MTU – Maximum Transmission Unit

NAT – Network Address Translation

ND – Neighbour Discovery

NTP - Network Time Protocol

QoS – Quality of Service

RFC – Request For Comments

RIR – Regional Internet Registrator

SMTP - Simple Mail Transfer Protocol

SQL - Structured Query Language

SSH – Secure Shell

TCP - Transmission Control Protocol

TLD – Top Level Domain

UDP - User Datagram Protocol

VoIP - Voice over Internet Protocol

WAN - Wide Area Network