Acta Informatica Pragensia ISSN 1805-4951

Šablona v1.0.

Online: aip.vse.cz

Problémy implementace IPv6

Problems with IPv6 Implementation

Vladimír Nulíček

Katedra informatiky a matematiky, Fakulta ekonomických studií,

Vysoká škola finanční a správní, a.s.

Estonská 500, 100 00 Praha 40

vnulicek@gmail.com

Abstrakt: Cílem článku je popsat aktuální stav zavádění IPv6 u nás i ve světě včetně srovnání různých přechodových mechanismů mezi IPv4 a IPv6 a výhledu do budoucna. Článek vychází z rozsáhlé rešerše aktuálních zdrojů vztahujících se k této problematice, dostupných na Internetu. Zabývá se rovněž hlavními bezpečnostními riziky spojenými s novou verzí IP protokolu. Pozornost je rovněž věnována ekonomickému zhodnocení implementace IPv6. Článek by měl být pomoci zájemcům o přechod k protokolu IPv6 k lepší orientaci v této složité problematice.

Klíčová slova: IP protokol, IPv4, IPv6, přechodové mechanismy, dvojí zásobník, tunelování, překladače.

Abstract: The aim of the article is to describe the current status of IPv6 implementation in our country and in the world, including the comparison of the different IPv4 and IPv6 transition mechanisms and the outlook for the future. The article is based on extensive research of current sources related to this issue, available on the Internet. It also describes the major security risks associated with the new IP protocol version. Attention is also paid to the economic evaluation of the implementation of IPv6. The article should help those interested in moving to IPv6 to better focus on this complex issue.

Keywords: IP protocol, IPv4, IPv6, transition mechanisms, dual stack, tunneling, translators.

1 Úvod

IP protokol je hlavním protokolem, fungujícím na síťové vrstvě architektury TCP/IP počítačových sítí a Internetu. Hlavním úkolem IP protokolu je zabezpečit datagramovou službu, tzn. je zodpovědný za směrování datagramů (paketů) ze zdrojového počítače k cílovému uzlu přes jednu nebo více IP sítí.

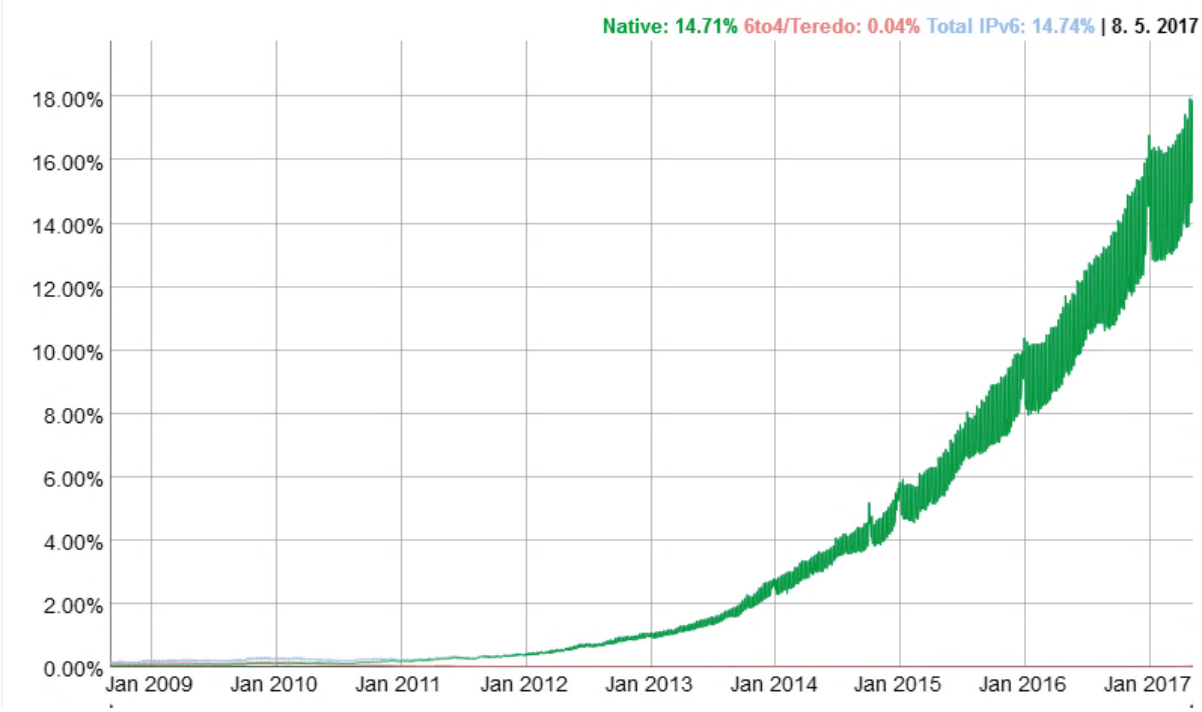
Již cca 20 let existuje nová verze IP protokolu IPv6, která by postupně měla nahradit verzi IPv4. Zavádění nové verze však stále naráží na řadu překážek a aktuální procento implementace IPv6 protokolu není zdaleka na takové výši, jak si tvůrci této verze (tedy především IETF – www.ietf.org) představovali. V tomto článku bych se chtěl zamyslet nad hlavními příčinami této situace a nad předpokládaným budoucím vývojem implementace IPv6 v České republice i ve světě.

Článek vychází z rozsáhlé rešerše aktuálních zdrojů k této problematice, dostupných v databázích Scopus (https://www.elsevier.com/solutions/scopus), Web of Science (https://clarivate.com/products/web-of-science/), databáze Proquest (https://search.proquest.com/central/index) a IETF RFC (https://www.ietf.org/rfc.html).

Článek by měl posloužit zájemcům o tuto problematiku k seznámení se se současným stavem, možnostmi a riziky přechodu na IPv6 . Zároveň by měl poskytnout informace zájemcům o připojení své sítě pomocí nové verze IP protokolu.

2 Současný stav implementace IPv6 u nás a ve světě

Na obrázku 1 je graf nárůstu procenta uživatelů, využívajících novou verzi IP protokolu – měřeno procentem uživatelů, kteří přes novou verzi protokolu přistupují k serveru google.com.



Obr. 1: Procento uživatelů využívajících IPv6 (Google, 2017)

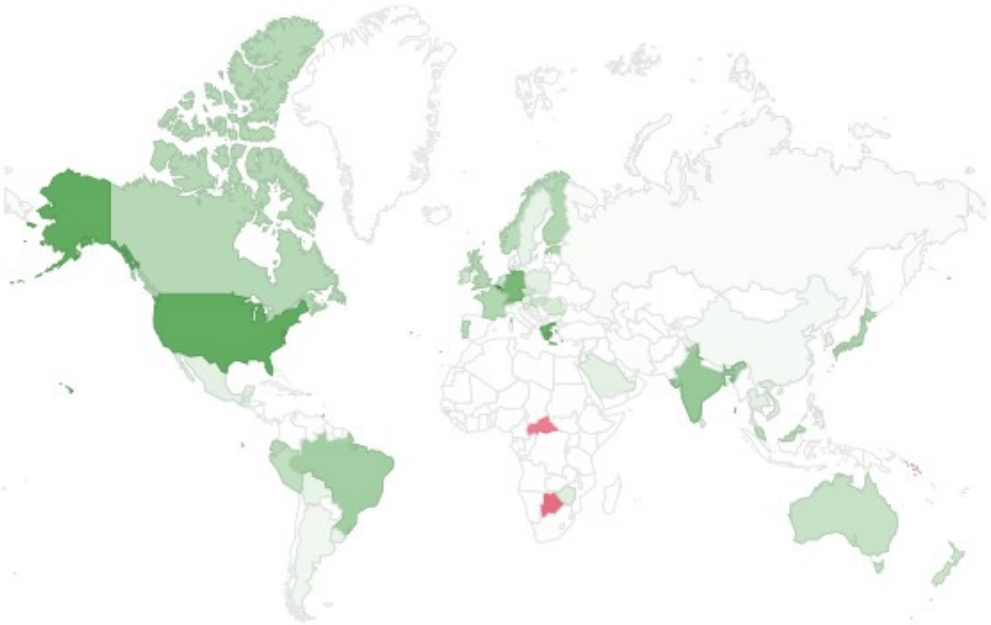
Z tohoto grafu lze přibližně odvodit i celkové procento uživatelů, kteří IPv6 v současné době používají. Přes poměrně rychlý nárůst od roku 2014 je současný poměr konektivity prostřednictvím IPv6 těsně pod hranicí 20%.

Velmi nerovnoměrné je rovněž rozložení implementace IPv6 ve světě – viz následující tabulka. Nejvíce se na rozšíření IPv6 podílejí Spojené státy a několik dalších zemí (Japonsko, Brazílie, Indie, v Evropě např. Belgie, Řecko a Německo) – viz následující tabulka.

USA	34,46
Brazílie	19,12
Kanada	16,65
Indie	21,78
Čína	17,28
Německo	29,11
Řecko	31,52
Belgie	47,91
Česká republika	10,55
Slovensko	1,23
Polsko	5,59
Rakousko	5,56

Tab. 1: Procento konektivity prostřednictvím IPv6 ve vybraných zemích (Google, 2017)

.



Obr. 2: Implementace IPv6 podle států (Google, 2017)

Řadu zajímavých prezentací, týkajících se současného stavu nasazení IPv6 ve srovnání s verzí IPv4 lze nalézt na webu Geoffa Hustona (http://www.potaroo.net/presentations/)

Česká republika je v současné době, co se týče procentní implementace IPv6 protokolu, někde na průměru Evropské unie – procentní podíl nové verze protokolu činí cca 10,5 %. Je to o mnoho méně než např. v Německu, Belgii nebo Řecku, ale naopak znatelně vyšší podíl než v sousedním Slovensku, Polsku nebo Rakousku

3 Co přináší IPv6 nového oproti IPv4

Základní nové charakteristické vlastnosti nové verze protokolu IPv6 jsou popsány např. v (Desmoules, 2003). Nejnovější specifikace IPv6 je obsažena v (Deering, Hinden, 2017)

Lze je shrnout do těchto bodů:

- Je zaveden nový formát IP adres – rozměr 128 bitů (16 bytů) přináší ohromný nárůst adresního prostoru na 2^{128}, tj. cca 3,4 x 10^{38} unikátních adres. V rámci přechodových mechanismů je nutno zajistit integraci (mapování) IPv4 adres do nového formátu IPv6 adres – touto problematikou se zabývá např. (Gnana, Albert, 2010)
- IPv6 přináší víceúrovňovou hierarchii IP adres, což napomáhá agregaci přenosových cest a podporuje efektivní a škálovatelný routing. Nový formát IP adres je specifikován v RFC 4291 (Hinden, Deering, 2006) a diskutován např. v (Brzozowski, 2007)
- Je umožněna automatická stavová i bezstavová konfigurace IP adres. Princip bezstavové automatické konfigurace je definován v RFC 4862 (Narten a kol., 2007)
- IPv6 umožňuje multihoming se zachováním striktní agregace přenosové trasy. Problematika multihomingu bez nutnosti použití NATu je popsána v RFC 7157 (Troan, 2014)
- Přechod mezi IPv6 providery je pro koncové uživatele tranparentní s využitím mechanismu přečíslování
- ARP broadcast je nahrazen multicastem (resp. anycastem).
- Hlavička IPv6 datagramů je jednodušší a přehlednější (méně polí, odstranění kontrolního součtu)
- Do hlavičky IPv6 datagramu byla zavedena tzv. „další hlavička – next header“, která nahradila pole „Option“ – specifikováno v RFC 6564 (Krishnan a kol, 2012)
- Služba IPv6 byla navržena tak, aby lépe zvládla mechanismy mobility a některé bezpečnostní mechanismy (např. povinné zavedení IPsec)
- Byla vytvořena řada přechodových mechanismů mezi protokoly IPv4 a IPv6 (tunely, dual stack, překladače), které podporují efektivní přechod k nové verzi IP protokolu
- Byly vytvořeny nové verze protokolů, podporující směrování v IPv6 sítích – např. nová verze protokolu RIPng – popsán v RFC 2080 (Malkin, Minnear, 1997) a dále diskutován např. v (Marsruroh a kol, 2016) – nebo protokol SEND – specifikován v RFC 3971 (Arkko a kol., 2005).

4 Překážky rychlejší implementace IPv6

Oproti původním plánům je reálná implementace IPv6 mnohem pomalejší než se při jeho vzniku předpokládalo. Dokonce i řada IT odborníků a specialistů na počítačové sítě jsou

k zavádění nové verze IP protokolu značně skeptičtí. Např. Randy Bush (2017) uvádí, že pro řadu korporátních uživatelů jsou velkým problémem nedostatky v DHCPv6. „*Současný internet je příliš velký, do IPv4 byly investovány obrovské prostředky a to všechno přináší setrvačnost a odpor k změnám.*“

Hlavními překážkami, které skeptici vůči IPv6 uvádějí, jsou:

- zpětná nekompatibilita – uživatel musí mít možnost dostat se k IPv4 zdrojům, což vyžaduje implementaci některých přechodových mechanismů
- nedostatek služeb podporujících IPv6 – zde nastává otázka, co je příčina a co důsledek. Protože není dostatek služeb IPv6, uživatelé nemají zájem o jeho zavádění, naopak vývojáři necítí tlak na vývoj služeb podporujících IPv6, protože je nedostatek uživatelů
- některé nedostatky a bezpečnostní rizika IPv6 – stav v oblasti bezpečnosti IPv6 se ale průběžně zlepšuje a tato rizika jsou skeptiky spíše nadhodnocována
- ekonomika – zavádění IPv6 něco stojí, tak proč jej zavádět, když zatím docela dobře funguje IPv4.

4.1 Řešení zpětné kompatibility IPv6 vs. IPv4

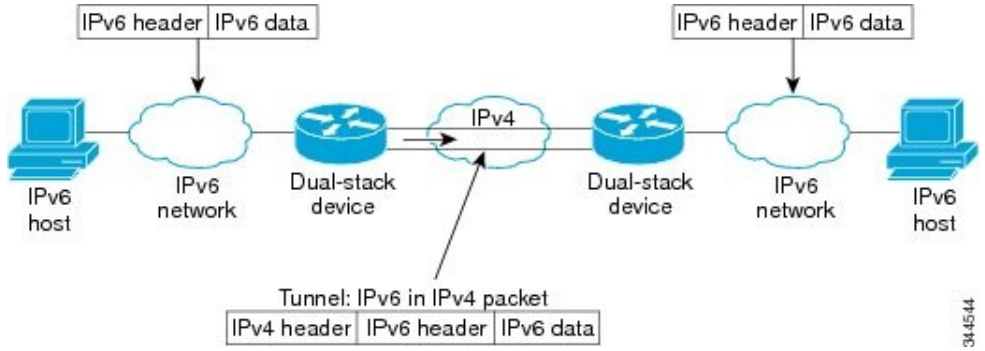
Nový protokol IPv6 přináší spoustu změn a nových vlastností, které jej činí nekompatibilním se starší verzí IPv4. Jako reakce na tyto problémy vznikly zároveň také různé přechodové mechanismy, které umožňují dočasnou funkčnost obou protokolů vedle sebe. Tyto mechanismy by měly v současné době umožnit připojit uživatele, kteří již používají IPv6 do celosvětové sítě. Poté, co převáží IPv6 nad IPv4, by naopak měly umožnit připojit do globální sítě zbývající IPv4 ostrůvky.
Přechodové mechanismy lze v zásadě rozdělit do tří kategorií:

- Dvojí zásobník (Dual Stack)
- Tunelování (Tunelling)
- Překladače (Translators)

V současné době existuje řada přechodových mechanismů mezi IPv4 a IPv6. Jejich srovnání lze nalézt např. v článcích (Kim, 2014), (Cui a kol., 2013), (Stefann a kol., 2013), (Altangerel a kol., 2016), (Quintero a kol., 2016), (Sookun, Bassoo 2016), (Kumar a kol., 2016), (Komal, 2015), (Aravind, Padmavathi, 2015) a řadě dalších.

V následujících podkapitolách se zaměříme na některé tunelovací mechanismy, které jsou nejčastěji používanými přechodovými mechanismy mezi IPv4 a IPv6. Podrobnou analýzou různých metod tunelování se zabývá např. (Pyung S. K., 2017). Podrobné srovnání tunelovacích mechanismů naleznete rovněž v RFC 7059 (Stefann, 2013).

Ne všechny routery na cestě mezi dvěma uzly pracujícími na IPv6 musí nutně podporovat tuto novou verzi protokolu. Princip tunelování spočívá v tom, že pakety IPv6 jsou umístěny do IPv4 paketů, které jsou následně směrovány pomocí IPv4 routerů – viz obr. 3.



Obr. 3: Základní princip tunelování (Cisco online: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-isatap-xe.html)

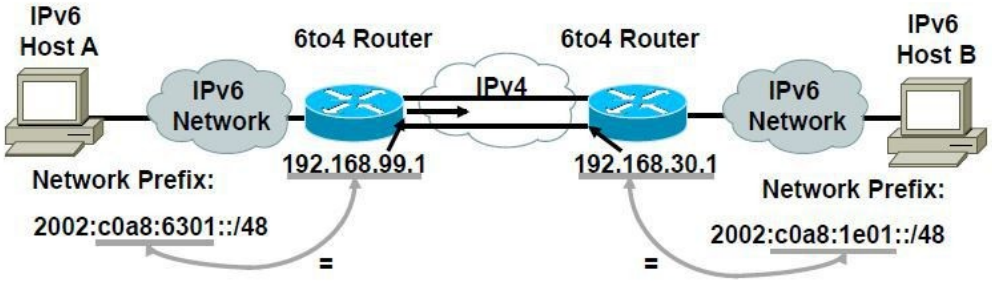
4.1.1 6in4

Mechanismus 6in4 je popsán v RFC 4213 (Nordmark, Gilligan, 2005). Princip tohoto přechodového mechanismu spočívá v tom, že IPv6 datagramy jsou posílány přímo uvnitř IPv4 paketů (využívá se číslo IP protokolu 41 nastavené v hlavičce IPv4 paketů). Po IPv4 hlavičce o velikosti 20 bytů následuje rovnou přenos paketu IPv6 (tedy režie zapouzdření představuje pouze 20 bytů hlavičky IPv4 protokolu).
Nevýhodou tohoto mechanismu je statická konfigurace koncových uzlů. Při použití dynamických IPv4 adres musí být příslušná data pravidelně aktualizována. Další nevýhodou mechanismu 6in4 jsou poněkud vyšší nároky na administraci – je třeba být zaregistrován a následně získat tunel od tzv. *Tunnel Broker* - seznam brokerů lze nalézt např. na https://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers Jedná se o server, který přijímá tunelovaný IPv6 provoz po IPv4 a dále jej přeposílá do nativního IPv6 internetu.

Celkově lze konstatovat, že mechanismus 6in4 je poměrně bezpečná a stabilní technologie pro poskytování přístupu k IPv6 síti. Tato technologie je vhodná pro provoz webových serverů, ke kterým je přístup přes IPv6.

4.1.2 6to4

Přechodový mechanismus 6to4 je specifikován v RFC 3056 (Carpenter, Moore, 2001). Byl navržen tak, aby umožňoval různým doménám IPv6 komunikovat s jinými IPv6 doménami přes IPv4 cloud bez nutnosti vytváření explicitních tunelů IPv4 (tj. jedná se o tzv. mechanismus *point-to-multipoint*). Jde tedy o metodu automatického tunelování, jejímž cílem je poskytnout možnost komunikace koncovým IPv6 sítím prostřednictvím IPv4 s minimální konfigurací. Není nutné explicitně konfigurovat tunel, stačí nakonfigurovat pouze 6to4 směrovač. Princip mechanismu 6to4 je zobrazen na obr. 4.



Obr. 4: Princip tunelovacího mechanismu 6to4 (http://www.ebrahma.com/2013/12/understanding-configuring-ipv6-6to4-tunnels/)

Mechanismus 6to4 vyžaduje, aby IPv6 síť měla k dispozici jednu veřejnou IPv4 adresu. Tu má přiřazenu 6to4 směrovač, jenž je připojen jak k IPv4 Internetu, tak ke koncové IPv6 síti. Z této veřejné IPv4 adresy se vytvoří 6to4prefix, což je IPv6 prefix standardní délky 48 bitů, jehož prvních 16 bitů obsahuje hodnotu 2002 (šestnáctkově) a následujících 32 bitů je tvořeno IPv4 adresou 6to4 směrovače (viz obr. 4). Tento prefix se používá v místní síti zcela obvyklým způsobem, umožňuje definovat podsítě a opatřit zdejší stroje adresami (včetně rozhraní 6to4 směrovače vedoucího do místní sítě). Standardními směrovacími mechanismy se nastaví, že datagramy směřující na adresy s prefixem 2002::/16 se mají předávat 6to4 směrovači. Ten je automaticky balí do IPv4 datagramů (jejichž cílovou IPv4 adresu si vyzvedne ze 6to4 adresy) a odesílá je IPv4 Internetem protějšímu 6to4 směrovači. Přicházející tunelované datagramy naopak vybaluje a předává protokolem IPv6 do místní sítě.

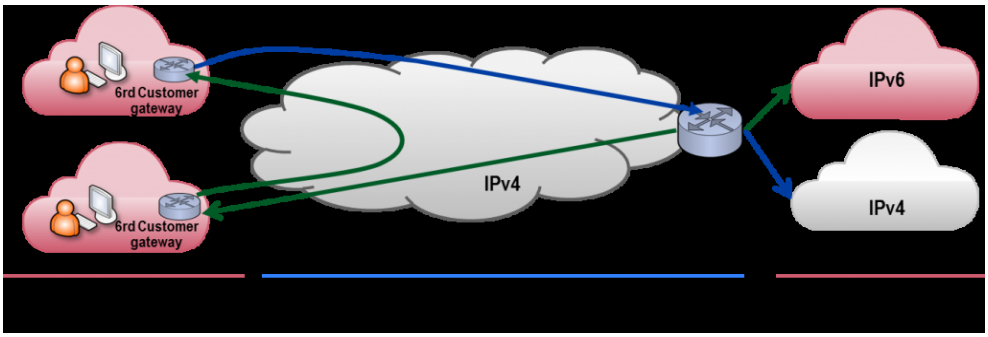
Hlavní výhodou 6to4 je jeho nenáročnost a jednoduchost. K jeho provozování v koncové síti stačí jedna veřejná IPv4 adresa a několik málo konfiguračních příkazů na přístupovém směrovači (který je ideálním kandidátem na 6to4 směrovač).

Největším problémem 6to4 je nespolehlivost. Využívá prvky (zejména zprostředkovatele) provozované různými subjekty, jejichž výběr ve směru od protějšího účastníka komunikace nelze nijak ovlivnit a tudíž garantovat funkčnost. Asymetrické směrování, kdy každý ze směrů komunikace využívá odlišného zprostředkovatele (tj. jiný 6to4 router), je spíše pravidlem než výjimkou. Firewally často mají nastaven zákaz obecného tunelování (protokol 41). Problematika bezpečnosti mechanismu 6to4 je diskutována např. v (Savola, Patel, 2004).

Tři konkrétní mechanismy 6to4 jsou srovnány v příspěvku (Repas, Horvath, Lencse, 2015) na konferenci TSP v r. 2015.

4.1.3 6rd

Tento přechodový mechanismus je definován v RFC 5969 (Townsley, 2010). Mechanismus 6rd je založen podobně jako 6to4 na automatických tunelech IPv6 v IPv4, používá podobné mechanismy jako 6to4, ale je provozován v rámci jednoho poskytovatele internetu (na rozdíl od 6to4, který používá různé IPv6 routery). Veškeré operace související s provozem 6rd probíhají v síti jednoho poskytovatele, je tedy snadnější vše nakonfigurovat, spravovat a garantovat funkčnost. 6rd díky tomu netrpí takovou mírou nespolehlivosti jako 6to4. Zákazníci ovšem nemohou (na rozdíl od 6to4) nasadit 6rd nezávisle na svém poskytovateli. Pokud tento mechanismus poskytovatel neimplementoval, je pro jeho zákazníky nedostupný. Princip mechanismu 6rd je na obr. 5.



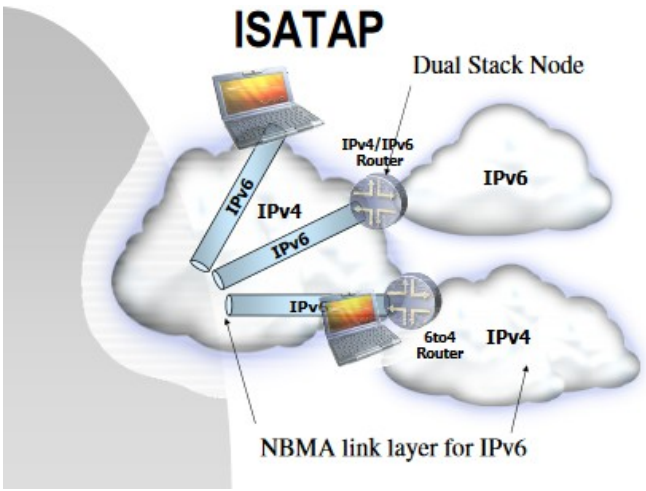
Obr. 5: Princip tunelovacího mechanismu 6rd (https://www.citrix.com/blogs/2012/03/02/6rd-%E2%80%93-ipv6-gets-a-ride-over-ipv4/)

4.1.4 6over4

Zatímco mechanismus 6to4 řeší připojení koncových IPv6 sítí, 6over4 se zaměřuje na jednotlivé počítače připojené pouze do sítě IPv4. Datagramy tunelují přímo koncové počítače, musí proto podporovat oba protokoly (tedy mít implementován Dual Stack). Automatickým tunelem předávají IPv6 datagramy IPv4 sítí 6over4 směrovači, který je pak předává do IPv6 sítě (předpokládá se, že k ní je připojen). Nevýhodou tohoto mechanismu je především to, že je nutné zajistit metodu automatické konfigurace a objevování sousedů, což jsou mechanismy běžně v IPv4 nepodporované. Mechanismus je popsán v RFC 2529 (Carpenter, Jung, 1999). Dynamická autokonfigurace mapování IPv4/IPv6 adres je popsána v (Liu a kol, 2012) a (Liu a kol., 2012).

4.1.5 ISATAP

Mechanismus ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) je specifikován v RFC 5214 (Templin a kol, 2008) ISATAP se snaží řešit podobný problém jako 6over4, ale zároveň nebýt závislý na podpoře broadcastu v IPv4. Z tohoto důvodu zde nelze používat broadcast a není tedy možné použít ani protokol objevování sousedů. Aby stanice nalezly směrovač, pomocí něhož mohou provést automatickou konfiguraci, řeší ISATAP tento problém pomocí seznamu potencionálních směrovačů. Princip mechanismu ISATAP je na obr. 6.



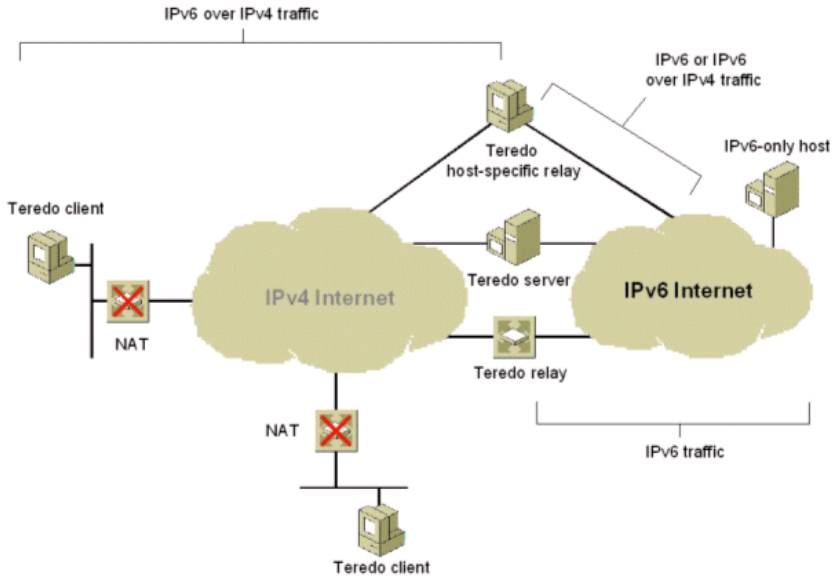
Obr. 6: ISATAP (http://www.it.uc3m.es/diederich/arc/tunnel_isatap.pdf)

4.1.6 Teredo

Mechanismus Teredo je popsán v RFC 4380 (Huitema, 2006). Většina tunelovacích mechanismů si neví rady s překážkou v podobě NATu, který se běžně používá pro překlad privátních IPv4 adres na adresy veřejné a zpět. Mechanismus Teredo tento problém překonává, ale za cenu značné režie, proto je vhodné ho použít až tehdy, kdy ostatní mechanismy selhaly. Je vhodný zejména pro malé domácí resp. firemní sítě, které bývají většinou za NATem. Nevýhodnou je ale jeho poměrně nízká efektivita a často dosti citelné prodloužení doby přenosu dat.

Mechanismus Teredo je tvořen softwarovým programem běžícím pod operačním systémem. Využívá se zde Teredo klient a Teredo server. Teredo klient je za NATem v síti IPv4 a žádá o přidělení IPv6 adresy, zatímco Teredo server má veřejnou IPv4 adresu a přiděluje Teredo

klientům IPv6 adresu. Princip mechanismu Teredo je znázorněn na obr. 7 a blíže popsán např. na serveru technet.microsoft.com.



Obr. 7: Teredo (https://technet.microsoft.com/en-us/library/bb457011.aspx)

Porovnání mechanismů Teredo vs. 6to4 je obsahem příspěvku (Mizoguchi, Ito, 2015) na konferenci ICTC 2015.

4.2 Bezpečnostní rizika IPv6

Vzhledem k tomu, že verze IPv6 je stále ještě poměrně málo rozšířena, jsou bezpečnostní rizika spojená s jejím nasazením větší než u dlouhé doby prověřené verze IPv4. Doladění implementačních detailů u protokolu IPv6 lze očekávat až po jeho masovém nasazení. V této kapitole se budeme věnovat aktuálnímu stavu v oblasti bezpečnosti IPv6 a bezpečnostními riziky spojenými s jeho nasazením. Vyšší bezpečnostní rizika nové verze IP protokolu jsou podle jejích kritiků jednou z překážek jejího rychlejšího zavádění do praxe.

4.2.1 IPsec

IPv6 poskytuje bezpečnostní mechanismy přímo na síťové vrstvě prostřednictvím IPsec (Internet Protocol Security). Oproti IPv4 je implementace IPsec v nové verzi protokolu povinná. IPsec poskytuje jednak službu autentizace, jednak službu šifrování dat. Autentizace slouží k ověření pravosti zdroje dat a ke zjištění, zda přenášená data nebyla během přenosu modifikována. Šifrování zamezuje prozrazení obsahu dat po celou dobu přenosu datagramu. Obě tyto služby jsou realizovány pomocí rozšiřujících hlaviček IPv6 datagramů.

Někteří odborníci se domnívají, že šifrování dat může mít negativní dopad na systémy detekce průniku a na zařízení zjišťující obsah přenášených dat (firewally, aplikační proxy), důsledkem čehož může vzrůst riziko šíření malwaru po síti.

4.2.2 Protokol NDP resp. SEND

Zavedení IPv6 v lokální síti nahrazuje protokol ARP (Adress Resolution Protocol) protokolem NDP (Neighbour Discovery Protocol) - tj. tzv. metodou hledání sousedů. Metoda objevování sousedů je specifikována v RFC 4861 (Narten a kol., 2007). Protože se však ukázalo, že stanice vyžadovaly příliš mnoho informací pro inicializaci bezpečnostních

mechanismů, byl postupně tento NDP protokol nahrazen jednodušším protokolem SEND (SEcure Neighbor Discovery), který používá kryptograficky generované adresy CGA (Arkko, 2005). Úzká vazba protokolu SEND na tyto hašované CGA adresy neumožňuje zabezpečení ostatních typů IPv6 adres.

4.2.3 Nepoužívání NATu

Protože adresní prostor je u IPv6 obrovský, nepočítá se u této verze protokolu s používáním privátních adres, potažmo NATu, jak je znám z verze IPv4. Každé zařízení má tedy svou veřejnou IPv6 adresu (není skryto za NATem), což vede k nutnosti většího důrazu na jeho zabezpečení.

4.2.4 Útoky s použitím přechodových mechanismů

Rovněž použití různých přechodových mechanismů (dual stack, tunelování) zvyšuje riziko nebezpečí napadení IPv6 sítí. IPv6 zavádí mechanismus objevování sousedů a bezstavovou automatickou konfiguraci. Tyto mechanismy rovněž zvyšují nebezpečí útoku proti IPv6 síti. Útočník se např. může vydávat za implicitní směrovač a může tak realizovat útoky založené na prostředníkovi (Man-In-The-Middle). Dále může ostatním počítačům přidělovat nesmyslné adresy nebo zablokovat přidělování nových adres tvrzením, že požadovaná adresa je již používána. Problematika útoků zaměřených proti sítím využívajícím přechodové mechanismy je diskutována např. v (Narayan a kol, 2015) nebo (Elejla a kol., 2016)

Tunelovací mechanismy standardně neimplementují autentizaci, ověření původu a šifrování dat. To má za následek jejich zranitelnost útoky jako je odposlechnutí či vkládání paketů. Potencionální bezpečnostní hrozby u tunelovacího mechanismu 6to4 jsou shrnuty v RFC 3964.
V současné době je v IPv6 kromě automatické bezstavové konfigurace (která byla implementována jako novinka v IPv6) k dispozici i DHCPv6, který umožňuje stavovou automatickou konfiguraci (podobně jako DCHP ve verzi IPv4). Specifikace DHCPv6 je popsána v RFC 3315 (Droms a kol, 2003) nebo v RFC 6334 (Hankins, Mrugalski, 2011).

4.2.5 Podpora mobility

Mobilní zařízení (smartphony, tablety aj.) jsou fenoménem dnešní doby a v budoucnu lze očekávat jejich další rozšiřování. Podpora mobilních zařízení je v IPv6 velmi promyšlená a měla by hrát roli jednoho z významných trumfů při prosazování tohoto protokolu do praxe.

Princip mobility vychází z předpokladu, že každé mobilní zařízení má svoji neměnnou domácí adresu, která by měla být dostupná i během cestování, kdy má zařízení přidělenu dočasnou IPv6 adresu. Mechanismus podpory mobility je dobře popsán v (Satrapa, 2011). Princip směrování v mobilních sítích s podporou IPv6 je specifikován v RFC 6705 (Krishnan a kol., 2012) a dále např. v RFC 7864 (Bernardos, 2016) nebo v RFC 6342 (Koodli, 2011).

Podpora mobility však z hlediska bezpečnosti může hrát negativní roli. Kvůli neustále se měnící topologii mobilní sítě bude obtížné prosazovat bezpečnostní opatření na fyzické vrstvě sítě a bránit se odposlechu při použití protokolů podporujících mobilitu.

4.2.6 Rozšiřující hlavičky

Bezpečnostní problém v nové verzi IPv6 mohou představovat rovněž tzv. „*rozšiřující hlavičky – next headers*“, které jsou novou součástí hlavičky IPv6 datagramu (Krishnan a kol, 2012). Kvůli zrychlení a zjednodušení směrování paketů má základní IPv6 hlavička pevně danou

velikost. Směrovače po cestě tak přesně vědí, kam sáhnout, aby mohly paket rychle poslat do další destinace. Problém je, že další zajímavé vlastnosti protokolu se využívají v rámci rozšiřujících hlaviček, které lze libovolně řetězit. Poslední hlavička v řadě pak obsahuje informace o protokolu, nesoucím data (TCP,UDP). Většina zařízení po cestě si vystačí s informacemi z první hlavičky, nicméně problém může nastat ve chvíli, kdy paket dorazí k nějakému sofistikovanějšímu zařízení, které se stará o filtrování paketů vstupujících do naší sítě. Pokud útočník šikovně zřetězí rozšiřující hlavičky, může se mu podařit celá škála útoků, od průchodu paketu, který měl být zastaven (a který obsahuje data, která chceme doručit cílovému zařízení za firewallem), až po pád zařízení, které paket zpracovávalo.

4.2.7 Multicast

Další novou funkcí IPv6 protokolu je náhrada broadcastu (tj. přenos dat od jednoho uzlu ke všem uzlům v síti), který je běžný v IPv4, za multicast, resp. vytváření tzv. multicastových skupin, k nimž se jednotlivé uzly přiřazují, a data se pak hromadně rozesílají do těchto multicastových skupin. Výhodou je efektivnější využití síťové infrastruktury, na druhou stranu však multicast může vést ke zneužití prostřednictvím DoS útoků (zahlcení sítě), protože většina jednotlivých uzlů si v rámci svých IPv6 adres vytváří několik multicastových skupin. Problematika řešení multicastu v IPv6 je popsána např. v RFC 8114 (Boucadair, 2017) a v RFC 7346 (Droms, 2014).

Komplexní informace o problematice bezpečnosti protokolu IPv6 naleznete v (Vyncke, 2010). Zajímavý je také seriál Bezpečné IPv6 na serveru root.cz (https://www.root.cz/serialy/bezpecne-ipv6)

4.3 Ekonomické hledisko

Přechod na novou verzi IP protokolu nebude samozřejmě zadarmo. Náklady na zavádění IPv6 jsou zejména:

- náklady na obnovu hardwaru – nové prvky obvykle podporují IPv6, staré většinou nikoliv
- náklady na software – mohou být značně rozdílné u řady firem, záleží na potřebách firmy, typu zvolené přechodové metody mezi IPv4 a IPv6 aj.
- náklady na správu sítě – nutnost vyškolení IT specialistů ke konfiguraci nové verze IP protokolu v síti a její následné údržbě

Z hlediska perspektivy lze předpokládat, že náklady na zavádění IPv6 budou postupně klesat s tím, jak se IPv6 stane běžnější záležitostí. Oproti tomu náklady na udržování IPv4 by měly naopak růst – náklady na další NATy, přeprodávání IP adres apod.

V blízké budoucnosti lze tedy očekávat, že komplikace s udržování IPv4 provozu povede řadu firem k názoru, že se jim vyplatí používání IPv4 postupně omezit a nahradit jej IPv6. Pro většinu běžných uživatelů internetu však bude pravděpodobně ještě několik let (či možná desítek let) nutno zachovat dual stack s využitím některých z popsaných přechodových mechanismů mezi oběma verzemi IP protokolu

5 Diskuse

Původní plán zavádění protokolu IPv6 do praxe nebyl zdaleka naplněn. Důvodů pro pomalejší postup implementace je celá řada, a to jak objektivních, tak subjektivních. Většina velkých

společností se v současné době nachází spíše v přípravné fázi přechodu na IPv6, kdy využívají různé přechodové (nejčastěji tunelovací) mechanismy.

Skepse u některých kritiků IPv6 dokonce dosáhla takového stupně, že začali považovat IPv6 za „mrtvé dítě“. Na přelomu let 2016 a 2017 se například znovu objevila diskuse o možnostech implementace inovované verze IPv10, jejíž koncept byl poprvé představen v publikaci (Carlberg, 2009).

Jak uvádí např. Lhotka (2017), zřejmě největším problémem přechodu k IPv6 je nedostatek motivace. V současné době je téměř vše dostupné po IPv4 a vzhledem ke zpětné nekompatibilitě IPv6 vůči IPv4 mohou uživatelé a poskytovatelé IPv6 očekávat různé problémy. Jedná se tak trochu o začarovaný kruh. Novým protokolem je poskytováno málo služeb, proto o něj uživatelé nemají příliš velký zájem. A naopak, protože je málo uživatelů nové verze IPv6, není motivace k poskytování služeb.

Hlavní motivací k zavádění nové verze IPv6 protokolu by měla být možnost obrovského rozšíření adresního prostoru, tj. možnost přidělování veřejných IPv6 adres všem novým zařízením v síti bez nutnosti použití NATu. V dnešní době je nedostatek nových IP adres řešen především použitím privátních adres za NATem, resp. nakupováním volných IPv4 adres. V budoucnu lze ale očekávat, že postupný růst cen IPv4 adres a růst nákladů spojených s NATem povede většinu uživatelů k jejich nahrazování novou verzi IPv6.

Další motivací může být rozšiřující se tzv. „Internet věcí - IoT“, kdy spousta dalších elektronických zařízení (kromě běžných PC, mobilních přístrojů, routerů a dalších dnes již běžných součástí Internetu) bude muset být opatřeny novými IP adresami (Minoli, 2013). IPv6 může být pro IoT potažmo tzv. Průmysl 4.0 velkou šancí a mohl by se stát základním standardním protokolem pro tento nový fenomén dnešní doby.

V příspěvku na konferenci IFIP (Bajpai, Schonwalder, 2015) je uvedeno srovnání obou verzí protokolů IPv4 a IPv6 z hlediska konektivity konečných uzlů v síti podporujících oba typy protokolů (dual stack). Výsledky měření rychlosti připojení byly víceméně srovnatelné.

Lze rovněž očekávat, že IEFT bude vyvíjet další úsilí o omezení řady bezpečnostních a technických problémů, které jsou s implementací nové verze IP protokolu spojené. IEFT vydává každý rok řadu RFC dokumentů, z nichž některé byly v tomto článku citované – kompletní index těchto dokumentů naleznete na webu https://www.rfc-editor.org/rfc-index.html.

Zájemci z řad firem, jejich administrátorů sítí i jednotlivců mohou čerpat informace o aktuálních možnostech využití služeb IPv6 z celé řady webových stránek – např. na serveru www.ipv6.cz nebo na stránkách www.nic.cz/ipv6 i na stránkách velkých poskytovatelů internetu, které služby IPv6 již několik let nabízejí. Konkrétní návody k využití různých přechodových mechanismů k postupnému převodu připojení sítě k IPv6 nabízí rovněž články (Quynh, Minh, 2012) nebo (Nikkhah, Guerin, 2016).

6 Závěr

Přes jisté přetrvávající nedostatky a bezpečnostní rizika lze v nejbližších letech očekávat urychlení procesu implementace protokolu IPv6. Hlavní motivací pro firmy i jednotlivce by mělo být zjednodušení směrování pomocí IPv6 protokolu a výrazné rozšíření adresního prostoru – odpadne problém s překladem privátních adres na veřejné (NAT). Dalším impulsem bude jistě neustále rostoucí počet mobilních zařízení a nový fenomén – Internet

věcí IoT. Nicméně kromě jisté „setrvačnosti“ ve využití IPv4 rychlejšímu rozšiřování IPv6 zatím stále brání některé objektivní a subjektivní příčiny popsané v tomto článku.

Seznam použitých zdrojů

Altangerel, G., Tsogbaatar, E. , Yamkhin, D (2016). Performance analysis on IPv6 transition technologies and transition method. In: *2016 11th International Forum on Strategic Technology (IFOST)* [online]. IEEE, s. 465-469 [cit. 2017-07-31]. DOI: 10.1109/IFOST.2016.7884155. ISBN 978-1-5090-0855-1. Dostupné z: http://ieeexplore.ieee.org/document/7884155/

Aravind, S., Padmavathi, G. (2015). Migration to Ipv6 from IPV4 by dual stack and tunneling techniques. In: *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)* [online]. IEEE, s. 107-111 [cit. 2017-07-31]. DOI: 10.1109/ICSTM.2015.7225398. ISBN 978-1-4799-9854-8. Dostupné z: http://ieeexplore.ieee.org/document/7225398/

Arkko, J. et al. *SEcure Neighbor Discovery* (SEND). http://www.ietf.org/rfc/rfc3971.txt.

Bajpai, V., Schonwalder, J. (2015). IPv4 versus IPv6 - who connects faster? In: *2015 IFIP Networking Conference (IFIP Networking)* [online]. IEEE, s. 1-9 [cit. 2017-07-31]. DOI: 10.1109/IFIPNetworking.2015.7145323. ISBN 978-3-9018-8268-5. Dostupné z: http://ieeexplore.ieee.org/document/7145323/

Bernardos, CJ., Ed. (2016). *Proxy Mobile IPv6 Extensions to Support Flow Mobility*. RFC 7864, DOI 10.17487/RFC7864. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc7864.txt

Boucadair, M., Qin, C., Jacquenet, C., Lee, Y., Wang. Q. (2017). *Delivery of IPv4 Multicast Services to IPv4 Clients over an IPv6 Multicast Network*. RFC 8114, DOI 10.17487/RFC8114. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc8114.txt

Brzozowski, J. J. (2007) Change of address: IPv6. (2007, 01). *Communications Technology, 24*, 1. Retrieved from https://search.proquest.com/docview/223753813?accountid=37662

Bush, R.: *IPv6-Predictions-for-2017*. Dostupné z: https://community.infoblox.com/t5/IPv6-Center-of-Excellence/IPv6-Predictions-for-2017/ba-p/8842

Carlberg K. et al. (2009): *IP Version 10.0: A Strawman Design Beyond IPv6,* [online]: https://saleem.host.cs.st-andrews.ac.uk/publications/2009/rearch2009/rearch2009-cbc2009.pdf

Carpenter, B., Jung, C.: *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels.(*1999). DOI: 10.17487/RFC2529. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc2529.txt

Carpenter, B., Moore, K.: *Connection of IPv6 Domains via IPv4 Clouds.* (2001). DOI: 10.17487/RFC3056. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc3056.txt

Cui, Y. et al. (2013). Tunnel-Based IPv6 Transition. *IEEE Internet Computing* [online]. 17(2), 62-68 [cit. 2017-07-31]. DOI: 10.1109/MIC.2012.63. ISSN 1089-7801. Dostupné z: http://ieeexplore.ieee.org/document/6197175/

Deering, S., Hinden, R. (2017). *Internet Protocol, Version 6 (IPv6) Specification*, STD 86, RFC 8200, DOI 10.17487/RFC8200. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc8200.txt

Desmeules, R. *Cisco self-study: implementing IPv6 networks (IPV6)*. Indianapolis, IN: Cisco, ISBN 15-870-5086-2.

Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., Carney, M. (2003). *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).* DOI: 10.17487/RFC3315. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc3315.txt

Droms, R. (2014). *IPv6 Multicast Address Scopes*. RFC 7346, DOI 10.17487/RFC7346. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc7346.txt

Elejla, O. E., Anbar, M., Belaton, B. (2016). ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review. *IETE Technical Review* [online]. 2016, **34**(4), 390-407 [cit. 2017-07-31]. DOI: 10.1080/02564602.2016.1192964. ISSN 0256-4602. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/02564602.2016.1192964

Huston G. – potaroo.net [online]. http://www.potaroo.net/presentations/

Gnana Jayanthi, J., Albert Rabara, S. (2010). IPv4 addressing architecture in IPv6 network. In: *2010 2nd International Conference on Advanced Computer Control* [online]. IEEE, s. 282-287 [cit. 2017-07-31]. DOI: 10.1109/ICACC.2010.5486617. ISBN 978-1-4244-5845-5. Dostupné z: http://ieeexplore.ieee.org/document/5486617/

Google Statistics [online]: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption

Grégr M., Podermański, T. (2015). *Bezpečné IPv6.* Seriál na serveru root.cz, 2015. [online]: https://www.root.cz/serialy/bezpecne-ipv6

Hankins, D., Mrugalski, T. (2011). *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite.* RFC 6334, DOI 10.17487/RFC6334. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc6334.txt

Hinden, R., Deering, S. (2006). *IP Version 6 Addressing Architecture*, RFC 4291, DOI 10.17487/RFC4291. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc4291.txt

Huitema, C. (2006). *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs).* DOI: 10.17487/RFC4380. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc4380.txt

Kim, P.S:: *Comparison and analysis of IPv4/IPv6 transition technologies*, Telecommunication Review, vol. 24, no. 3, s. 419–432, 2014.

Komal, L. (2015). Performance Evaluation of Tunneling Mechanisms in IPv6 Transition: A Detailed Review. In: *2015 Second International Conference on Advances in Computing and Communication Engineering* [online]. IEEE, 2015, s. 144-149 [cit. 2017-07-31]. DOI: 10.1109/ICACCE. ISBN 978-1-4799-1733-4. Dostupné z: http://ieeexplore.ieee.org/document/7306667/

Koodli, R. (2011). *Mobile Networks Considerations for IPv6 Deployment.,* RFC 6342, DOI 10.17487/RFC6342. [cit. 2017-07-31]. Dostupné z: https://www.ietf.org/rfc/rfc6342.txt

Krishnan, S., Woodyatt, J., Kline, E., Hoagland, J., Bhatia, M. (2012). *A Uniform Format for IPv6 Extension Headers*, RFC 6564, DOI 10.17487/RFC6564. [cit. 2017-07-31]. Dostupné z: https://www.ietf.org/rfc/rfc2080.txt

Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., Dutta, A. (2012). *Localized Routing for Proxy Mobile IPv6*. RFC 6705, DOI 10.17487/RFC6705. [cit. 2017-07-31]. Dostupné z: https://www.ietf.org/rfc/rfc6705.txt

Lhotka, L. (2017). *Stalo se z IPv6 nechtěné dítě Internetu?* Archiv článků CZ NIC, 2017 [online]: https://www.nic.cz/page/922/archiv-publikaci/

Liu, L., Cui, Y., Sun, J., Sun, Q. (2012). The research of 4over6 transition system deployment for IPv6 backbone. *In Computer Science and Network Technology (ICCSNT)*, 2012 2nd International Conference on (pp. 912-915). IEEE.

Liu, Z., Dong, J., Cui, Y., Zhang, C. (2015). Dynamic configuration for IPv4/IPv6 address mapping in 4over6 technology. *In Anti-counterfeiting, Security, and Identification (ASID),* 2015 IEEE 9th International Conference on (pp. 132-136). IEEE.

Malkin, G., Minnear, R. (1997). *RIPng for IPv6*. RFC 2080, DOI 10.17487/RFC2080. [cit. 2017-07-31]. Dostupné z: https://www.ietf.org/rfc/rfc2080.txt

Masruroh, S. U., Fadly, R., Hakiem, N. (2016). Performance evaluation of routing protocols RIPng, OSPFv3, and EIGRP in an IPv6 network. In: *2016 International Conference on Informatics and Computing (ICIC)* [online]. IEEE, s. 111-116 [cit. 2017-07-31]. DOI: 10.1109/IAC.2016.7905699. ISBN 978-1-5090-1648-8. Dostupné z: http://ieeexplore.ieee.org/document/7905699/

Minoli, D. (2013). *Building the internet of things with IPv6 and MIPv6: the evolving world of M2m communications*, 2013. ISBN 978-1-118-47347-4.

Mizoguchi, T., Ito, Y. (2015). Comparison of WebQoE between 6to4 and Teredo. In: *2015 International Conference on Information and Communication Technology Convergence (ICTC)* [online]. IEEE, s. 576-578 [cit. 2017-07-31]. DOI: 10.1109/ICTC.2015.7354614. ISBN 978-1-4673-7116-2. Dostupné z: http://ieeexplore.ieee.org/document/7354614/

Narayan, S., Gupta, R., Kumar, A., Ishrar, S., Khan, Z. (2015). Cyber security attacks on network with transition mechanisms. In: *2015 International Conference on Computing and Network Communications (CoCoNet)* [online]. IEEE, s. 163-169 [cit. 2017-07-31]. DOI: 10.1109/CoCoNet.2015.7411182. ISBN 978-1-4673-7309-8. Dostupné z: http://ieeexplore.ieee.org/document/7411182/

Narten, T., Nordmark, E., Simpson, W., Soliman, H. (2007). *Neighbor Discovery for IP version 6 (IPv6).,* RFC 4861, DOI 10.17487/RFC4861. [cit. 2017-07-31]. Dostupné z: https://www.ietf.org/rfc/rfc4861.txt

Narten, T., Thomson, S., Jinmei, T. (2007). IPv6 stateless address autoconfiguration. (No. RFC 4862). [cit. 2017-07-31]. Dostupné z: https://www.ietf.org/rfc/rfc4862.txt

Nikkhah, M., Guerin, R. (2016). Migrating the internet to IPv6: An exploration of the when and why. *IEEE/ACM Transactions on Networking, 24*(4), 2291-2304.

Nordmark, E., Gilligan, R. (2005), "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, DOI 10.17487/RFC4213. [cit. 2017-07-31]. Dostupné z: https://www.ietf.org/rfc/rfc4213.txt

Quintero, A., Sans, F., Gamess, E. (2016). Performance evaluation of IPv4/IPv6 transition mechanisms. *International Journal of Computer Network and Information Security, 8*(2), 1. Retrieved from https://search.proquest.com/docview/1769733834?accountid=37662

Quynh Anh, N., Minh Nguyen, N. P. (2012). *Transition from IPv4 to IPv6: best transition method for large enterprise networks.* [cit. 2017-07-31]. Dostupné z: https://www.theseus.fi/bitstream/handle/10024/40098/Nguyen_Phu.pdf?sequence=2&isAllowed=y

Ravi Kumar, C. V., Venkatesh, K., Vinay Sagar, M., Praveen Bagadi, K. (2016). Performance Analysis of IPv4 to IPv6 Transition Methods. *Indian Journal of Science and Technology* [online]. 2016, 9(20), - [cit. 2017-07-31]. DOI: 10.17485/ijst/2016/v9i20/90005. ISSN 0974-5645. Dostupné z: http://www.indjst.org/index.php/indjst/article/view/90005

Repas, S., Horvath, V., Lencse, G. (2015). Stability analysis and performance comparison of three 6to4 relay implementations. In: *2015 38th International Conference on Telecommunications and Signal Processing (TSP)* [online]. IEEE, s. 82-87 [cit. 2017-07-31]. DOI: 10.1109/TSP.2015.7296228. ISBN 978-1-4799-8498-5. Dostupné z: http://ieeexplore.ieee.org/document/7296228/

Satrapa, P. (2011). *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, CZ.NIC. ISBN 978-80-904248-4-5.

Savola, P., Patel, C.: *Security Considerations for 6to4.* (2004). DOI: 10.17487/RFC3964. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc3964.txt

Sookun, Y., Bassoo, V. (2016). Performance analysis of IPv4/IPv6 transition techniques. In: *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)* [online]. IEEE, s. 188-193 [cit. 2017-07-31]. DOI: 10.1109/EmergiTech.2016.7737336. ISBN 978-1-5090-0706-6. Dostupné z: http://ieeexplore.ieee.org/document/7737336/

Steffann, S., Van Beijnum, V., van Rein, R. (2013): *A Comparison of IPv6-over-IPv4 tunnel mechanisms*, IETF RFC 7059,

Templin, F., Gleeson, T., Thaler, D. (2008). *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).* DOI: 10.17487/RFC5214. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc5214.txt

Townsley, W., Troan, O. (2010). *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) - Protocol Specification.* DOI: 10.17487/RFC5969. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc5969.txt

Troan, O., Ed., Miles, D., Matsushima, S., Okimoto, T., Wing, D. (2014) *IPv6 Multihoming without Network Address Translation.* RFC 7157, DOI 10.17487/RFC7157. [cit. 2017-07-31] Dostupné z: https://www.ietf.org/rfc/rfc7157.txt

Vyncke, E. et al. *Advanced Security for IPv6 CPE*. http://tools.ietf.org/id/draft-vyncke-advanced-ipv6-security-01.txt