# POČÍTAČOVÉ SÍTĚ - PROTOKOL IPV6: ANO ČI NE?

**Josef Kaderka**

**Univerzita obrany, Fakulta vojenských technologií,
katedra komunikačních a informačních systémů
Kounicova 65, 662 10 Brno**
*josef.kaderka@unob.cz*

## Abstrakt:

*Protokol IP verse 6 (IPv6) velmi pravděpodobně nahradí dnes nejběžněji užívaný protokol IP verze 4 (IPv4), neboť není jiná alternativa. K základním nedostatkům IPv4 patří malý adresní prostor, poměrně komplikované záhlaví IP paketů, znesnadňující provoz ve vysokorychlostních sítích a další. Protokol IPv6 tyto problémy řeší, avšak přestože byl standardizován již před 13 lety, není dosud rozšířen tak, jak bylo očekáváno. Příčin je řada, ať již jde o konservatismus nebo o snahu o finanční úspory. IPv4 a IPv6 nejsou vzájemně kompatibilní, takže přechod na IPv6 nemůže být hladký. Postupně byla navržena řada řešení jeho realizace, některá, ač podporovaná významnými institucemi však již byla zavržena.*

## 1. Úvod

Sada protokolů TCP/IP je již pro mírně poučené laiky nedílně spjata s Internetem a IP adresa zapisovaná formou čtveřice čísel oddělených tečkami samozřejmostí. Zdá se neuvěřitelné, že Internet (či spíše jeho předchůdce ARPANET, existující od roku 1969) dlouhou dobu používal zcela jiné protokoly, jako byl například NCP, a na protokol IP verze 4 (IPv4) přešel počínaje rokem 1981. Datum zrodu vlastního protokolu IPv4 je ovšem starší, obvykle se uvádí rok 1974. Komponenty jako maska podsítě či třídy adres v původním IPv4 nebyly a jejich doplnění si vyžádal život (u tříd také později faktické zrušení). K nám se sice IPv4 dostal nepříliš později, avšak jeho masové rozšíření nastalo až po roce 1991 s budováním akademických sítí. V té době představoval již vyzrálý produkt, prostý dětských nemocí, který až současnosti nebylo třeba dále výrazněji modifikovat.

S odstupem času lze konstatovat, že až na několik málo výjimek byl IPv4 navržen velmi dobře. Bohužel tyto výjimky jsou závažné a speciálně malý, jak se ukázalo, adresní prostor představuje fundamentální problém. Na omluvu tvůrců je nutno říci, že v dané době světu vládly sálové počítače, takže za jedinou IPv4 adresou se ukrývalo celé výpočetní středisko se všemi jeho zaměstnanci; jiné osoby se s počítači téměř nepotkávaly, leda jako uživatelé zadávající své požadavky prostřednictvím děrných štítků, později pak terminálů.

S nástupem mikroprocesorového věku se okamžitě ukázalo, že perspektiva IPv4 není dlouhodobá, což se po komercionalizaci Internetu, která přinesla obrovský hlad po IP adresách, potvrdilo. Ještě v roce 1992 však bylo možné bezproblémově získat IP adresu sítě třídy B (v České republice si takto „nahrabalo“ 14 subjektů; 13 vysokých škol a bývalá Správa pošt a telekomunikací Praha, s.p.), avšak po roce 1993 již toto nebylo možné.

Díky opatřením jako je CIDR (Classless Inter-Domain Routing – jde fakticky o zrušení tříd adres a o přidělování adres podle skutečných potřeb uživatele) a také nesystémovým berličkám typu překlad adres (NAT - Network Address Translation; ten se dnes zdá samozřejmostí, ač tak tomu rozhodně není) se podařilo vyčerpání IPv4 adres oddálit až do dnešních dnů.

Nicméně vývojáři nespali a výsledkem jejich snažení je IP protokol verze 6, IPv6 (číslo verze 5 byla použito poněkud zmatečným způsobem pro tzv. Streaming Protocol, viz RFC 1819; pod označením IPv5 se také ukrývá jiný, čínský produkt). První úplný standard popisující IPv6 byl publikován jako RFC 1883 [1] roku 1995 a poměrně brzy (1998) byl nahrazen inovovanou verzí označenou jako RFC 2460 [2], která platí dodnes. Protokol IPv6 vyřešil problém nedostatečného adresního prostoru a některé další. Přechod na IPv6 je však pozvolný, rozhodně pomalejší, než bylo dříve očekáváno, a je spojen s řadou postupných změn, které se občas vzájemně negují. Došlo tak například k vypuštění jedné z kategorií adres, k doplňování a zase rušení metod implementace či přechodu od IPv4 k IPv6 nebo (v roce 2007) likvidaci značně rozpracovaného mechanismu překladu adres a protokolů (NAT-PT - Network Address Translation – Protocol Translation).

Oproti minulosti má na nás proces dospívání IPv6 bezprostřední dopad, neboť již nejsme izolováni od síťového dění.

Popis problematiky protokolu IPv6 je velmi rozsáhlý a existuje celá řada kvalitních zdrojů, v češtině například [3], [4].

Je třeba zdůraznit, že protokol IPv6 leží z pohledu referenčního modelu síťové architektury dle ISO/OSI na 3., tj. síťové vrstvě, zbývající vrstvy zůstávají v zásadě nezměněny (výjimku tvoří například jmenná služba - DNS).

## 2. IPv6 adresa

Adresa představuje asi nejmarkantnější rys protokolu IPv6. Její délka činí 128 bitů, takže celý adresní prostor obsahuje asi $3{,}4.10^{38}$ unikátních adres. Díky pravidlům pro hospodaření s nimi jich sice v praxi bude možno využít poněkud méně, ale rozhodně se jedná o číslo v pravém smyslu slova astronomické. V rámci zeměkoule je nedostatek IP adres napříště vyloučen.

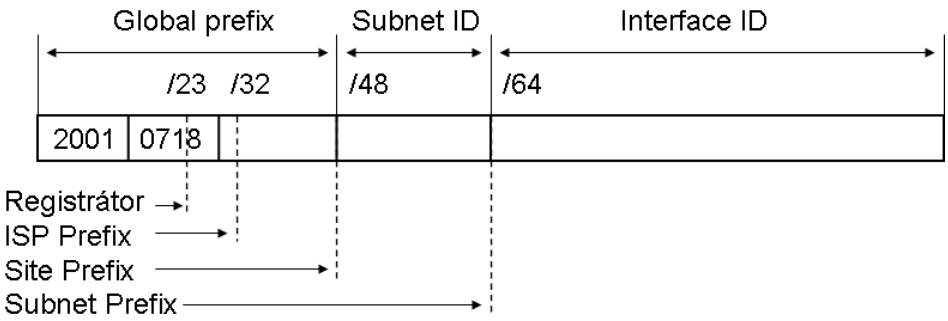
IPv6 adresa se zapisuje formou osmi dvojtečkami oddělených čtveřic hexadecimálních číslic, přičemž tento zápis někdy lze zkrátit (systémy ovšem interně pracují s plnou délkou). Je například možné vypustit vedoucí nulu či nuly ve čtveřici nebo nahradit čtveřici či posloupnost čtveřic obsahujících pouze nuly dvojicí dvojteček (toto v celé adrese pouze jedenkrát). IPv6 adresa se stejně jako IPv4 adresa dělí na část identifikující síť či podsíť a část označující konkrétní rozhraní. Rozsah síťové části se v IPv6 nepopisuje maskou podsítě (ta zcela zmizela), ale prefixem, tj. počtem bitů síťové části - stejně jako v případě CIDR u IPv4.

Příklad tří forem zápisu téže IPv6 adresy

- `2001:0A40:0000:0000:0005:0000:7654:0022`
- `2001:A40:0:0:5:0:7654:22`
- `2001:A40::5:0:7654:22`

Nejkratší zápis funkční IPv6 adresy (jde o loopback, obdoba 127.0.0.1 z prostředí IPv4)

- ::1




*Obr. 1 Typická struktura IPv6 adresy*

Další významnou novinkou je jiné rozdělení typů IP adres. V prostředí IPv6 se lze setkat s těmito typy adres:

- unicast - adresace jediného uzlu (přesněji rozhraní),
  - globální (dosah či platnost celosvětová),
  - site-local (platnost v rámci sítě instituce – tento typ adres již byl zrušen),
  - link-local (platnost v rámci segmentu sítě),
- multicast - adresace skupiny uzlů, pracuje se všemi,
- anycast – adresace skupiny uzlů, pracuje se pouze s jedním.

Adresa typu broadcast známá z IPv4 již v IPv6 není, místo ní se používá multicast s volitelným rozsahem. Rozdíl mezi adresami typu multicast a anycast spočívá v reakci uzlů (resp. příslušných aplikací) na příjem paketu. V případě multicastu se všichni příjemci přijatými daty aktivně zabývají, u anycastu se v rámci skupiny ozve jediný uzel (zřejmě v dané chvíli nejméně zatížený) a komunikace pak probíhá pouze s ním.

| Adresa/prefix | Význam/užití |
|---|---|
| ::/0 (prefix délky 0) | default route |
| ::/128 (samé nuly) | neexistující adresa (RFC4291) |
| ::1/128 (1 na konci) | loopback (RFC4291) |
| ::0:IP:V4/96 | IPv4 kompatibilní adresa (RFC4291 zrušilo) |
| ::ffff:IP:V4/96 | IPv4 mapovaná IPv6 adresa (RFC4291) |
| 2000::/3 | globální unicast adresy (RFC3513) |
| 2002::/16 | 6to4 globální unicast adresy (RFC3056) |
| 3ffe::/16 | 6bone (RFC1897 historické) |
| FC00::/7 | unique local unicast (RFC4193) |
| FE80::/10 | link local unicast (RFC4291) |
| FEC0::/10 | site local unicast (RFC3513 zrušilo) |
| FFgs::/8 | multicast (g=flags, s=scope, RFC4291) |

*Obr. 2 Základní rozdělení IPv6 adresního prostoru*

Díky obrovskému rozsahu adresního prostoru není nutné adresami šetřit a naopak lze přidělenou adresu vhodně členit, resp. v opačném pohledu menší sítě agregovat. Toto

představuje jednu z důležitých výhod IPv6, neboť při dobrém návrhu sítě lze výrazně zefektivnit činnost směrovacích protokolů a směrovačů.

| Adresa/prefix | Uživatel |
|---|---|
| 2001:0718::/32 | CESNET, z.s.p.o. |
| 2001:0718:0800::/42 | CESNET, z.s.p.o., oblast Brno |
| 2001:0718:0808::/48 | CESNET, z.s.p.o., oblast Brno, Univerzita obrany |

*Obr. 3 Příklad členění IPv6 adresního prostoru*

Poměrně značná délka IPv6 adresy dosti limituje její manuální zadávání, byť je toto samozřejmě možné a užívané, například u směrovačů nebo obecně u aktivních síťových prvků. Význačným rysem IPv6 je proto bezstavová autokonfigurace adres. Uzel může získat IPv6 adresu bez potřeby komunikace s DHCP serverem (ten samozřejmě může a bývá v síti přítomen). Při své aktivaci uzel vyšle žádost o konfigurační parametry (multicastem) do místního segmentu; je-li zde přítomen příslušně nastavený směrovač, odpoví uzlu odesláním konfiguračních parametrů síťové vrstvy.

Specifické místo má adresa typu Link Local. Ta se nijak nekonfiguruje, nýbrž ji každé rozhraní získá automaticky po své aktivaci. Adresa typu Link Local má sice jen místní dosah (tj. v rámci segmentu), plně však postačuje pro řadu úkonů jako je objevování sousedů, oznamování směrovače a detekci duplicitních adres, ale i pro účely výměny informací pro účely směrovacích protokolů jako jsou OSPFv3 nebo RIP-NG.

Další nový typ IPv6 adresy nese označení ULA - Unique Local Unicast. Jedná se o určitou obdobu IPv4 adres pro privátní sítě (viz RFC 1918), tj. tyto adresy nelze použít ve veřejných sítích jako je Internet, avšak síťový část je generována tak, aby výsledná adresa byla unikátní. To dovoluje bez problémů vytvářet i velmi velké sítě.

Hostitelská část má nejčastěji délky 64 bitů a typicky zajišťuje unikátnost celé IPv6 adresy. Může být odvozena např. od MAC adresy daného rozhraní jednoduchou transformací (algoritmus IPv6 EUI-64). Takto vytvořená adresa umožňuje identifikaci daného uzlu i při jeho migraci, což někdy vadí, neboť uživatel může být sledován. Řešením se nazývá Privacy Extensions a je popsáno v RFC 4941. Jeho podstata spočívá v náhodném generování hostitelské části IPv6 adresy a její pravidelné změně.

Problematika IPv6 adres je daleko rozsáhlejší a složitější, například pochopení činnosti multicastingu není zcela triviální, viz již zmíněná literatura [3].

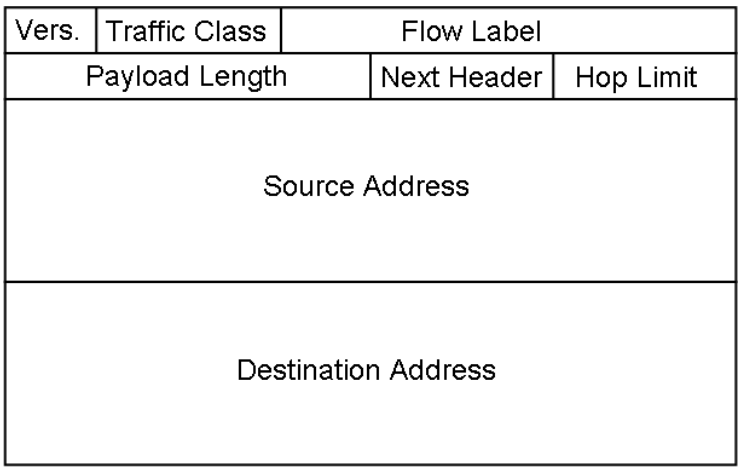
V praxi je třeba počítat s tím, že každý IPv6 uzel (resp. rozhraní) bude mít vždy více adres. Kromě globální unicastové adresy to bude i unikátní místní linková adresa (Link Local Unicast), multicastová adresa a dále pak adresy umožňující koexistenci mezi světy IPv4 a IPv6 (viz kapitola 5).

## 3. Formát IPv6 paketu

Formát IPv6 paketu, konkrétněji jeho záhlaví, je oproti svému předchůdci co do počtu polí a manipulace s nimi zjednodušen, ovšem jeho velikost se díky delší adrese zvětšila. Dále byla pozměněna koncepce zpracování tohoto záhlaví, které se nyní skládá ze základního záhlaví a rozšiřujících záhlaví (toto uspořádání sice bylo možné i v IPv4, avšak využívalo se málo).

- Základní záhlaví IPv6 paketu má tato pole:
- Version (verze, 4 bity; obsahuje hodnotu 6),
- Traffic Class (třída provozu, 8 bitů; umožňuje označit požadavek na prioritní zpracování),

- Flow Label (označení toku, 20 bitů; tokem se rozumí související pakety, například náležící do téhož TCP spojení – ty pak sdílí stejné označení toku),
- Payload Lenght (délka datové části; 16 bitů),
- Next Header (identifikace typu následujícího rozšiřujícího záhlaví; 8 bitů),
- Hop Limit (životnost paketu - každý průchozí směrovač toto pole dekrementuje a při dosažení nuly paket zahodí; 8 bitů),
- Source Address (zdrojová IPv6 adresa; 128 bitů),
- Destination Address (cílová IPv6 adresa; 128 bitů).




*Obr. 4 Základní záhlaví IPv6 paketu (dle [2])*

Základní IPv6 záhlaví se tedy skládá z 8 polí a má celkovou délku 40 oktetů (záhlaví IPv4 má 13 polí a délku 20 oktetů).

K některým dalším změnám: u IPv6 se oproti IPv4 nevyskytuje kontrolní součet záhlaví, jehož ověření a výpočet nové hodnoty po dekrementaci pole doby života paketu jsou výpočetně náročné operace, které zejména ve vysokorychlostních sítích nelze zanedbat. Chyby v současných sítích jsou jednak velmi vzácné, jednak bývají odhaleny již na 2. vrstvě.

Nově je definována maximální délka IPv6 paketu. Standardní hodnota činí stejně jako u IPv4 64 KiB, avšak v případě potřeby lze využít i tzv. jumbogramy o délce až 4 GiB. Použití jumbogramů je v praxi omezené. Sice potenciálně zrychlují přenosy, avšak je třeba, aby i linková vrstva podporovala náležité dlouhé rámce a dále se vyžaduje modifikovaná implementace TCP a UDP protokolů, neboť maximální velikost jejich segmentů je 64 KiB.

## 4. Zpracování IPv6 paketu

Zpracováním IPv6 paketu se rozumí manipulace s paketem během jeho dopravy sítí a to ve směrovačích. U IPv4 paketu směrovač pouze zjistil cílovou adresu, porovnal ji se směrovací tabulkou a pokud nalezl cestu, paket poslal dále, v opačném případě jej zahodil. Později ještě přibyla možnost přednostně vybavovat označené pakety, typicky nesoucí hlasová či obrazová data. U protokolu IPv6 bylo třeba vzhledem odlišnému přístupu k vyhodnocování paketu během jeho dopravy zvolit složitější řešení. To spočívá v zavedení rozšiřujících záhlaví, která mohou být zřetězena. V takovém případě je součástí každého záhlaví informace o typu následujícího záhlaví a o vlastní délce, poslední záhlaví pak má jako typ uvedenu hodnotu 59 (No Next Header).

| |
|---|
| 1. Základní záhlaví IPv6 |
| 2. Volby pro všechny |
| 3. Volby pro cíl (pro první cílovou adresu) |
| 4. Směrování |
| 5. Fragmentace |
| 6. Autentizace |
| 7. šifrování obsahu |

*Obr. 4 Striktně doporučené pořadí rozšiřujících záhlaví IPv6 paketu*

Uvedené pořadí však nemusí být záměrně dodrženo a může sloužit k realizaci útoku, viz kapitola 6. Následující obrázky vycházejí z [2] a ukazují vybrané příklady použití rozšiřujících záhlaví.

| | |
|---|---|
| IPv6 Header<br>Next Header = TCP | TCP Header + data |

*Obr. 5 IPv6 paket nese pouze TCP segment*

| | | |
|---|---|---|
| IPv6 Header<br>Next Hdr = Routing | Routing Header<br>Next Header = TCP | TCP Header + data |

*Obr. 6 IPv6 paket nese požadavek na směrování a TCP segment*

| | | | |
|---|---|---|---|
| IPv6 Header<br>Next Hdr = Routing | Routing Header<br>Next Hdr = Fragm | Fragment Header<br>Next Header = TCP | fragment of TCP<br>Header + data |

*Obr. 7 IPv6 paket nese požadavek na směrování, informaci o fragmentaci a TCP segment*

Protokol IPv6 podporuje fragmentaci, tj. dělení paketů na menší. Lze ji však provádět pouze u odesilatele, nikoli kdykoliv po cestě jako je tomu u IPv4. Je-li odesílaný IPv6 paket pro některý úsek cesty příliš dlouhý, je příslušným směrovačem zahozen a původnímu odesilateli se pošle relevantní informace, takže tento má možnost paket rozdělit na menší části a ty poslat znovu. Uvedená informace se odesílá protokolem ICMPv6, jehož plná funkčnost je v prostředí IPv6 nutností. Nelze jej tedy preventivně blokovat, jak se často dělává u protokolu ICMP v prostředí IPv4.

# 5. Přechod na protokol IPv6

## *5.1. Všeobecné úvahy o přechodu na protokol IPv6*

Především je třeba si uvědomit, že protokol IPv6 není zpětně kompatibilní se svým předchůdcem IPv4. To přináší komplikace pro administrátory a také zvýšené náklady, což zajímá vedoucí pracovníky. Proto ze strany poskytovatelů připojení do Internetu není znát přílišná snaha přejít na IPv6, ten je tudíž málo rozšířen a tvůrci obsahu proto nemají důvod nabízet svá díla prostřednictvím něj, takže vzniká začarovaný kruh. Všeobecně lze očekávat, že přechod na IPv6 bude velmi dlouhodobá záležitost, snad až desetiletí. Svědčí o tom

okolnost, že tomuto přechodu bylo věnováno několik desítek standardů RFC a některá dlouhodobě prosazovaná řešení byla překvapivě opuštěna. Jaké jsou technické možnosti řešení problému přechodu na IPv6? V úvahu připadá:

a) setrvat na IPv4 a nechat událostem volný průběh,
b) nasadit výhradně IPv6,
c) použít tunelování IPv6 prostřednictvím IPv4 sítí nebo překlad adres a protokolů,
d) implementovat současnou podporu IPv4 a IPv6 (Dual stack).

**Ad a) Setrvat na IPv4 a nechat událostem volný průběh**

Toto řešení znamená ponechat i nadále v páteřních sítích výhradně protokol IPv4. Klienti by mohli využívat IPv6 prostřednictvím automatických tunelů takto:

1) pomocí automatické konfigurace (Windows, Unix),
2) prostřednictvím lokálních 6to4 směrovače.

Tím se sice řeší základní problémy instituce, avšak určité aplikace mohou vyžadovat služby dostupné jen protokolem IPv6. Vyvstává i otázka správy, někteří klienti (například Windows Vista) budou moci používat tunelované IPv6 bez filtrování, správy, monitorování atd.

**Ad b) Nasadit výhradně IPv6**

Tato strategie předpokládá bezvýhradní přechod na výlučné používání protokolu IPv6. Znamenalo by to potřebu kompletní výměny všech aktivních prvků síťové infrastruktury, případně aktualizace jejich operačních systémů či firmware. Toto by bylo problémem u starších, nicméně uživatelům dosud plně vyhovujících zařízení jako jsou koncové přepínače. Ještě horší situace by byla malých účelových síťových zařízení, jako jsou tiskové servery či sdílené tiskárny, přístupové body bezdrátových sítí, IP kamery, různá čidla atd. Výrobci takovýchto zařízení se zpravidla ke svým starším produktům nehlásí. Další oblastí jsou aplikační programy, které mohou obsahovat knihovny a moduly podporujícími pouze IPv4.

Bez komunikace s vnějším IPv4 světem by však nebylo možné existovat, tudíž by byl nutný překlad adres (NAT-PT, proxyWeb, apod.).

**Ad c) Tunelování nebo překlad**

V úvahu připadá několik metod realizace, většinou dobře popsaných v literatuře. Pro názornost lze uvést hlavní představitele:

1) Pevně konfigurované tunely (propojení IPv6 ostrůvků tunely přes IPv4 síť)
2) RFC3053 - Tunnel Broker (www.freenet6.net)
3) RFC3056 - 6to4 (doporučeno, lze použít pro uzel i celou síť, vyžaduje veřejnou IPv4 adresu, tunel IPv4 protokolem 41, adresa 2002:IP:V4::/48)
4) RFC5214 - ISATAP (Microsoft, obdobné, pouze pro uzel, adresa prefix::5EFE:IP:V4)
5) RFC4380 - Teredo (tunelování přes NAT v UDP paketech, vyžaduje server)
6) Překlad IPv6/IPv4 (SIIT, NAT-PT, TRT+DNS-ALG)

**Ad d) Současná podpora IPv4 a IPv6**

V tomto případě lze zvolit mezi dvěma základními řešeními:

1) oddělené nezávislé sítě (broadcastové domény),
    a) samostatné porty VLAN nebo protokol VLAN,
    b) nativní (netagovaná) VLAN IPv4, tagovaná VLAN IPv6,
    c) topologie VLAN pro IPv4 se může lišit od topologie pro IPv6,
    d) problematická správa, údržba;

2) paralelní (překryvná) topologie,
    a) VLAN bude podsítí pro IPv4 i IPv6,
        - EthertypeIPv4 = 0800
        - EthertypeIPv6 = 86DD
    b) Ve VLAN budou přítomna dvě rozhraní směrovače, IPv4 a IPv6 (fyzicky nemusí být na stejném HW),
    c) většina uzlů bude mít v dané VLAN obě adresy.

K převodu IPv6 adresy na MAC adresu slouží protokol ICMP6 (funkce Neighbor Discovery), ARP známý z IPv4 se IPv6 nevyskytuje.

### *5.2. Možný scénář přechodu na IPv6*

Zatím poslední souhrnný scénář celosvětového přechodu na IPv6 přinesl velmi stručný dokument RFC 5211, An Internet Transition Plan, vydaný v červenci 2008 [5]. Přepokládá tři fáze tohoto přechodu:

- přípravná (do 12/2009),
- vlastní přechod (do 12/2011),
- popřechodová (od 1/2012).

Přípravná fáze byla významná zejména pro poskytovatele připojení do Internetu. V jejím rámci měli začít poskytovat nějakou formu IPv6 konektivity organizacím a tyto měly mít své hlavní servery dostupné prostřednictvím IPv6. Bylo již možné poskytnout i IPv6 konektivitu koncovým uživatelům.

Fáze vlastního přechodu předpokládá, že poskytovatelé musí začít poskytovat nějakou formu IPv6 konektivity organizacím, přičemž je preferována její nativní verze, v krajním případě pak pomocí přechodových mechanismů, tj. tunelování. Organizace již musí mít veřejné servery dostupné pomocí rutinně fungujícího IPv6 a měly by poskytovat svým uživatelům IPv6 konektivitu včetně podpůrných služeb (DNS, DHCP).

V popřechodové fázi by nemělo existovat žádné omezení pro nové uživatele, kteří se budou připojovat pouze protokolem IPv6. Poskytovatelé tudíž budou muset dát uživatelům k dispozici IPv6 konektivitu, která by měla být nativní. Organizace budou muset mít IPv6 konektivitu pro své veřejné servery a IPv6 služby poskytovat jako rutinní. Organizace by dále měly poskytovat IPv6 konektivitu uživatelům a to včetně interních služeb (DNS, DHCP). Poskytovatelé budou moci stále nabízet IPv4 konektivitu a organizace ji mohou používat.

Je třeba konstatovat, že uvedený scénář má, jak se dalo očekávat, značný skluz, ovšem existují výjimky - například vícekrát zmíněný CESNET, z.s.p.o.:

- 1999 – experimentální provoz v síti 6bone, testy implementací,
- 2001 – přidělený provozní prefix 2001:718:: /35, později /32 od RIPE,
- 2002 – zapojení se do evropského projektu 6net,
- 2003 – nativní konektivita do zahraničí a nativní peering do CZ.NIXu,
- 2003 – nativní IPv6 páteř (MPLS), dual stack, DNS, monitoring,
- ...
- 2011 – rutinní IPv6 provoz, záleží jen na uživatelích.

## 6. Bezpečnost IPv6

Je třeba konstatovat, že IPv6 nemá oproti IPv4 žádná skutečně zásadní bezpečnostní vylepšení a díky své relativní nedospělosti přináší obecně nová úskalí.

Povinnou součástí implementace IPv6 je sice podpora protokolu IPSec, který mj. zajišťuje identifikaci, autentizaci, utajení a integritu přenášených dat, nicméně IPSec je k dispozici i pro IPv4. IPSec však umožní hojné využívání zabezpečených přenosů dat mezi koncovými počítači, díky tomu nebude možno zkoumat obsah přenášených datagramů a tudíž firewally či detektory průniku v dnešní podobě nebude možné efektivně nasadit (paranoidní administrátoři raději provoz IPSec úplně blokují). Předpokládá se, že pro prostředí IPv6 bude vytvořen bezpečnostní model lišící se od současného, který umisťuje ochranu sítě typicky na její obvod, kdy vstupní body představují firewally či směrovače (často s funkcí NAT) a tam jsou prověřována procházející data.

V budoucnosti se zřejmě péče o bezpečnost více přesune do koncových zařízení, ovšem za účasti centrální správy bezpečnostních politik včetně distribuci. To na jedné straně znamená alespoň částečný návrat k původní transparentnosti IP sítí (a tudíž k větší svobodě pro experimenty a nová řešení), na druhé ovšem zvyšuje bezpečnostní rizika.

Nebezpečné jsou útoky DoS či DDoS, které lze v prostředí IPv6 potenciálně realizovat řadou postupů: pomocí směrovacích záhlaví, skupinově adresovaných ICMPv6 zpráv či v ohlášení směrovače pro automatickou konfiguraci (útočník může ohlásit nulovou životnost pro adresní prefix, který síť používá) aj. Útok obdobný TCP SYN lze realizovat i vůči IPSec, oběť lze zahltit množstvím nekorektně upravených paketů, jejichž zpracování ji značně zatíží.

Rovněž systémy detekce průniku budou muset více spoléhat na vyhledávání statistických anomálií, případně jiné nepřímé metody, neboť dnes často užívané vyhledávání signatur nebude vzhledem k IPSec použitelné

Prostor pro zneužití otevírá sama koncepce rozšiřujících záhlaví. Současné filtrační firewally k posouzení přípustnosti paketu primárně využívají informaci o TCP či UDP portech. Bohužel tato informace se v IPv6 paketu nalézá až na konci řetězu rozšiřujících záhlaví, kterými musí firewall nejen projít, ale analyzovat je. Může se stát, že některé z těchto záhlaví nezná, pak může paket zahodit nebo propustit. Zahození může narušit činnost některého ze zcela nově definovaných mechanismů, propuštění by zase mohlo ohrozit bezpečnosti.

Jiné úskalí představuje fragmentace. Díky zřetězování může být záhlaví transportní vrstvy odsunuto až do dalšího fragmentu, což vyžaduje nově řešený stavový firewall.

Možný předmět zájmu útočníků představují také tunely, neboť jejich prostřednictvím lze pronikat ochrannými mechanismy. Proto je třeba důsledně testovat procházející datagramy na obou koncích. Horší situace je u tunelů automaticky navazovaných (například 6to4 či Teredo), jejichž konce vznikají dynamicky, a jsou tudíž podstatně hůře kontrolovatelné.

## 7. Závěr

Protokol IPv6 představuje perspektivní řešení. Jeho používání se v posledních letech celosvětově intenzivně zvyšuje, což s sebou přinese nová bezpečnostní rizika. Je třeba mít také na mysli, že implementace IPv6 bude kromě nákladů spojených s někdy nutnou inovací aktivních prvků sítí znamenat i značnou zátěž pro administrátory, neboť tato protokolová sada je po stránce důsledné konfigurace mnohem složitější záležitostí nežli její předchůdce.

## Literatura

[1] DEERING, Stephen; HINDEN, Robert. Internet Protocol, Version 6 (IPv6). The Internet Engineering Task Force [online]. 1995, RFC 1883, [cit. 2011-09-19]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc1883.txt>.

[2] DEERING, Stephen; HINDEN, Robert. Internet Protocol, Version 6 (IPv6). The Internet Engineering Task Force [online]. 1998, RFC 2460, [cit. 2011-09-19]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc2460.txt>.

[3] PODERMAŃSKI, Tomáš. Lupa.cz [online]. 2011 [cit. 2011-09-19]. IPv6 Mýty a skutečnost. Dostupné z WWW: <http://www.lupa.cz/autori/tpoder/>.

[4] SATRAPA, Pavel. IPv6 : Internetový protokol IPv6 [online]. 2. dopl. vyd. Praha : CZ.NIC,z.s.p.o., 2008 [cit. 2011-09-19]. Dostupné z WWW: <knihy.nic.cz/files/nic/edice/pavel_satrapa_ipv6_2008.pdf>. ISBN 978-80-904248-0-7.

[5] CURRAN, John. An Internet Transition Plan. The Internet Engineering Task Force [online]. 2008, RFC 5211, [cit. 2011-09-19]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc5211.txt>