**Computerworld, 11.2.**
**2011**

# Vlastnosti protokolu IPv6 (II)

**Jelikož je seznam vlastností IPv6 protokolu vcelku hojný a do minulého dílu se nám všechny nevešly, budeme se vlastnostem IPv6 věnovat i v tomto díle IPv6 seriálu.**

## Absence překladu adres (NAT)

Díky většímu adresnímu prostoru (128 bitů oproti 32 bitům), mohou mít všechna zařízení v IPv6 sítí svou veřejnou adresu, která zajišťuje globální konektivitu mezi koncovými stanicemi a proto není důvod používat NAT. To může vyvolat obavy nad bezpečností, ale většina firewallů na osobních stanicích podporuje IPv6. A mnohdy mají i výchozí nastavení s pravidlem blokace nevyžádaných příchozích IPv6 spojení a tedy i potencionálních útoků z Internetu. Více o ochraně lokální IPv6 sítě si lze přečíst v RFC dokumentu s číslem 4864 na adrese http://tools.ietf.org/html/rfc4864.

## ARP je u IPv6 nahrazen ICMPv6 ND

Pro objevování sousedů (Neighbor Discovery) se v IPv6 využívá několika ICMPv6 zpráv. Pokud je potřeba k IPv6 adrese zjistit fyzickou adresu (MAC[1] adresu), pošle tazatel ICMP zprávu typu 135: *Výzva sousedovi* (Neighbor Solicitation) na specifickou skupinovou adresu pro vyzývaný uzel (Solicited-Node), kterou si blíže popíšeme v dalším článku seriálu. Pokud na lokální sítí existuje stanice s danou IPv6 adresou, odpoví na dotaz ICMP zprávou typu 136: *Ohlášení souseda* (Neighbor Advertisement), ve které uvede svou fyzickou MAC adresu síťového rozhraní.

## Detekce duplicitních adres (DAD)

IPv6 zajišťuje detekci duplicitní adresy, nemůže tedy nastat situace, kdyby v lokální sítí existovalo více stejných adres. Při požadavku na přiřazení nové adresy k rozhraní operační systém automaticky pošle ICMP zprávu *Výzva sousedovi* pro tuto adresu, pokud na výzvu přijde odpověď ve formě ICMP zprávy *Ohlášení souseda*, znamená to, že zvolenou adresu již používá jiná stanice a systém ji odmítne. Adresa se sice u rozhraní zobrazí, ale s označením *Tentative dadfailed (Prozatímní selhání DAD)*, což signalizuje, že detekce duplicitní adresy neproběhla v pořádku a adresa se nebude používat.

## Prostředky pro „jednodušší“ správu sítě

Bezstavová automatická konfigurace (viz. minulý článek) umožňuje snadněji[2] přečíslovat celou síť, stačí na

1 MAC je identifikátor síťového zařízení, kterou jednoznačně přiděluje přímo výrobce a má velikost 6 bajtů.
2 Přečíslování sítě samozřejmě není jenom o stanicích, ale je to komplexní proces, který je pěkně popsán v RFC dokumentu s číslem 4192.

daném směrovači nastavit nový IPv6 prefix sítě a stanice se sami překonfigurují.

IPv6 nově zavádí životnost síťových údajů, jako je životnost propagovaného prefixu a tedy i automaticky vygenerované globální individuální adresy či životnost výchozího směrovače samotného. Těmito prostředky lze tedy plánovaně stanicím v sítí sdělit, kdy a které síťové údaje si mají ze svých systému odstranit.

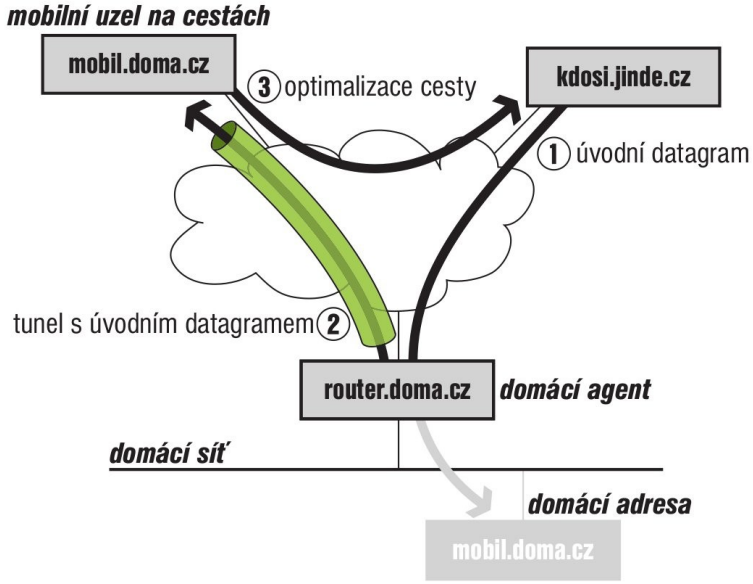
Pokud je potřeba mít v síti více směrovačů pro zajištění vysoké dostupnosti služeb, nabízí IPv6 možnost preference některého z nich prostřednictvím nastaveného příznaku *Preference směrovače* v ICMP zprávě *Ohlášení směrovače*, která se pro bezstavovou autokonfiguraci stanic používá. To spolu s výše uvedenou životností směrovače a možností měnit interval jeho ohlašování poskytuje řešení, které se muselo v IPv4 zajišťovat prostřednictvím dodatečných technologií, jako je UCARP či VRRP.

## Vestavěné bezpečnostní mechanismy (IPsec)

Technologie IPsec, která zajišťuje autentizaci a šifrování síťové komunikace, je oproti IPv4 povinnou součástí IPv6 implementace a pro některé IPv6 vlastnosti, jako je například mobilita, i nutnou podmínkou pro jejich fungování. Popisovat IPsec je mimo rámec tohoto článku, ale hezky česky si o IPsec lze přečíst v knížce Pavla Satrapy, která je zdarma ke stažení na stránkách 'Edice CZ.NIC' http://knihy.nic.cz/.

## Mobilita

Protokol IPv6 byl navržen s ohledem na mobilitu. Myšlenka je taková, že pokud se bude cestovat s notebookem či jiným mobilním zařízením a přecházet mezi různými sítěmi poskytovatele internetového připojení, bude mobilní zařízení stále dosažitelné na původní (domácí) adrese, pod kterou je například vedeno v DNS. Když vezmeme v potaz, že v dnešní době mnozí poskytovatelé internetu vůbec IPv6 konektivitu nenabízí, na praktické využíti IPv6 mobility si ještě určitě chvilku počkáme.




zdroj: Satrapa, P.: IPv6, Praha, Edice CZ.NIC 2008

## Podpora jumbogramů (>64 KiB až 4GiB)

Oproti IPv4, kde je velikost paketu omezena hranicí 64KiB, umožňuje IPv6 vytvořit paket teoreticky až do velikosti 4GiB, danou velikost ovšem musí podporovat i linková technologie (MTU[3]). Užití této vlastnosti je dosti specifické, protože velikost MTU na Ethernetu je obvykle 1500 bajtů.

## Optimalizace pro směrování

IPv6 hlavička má fixní velikost 40 bajtů a neobsahuje kontrolní součet hlavičky, který by se jinak musel přepočítávat po každém průchodu směrovačem (z důvodu snížení TTL[4]), jako tomu je u IPv4. Dalším podstatným rozdílem oproti IPv4 je, že IPv6 směrovače už neprovádí fragmentaci.

## IP fragmentace

Fragmentaci u IPv6 zajišťuje pouze odesílatel a na jeho bedrech leží i zjištění MTU cesty. Pokud směrovač obdrží požadavek k poslání paketu na linku s nedostatečným MTU, paket zahodí a pošle odesílateli ICMP

3 MTU (Maximum Transmission Unit) hodnota určuje maximální velikost rámce, které je po médiu možno přenést.

4 TTL (Time to Live), je součástí IPv4 hlavičky a její hodnota se snižuje každým průchodem směrovače v sítí, pokud hodnota klesne na nulu, musí být datagram zahozen. TTL tedy slouží jako ochrana proti zahlcení sítě v případě, kdyby došlo k zacyklení z důvodu chybného směrovaní. V IPv6 je tato položka přejmenována na 'Hop Limit', protože se v dnešní době hodnota stejně snižuje pouze o jedničku a nepředpokládá se, že by datagram strávil na směrovači více než jednu sekundu.

zprávu 'příliš velký paket' s připojenou informací o MTU, které je schopen přenést. Odesílatel pokus opakuje s menší velikostí paketu, dokud se paket nedostane k cíli, přičemž dolní hranice pro MTU linky je u IPv6 stanovena na 1280 Bytů. To znamená, že jednodušší implementace IPv6 mohou rovnou poslat paket o velikosti 1280 Bytů a s procesem fragmentace se vůbec nezabývat.

V dalším díle seriálu se budeme podrobně věnovat různým typům IPv6 adres, vysvětlíme si jejich formát zápis, k čemu se používají a kde se s nimi můžeme setkat.

Autoři:
Emanuel Petr a Ondřej Surý pracují v Laboratořích CZ.NIC, výzkumném a vývojovém centru správce české národní domény.