Přechodové mechanismy k IPv6 (1)

David Rohleder, ÚVT MU

1 Konec IPv4 se kvapem blíží

Dnešního dne nám zbývá pouze kolem 4% adresního prostoru IPv4 a den, kdy dojde k vyčerpání adresního prostoru se nezadržitelně přibližuje. V době, kdy vychází tento článek (únor 2011), jsou již segmenty adres přidělované centrálním orgánem IANA (Internet Assigned Numbers Authority `http://www.iana.org/`) jednotlivým regionálním RIR (Regional Internet Registry) úplně vyčerpány. Po tomto termínu zbývají volné IPv4 adresy jenom u pěti RIR (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC) a konečný termín vyčerpání všech volných IPv4 adres se očekává někdy na konci roku 2011. Postupné vyčerpávání adresního prostoru můžete vidět např. na `http://inetcore.com/project/ipv4ec/index_en.html`.

Na první pohled by se mohlo zdát, že nás, kteří už máme IPv4 adresy přidělené, se tento problém až tak netýká. IPv4 adresu nám nikdo nesebere a tak si můžeme pohodlně komunikovat po stávajícím Internetu bez sebemenšího omezení. Nicméně časem vzniknou informační zdroje, které budou kvůli nemožnosti získat IPv4 adresu, přístupné pouze po IPv6.

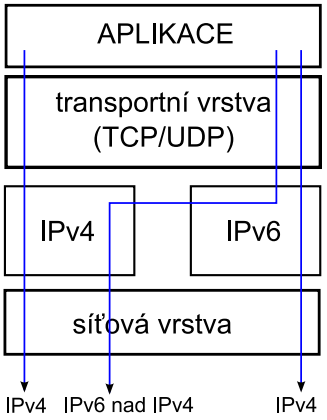
Je tedy na čase se podívat jakým způsobem se vlastně na takový IPv6 Internet můžeme dostat.

Pro začátek si můžeme na adrese `http://ip6.me/` ověřit, jestli je nám IPv6 dostupné a jestli se jedná o preferovaný způsob připojení.

V současnosti je většina operačních systémů připravena k použití IPv6. Překvapivě asi nejkompletnější implementací disponují operační systémy firmy Microsoft. Sami si tedy na svých Windows můžete zadat příkaz `ipconfig /all` a možná budete překvapeni, kolika IPv6 adresami je váš počítač vybaven.

2 Dual stack

Asi nejjednodušší možnost připojení k IPv6 Internetu je ta, kdy IPv6 pracuje v naší síti nativně. Počítač pak používá obě sítě IPv4 i IPv6 rovnocenně, většinou s tím, že v případě možnosti připojení přes IPv6 dává přednost připojení právě



Obrázek 1: TCP/IPv4+IPv6

přes tuto novou technologii. Protože se jedná pouze o jednu vnitřní vrstvu v síťovém modelu TCP/IP, tak aplikace, které se nijak o síťové adresy nezajímají, nemusejí vůbec vědět, po které z těchto sítí vlastně běhají jejich data a jsou tedy na zvolené síti nezávislé.

V případě, že naše síť není vybavena nativní podporou IPv6 nastupují mechanismy, které mají zpřístupnit IPv6 i v těchto sítích.

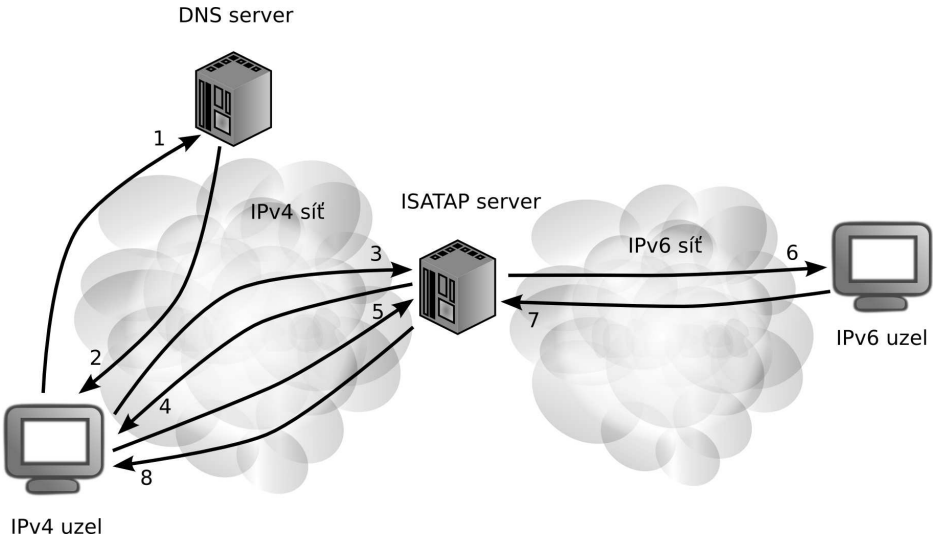
3 Tunelování IPv6 provozu přes IPv4 síť

Mezi koncovými body IPv6 a IPv4 není možné provést přímé spojení kvůli rozdílné adresaci obou protokolů (IPv4 nebude rozumět IPv6 adresám). Proto musí každý koncový uzel IPv4, který chce komunikovat s IPv6 uzlem získat i IPv6 adresu. Ve chvíli, kdy získá tuto adresu, může vytvořit IPv6 datagram, který je následně zabalen do IPv4 datagramu (viz. obr.), který je přenesen IPv4 sítí k uzlu, který se postará o odstranění IPv4 hlavičky a další cestu datagramu, tentokrát IPv6 sítí.

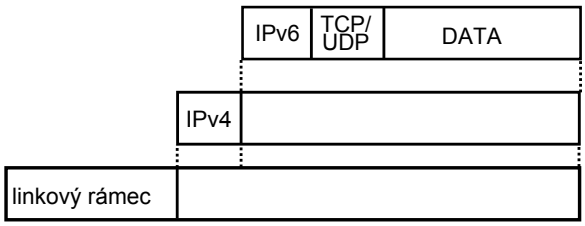
Mechanismů, které umožňují toto zabalení je několik, lišících se podle způsobů a mechanismů vytvoření a možností, které poskytují. V následujících částech si popíšeme metody automatického tunelování prostřednictvím ISATAP, 6to4 a Teredo protokolů.

4 ISATAP

ISATAP (Intra-site Automatic Tunnel Adressing Protocol) mechanismus (RFC 5124) se skládá celkem ze tří částí. Je to počítač připojený pouze



Obrázek 3: ISATAP komunikace



Obrázek 2: IPv6 datagram zabalený v IPv4 datagramu

do IPv4 sítě, počítač připojený do IPv6 sítě a ISATAP serveru, který je připojen do obou těchto sítí. ISATAP server hraje hlavní roli v přidělení globální IPv6 adresy IPv4 uzlu a přeposílá komunikaci mezi IPv4 a IPv6 sítí.

Jak už jsme zmínili v předcházející části, základní věc, kterou musí každý mechanismus tunelování IPv6 provozu udělat, je přidělení IPv6 adresy.

ISATAP používá jednoduchého odvození spodních 64bitů IPv6 adresy z přidělené IPv4 adresy. V případě, že je použit jeden z privátních IPv4 adresních rozsahů (RFC 1918), IPv6 adresa je vytvořena jako `::0:5EFE:w.x.y.z`, kde `w.x.y.z` jsou části privátní IPv4 adresy. V případě, kdy počítač používá veřejně dostupnou IPv4 adresu, je IPv6 adresa vytvořena jako `::200:5EFE:w.x.y.z`. Těchto spodních 64 bitů může být zkombinováno s libovolným 64 bitovým prefixem včetně link-local prefixů (`FE80::/64`), ULA nebo globálním prefixem.

ISATAP adresy tedy mohou být např. `FE80::0:5EFE:192.168.1.2` (převedeno do plně IPv6 kompatibilní notace `FE80::0:5EFE:C0A8:102`) nebo `2001:718:801:101:200:5EFE:147.251.4.33` (`2001:718:801:101:200:5EFE:93FB:421`).

Máme tedy vytvořeno spodních 64 bitů IPv6 adresy bez pomoci od ISATAP serveru. Protože každé rozhraní v IPv6 má tzv. link-local IPv6 adresu, tak IPv4 uzel dostane také jednu (výše zmíněnou `FE80::/64`). Máme tedy k dispozici IPv6 adresu, která se používá v místní, většinou ethernetové, síti (u ISATAP to má ten vedlejší efekt, že IPv4 síť je používána jako linková vrstva, tj. i s lokální IPv6 adresou je možné komunikovat s počítači v celé IPv4 síti nejen na lokální síti, jak by tomu bylo u klasického IPv6).

Přidělení globálního IPv6 prefixu pro koncový uzel probíhá téměř shodně se standardním přidělením IPv6 prefixu v IPv6 síti pomocí *router solicitation* a *router advertisement* zpráv. Protože ISATAP neklade žádné nároky na IPv4 síť z pohledu podpory multicastu, jedná se o zprávy unicastové. Uzel A (IPv4 uzel) vytvoří router solicitation zprávu se zdrojovou IPv6 link-local adresou a cílovou IPv6 adresou odpovídající link-local IPv6 adrese ISATAP serveru (IPv4 adresa ISATAP serveru je mechanismem, který si objasníme později, už známa a link-local IPv6 adresu

je tedy možné jednoduše vytvořit pomocí prefixu *FE80::* a spodních 64 bitů, které se odvodí z IPv4 adresy), tento datagram zabalí do IPv4 datagramu se zdrojovou IPv4 adresou uzlu A a cílovou IPv4 adresou ISATAP serveru. ISATAP server odpoví stejným způsobem zprávou router advertisement s informacemi o přiděleném prefixu. V této chvíli je uzel A vybaven i globální IPv6 adresou a může začít pomocí této adresy komunikovat s IPv6 sítí.

Uzel A nyní vybavený jak IPv4, tak globální IPv6 adresou navazuje komunikaci s IPv6 uzlem tak, že vytvoří IPv6 datagram s odpovídající zdrojovou (adresa uzlu A) a cílovou IPv6 adresou (adresa vzdáleného uzlu), tento datagram vloží do IPv4 datagramu s protokolovým číslem 41, zdrojovou IPv4 adresou uzlu A a cílovou IPv4 adresou ISATAP serveru a prostřednictvím IPv4 sítě jej pošle k ISATAP serveru. ISATAP server tento datagram přijme, odstraní IPv4 hlavičky a podle svých směrovacích tabulek pošle IPv6 datagram do IPv6 sítě. Cílový IPv6 uzel B datagram přijme a odpoví na něj. Odpověď z uzlu B dorazí na ISATAP server (protože ISATAP server je také směrovačem, který směruje IPv6 adresy uzlu A do IPv6 sítě). Zde proběhne zabalení do IPv4 datagramu jednoduchým převodem z IPv6 adresy cíle (uzlu A) do IPv4 adresy uzlu A – stačí jen vzít posledních 32 bitů adresy a ty přímo vložit do IPv4 hlavičky. Jako zdrojová IPv4 adresa pak poslouží IPv4 adresa ISATAP serveru. Tento datagram je přenesen IPv4 sítí ke cíli – uzlu A, který tak dostal odpověď na svůj vyslaný datagram. Komunikace je tedy z obou stran průchozí a může bez potíží standardně pokračovat.

Na tomto místě nám zůstala jediná nevyřešená záhada a to je, jakým způsobem se uzel A dozví adresu ISATAP serveru. Specifikace protokolu připouští několik možností, nejběžnější je použití DNS, kdy se uzel A zeptá na IPv4 adresu isatap.domainname, např. `isatap.ics.muni.cz`. Pokud DNS server odpoví IPv4 adresou, uzel A se pokusí sestavit spojení na ISATAP server `isatap.ics.muni.cz`. Další možností je udání této adresy prostřednictvím rozšíření protokolu DHCPv4. Windows používají ještě několik dalších metod, využívají službu LLMNR (Local Multicast Name Resolution), hledají NetBIOS jméno „ISATAP <00>“ v NetBIOS cache, pokoušejí se dotázat nakonfigurovaného WINS serveru (Windows Internet Name Service) nebo posílají po místní síti NetBIOS broadcasty. Poslední možností pak zůstává manuální nastavení IPv4 adresy ISATAP serveru (nicméně tato metoda ztrácí kouzlo automatické konfigurace).

Jedna ze zajímavostí tohoto mechanismu je ta, že umožňuje komunikaci prostřednictvím IPv6 adres i uzlům, které leží oba v IPv4-only síti a bez nutnosti využití ISATAP serveru. Stačí pouze komunikovat prostřednictvím automaticky přiděleného link-local prefixu `FE80::`. I na IPv4 síti tedy můžete zkusit IPv6 komunikaci (příklad pro Windows) – ping `FE80::200:5EFE:w.x.y.z%I`, kde `w.x.y.z` je IPv4 adresa cíle a `I` číslo rozhraní, přes které chcete ping poslat (z pohledu IPv6 je toto adresa s linkovou platností).

Popis ISATAP komunikace:

1. IPv4 uzel zjišťuje adresu ISATAP serveru dotazem DNS serveru na jméno `isatap.domainname`
2. DNS server odpovídá IPv4 adresou ISATAP serveru
3. IPv4 uzel požádá o IPv6 prefix pomocí router solicitation zprávy
4. ISATAP server posílá prefix pomocí router advertisement zprávy
5. IPv4 uzel posílá IPv6 datagram zabalený v IPv4 datagramu IPv6 uzlu prostřednictvím ISATAP serveru
6. ISATAP server vybalí IPv6 datagram z IPv4 datagramu a posílá jej IPv6 sítí
7. IPv6 uzel odpovídá
8. ISATAP server zabalí odpověď do IPv4 datagramu a posílá IPv4 uzlu
9. IPv4 uzel dostal IPv6 datagram zabalený v IPv4 datagramu
10. opakují se kroky 5—9

V příštím díle se podíváme na mechanismy 6to4 a Teredo. □