Úvod do IPv6

David Antoš, ÚVT MU

Třebaže se mezi lidmi od sítí o protokolu IPv6 (Internet Protocol version 6) hovoří již docela dlouho, jeho rozšíření mezi běžné uživatele je stále značně neobvyklé. Zakořenila představa, že IPv6 má za cíl pouze kompenzovat nedostatek adres protokolu IPv4. A protože typický uživatel univerzitní sítě se s nedostatkem adres obvykle nepotýká, má obvykle pocit, že se o tento protokol není třeba zajímat. Nicméně i MU musí řešit nedostatek adres, a je třeba se na postupný přechod na nový protokol připravit.

Kromě zjevných výhod většího adresního prostoru ovšem IPv6 přináší i další vlastnosti, jako přímou adresovatelnost (bez překladu adres – NATu [4], čímž odstraňuje problémy, které je nutno u některých aplikací složitě obcházet, např. jako v [2]), možnost stanovit dosah platnosti adres, automatickou konfiguraci adres včetně mechanismů pro zabránění duplicitních adres na jedné síti, zabezpečovací mechanismy, podporu mobilních klientů a další.

Podpora IPv6 v operačních systémech je už dostatečně rozšířena, protokol sám je vyzrálý a stabilní. Některé jeho vlastnosti, které nepřevzal z IPv4 (jako mobilita nebo zabezpečení), jsou sice stále v experimentálním stádiu vývoje, ale obecně lze říci, že cokoli šlo dělat s IPv4, jde také s IPv6. Podívejme se tedy na tento protokol z hlediska lehce pokročilého uživatele. Povíme si, jak vypadají adresy v IPv6 a s jakými typy adres se potkáváme, jak se připojit do IPv6 světa a jaký je stav podpory tohoto protokolu v operačních systémech a aplikacích.

1 S čím by se uživatel měl potkávat

Běžný uživatel „v ideálním světě" identifikuje stroje na síti pomocí doménových jmen (např. `despil.fi.muni.cz`). Nepotřebuje vědět, na jakou IP adresu (a jakou verzi protokolu) se doménové jméno přeloží. Stačí, když všechno funguje.

Svět ovšem tak ideální není, takže i uživatel se občas potká s IP adresou. Někdy IP adresa vykoukne ve webovém prohlížeči, často je potřeba ji použít při konfiguraci systému nebo aplikací.

2 Adresy v IPv6

Připomeňme si staré dobré IP adresy ve verzi protokolu 4. Ty mají 32 bitů, které obvykle zapisujeme jako čtveřici desítkových čísel oddělených tečkami (`147.251.54.47`), za lomítkem se někdy uvádí délka prefixu sítě (třeba `/24`), za dvojtečkou port protokolů TCP nebo UDP.

Principy adresace sítí a strojů v nich zůstaly u IPv6 zachovány, jen adresa se oproti předchozí verzi zvětšila čtyřikrát, na 128 bitů.

2.1 Zapisování adres

Adresy IPv6 se zapisují jako šestnáctková čísla po čtveřicích oddělených dvojtečkami (celkem jde o 8 čtveřic šestnáctkových čísel). Nuly ve čtveřicích zleva se často vypouštějí. Je obvyklé, že se v adresách nachází dlouhé řetězce nul. Ty je možno pro stručnost nahradit dvojicí dvojteček. Toto nahrazení lze samozřejmě použít v zápisu adresy pouze jednou. Za lomítkem se může uvést desítkově délka prefixu sítě.

Například adresa `fdce:9f6a:995::47/64` by v nezkráceném zápisu vypadala `fdce:9f6a:0995:0000:0000:0000:0000:0047/64`. Volba dvojtečky jako oddělovače nebyla zrovna nejšťastnější, tento znak se také používá pro oddělení čísla portu. Aby bylo jasné, co je adresa a co port, obalí se adresa do hranatých závorek. Například naši známou adresu a port 80 bychom zapsali `[fdce:9f6a:995::47]:80`. Takto lze adresu zapsat třeba i do URL ve webovém prohlížeči (`http://[fdce:9f6a:995::47]:80`).

Prefix sítě včetně délky určil její administrátor. Velcí poskytovatelé připojení dostávají prefixy délky 48 bitů, koncové lokální sítě 64. Rozdělení adresního prostoru uvnitř organizace je určeno její vlastní politikou. V literatuře i na webu se lze setkat se starším podrobným schématem dělení adresního prostoru IPv6 (obsahoval pojmy jako Top-Level Aggregation, Site-Level Aggregation a podobně). Toto schéma se ukázalo jako přehnaně složité a bylo prohlášeno za zastaralé.

Ve speciálních případech může IPv6 adresa v sobě obsahovat IPv4 adresu. Pak se z důvodu čitelnosti setkáváme i se zápisem posledních

32 bitů IPv6 adresy způsobem obvyklým v IPv4, například `::ffff:147.251.54.47`. Takový zápis pro IPv6 adresy se často objevuje v operačních systémech, které oba typy adres vnitřně ukládají do shodných struktur.

2.2 Typy adres

Adresy rozlišujeme individuální (unicast), skupinové (multicast) a výběrové (anycast). Individuální označují jedno síťové rozhraní, skupinové skupinu (poznají se podle toho, že začínají `ff`, multicast v IPv6 je postaven na stejných principech jako v IPv4, liší se technickými detaily).

Výběrové adresy jsou poměrně obskurní, byly míněny pro použití v případech, kdy je klientovi jedno, který konkrétní stroj bude serverem pro jeho spojení, například při komunikaci s velkým webovým vyhledávačem, který má webové servery na řadě strojů. Tato situace se dnes běžně řeší pomocí překladu doménových jmen na adresu ze skupiny, a mechanismus výběrových adres k tomu nepřináší další hodnotu, je pouze „návrhově správnější".

K adrese se váže její dosah, kterým určujeme, kde je adresa platná. Přestože první návrhy protokolu IPv6 počítaly s bohatým repertoárem dosahů adres (jako podsíť nebo administrativní doména), do dnešních dnů přežily globální a linkové adresy.

Linkové adresy platí pouze v lokální síti (nesmí se tedy směrovat) a poznají se podle prefixu `fe80::`. Obvykle bývají na rozhraní konfigurovány automaticky, a pokud se používají ke komunikaci, je nezbytné specifikovat síťové rozhraní, přes které se k dané adrese dostat. Syntakticky se to dělá zápisem jména rozhraní za znak `%` na konec adresy, nicméně zdaleka ne všechny programy s tím počítají, například program `ping6` v Linuxu má místo toho parametr `-I`.

Globální adresy jsou celosvětově jednoznačné. IPv6 zcela vypouští privátní adresy, které byly v IPv4 používány v sítích za překladem adres (Network Address Translation, NAT). Globální adresy v IPv6 jsou tedy odkudkoli přímo adresovatelné, čímž se navracíme k prapůvodním myšlenkám Internetu o globální dostupnosti adresovaných strojů.

Přestože obecně zrušení mechanismu NATu považujeme za jeden z hlavních přínosů IPv6, existují situace, pro které se hodí soukromé adresy, ať už z důvodu skrytí určité sítě před vnějším světem, či pro možnost snadné změny poskytovatele připojení. Uvážíme-li, že adresy uvnitř organizace mají prefix, který organizace obdržela od toho, kdo ji připojuje, tak při změně by se i všechny vnitřní adresy změnily (což je problém, který známe samozřejmě i ze světa IPv4). Před několika lety se dokonce diskutovalo i o zavedení NATu do IPv6. Našlo se ovšem elegantnější řešení: unikátní lokální adresy. Ty slouží pro adresaci uvnitř organizace, poznají se podle prefixu `fd` (RFC hovoří o prefixu `fc::/7`, nicméně 8. bit je indikace, zda prefix je lokálně nebo globálně spravován), který je následován dvaceti náhodně vygenerovanými bity. Pakety s unikátní lokální adresou nesmí opustit síť organizace. Náhodná část prefixu navíc dává vysokou pravděpodobnost, že pokud budeme dvě takové sítě spojovat, budou mít různý prefix.

2.3 Získání IPv6 adresy

Adresy rozhraní v IPv4 se konfigurovaly ručně nebo pomocí DHCP. V IPv6 je sice ruční konfigurace možná také, ale prakticky se s ní nepočítá zejména proto, že do takto dlouhé adresy je velmi snadné zanést chybu.

Předpokládejme nyní, že se připojujeme do sítě, která je globálně připojena do IPv6 světa.

IPv6 zavádí mechanismus autokonfigurace, který umožňuje získat globální adresu každému uzlu připojenému do sítě. Autokonfigurace funguje tak, že směrovač na příslušné lokální síti oznamuje, jaký má tato síť prefix a přes který směrovač posílat svůj provoz do vnější sítě. Uzel vezme tento prefix a doplní jej na celou adresu tak, že spodní část adresy vygeneruje na základě MAC adresy síťové karty. IPv6 je tedy skutečně „plug&play".

Navíc pokaždé, než uzel nastaví nějakou adresu, musí zkontrolovat, že tuto adresu na dané síti nikdo nepoužívá. Je to sice velmi nepravděpodobné, ale každý, kdo někdy hledal duplicitní adresy na IPv4 síti, takovou automatizovanou kontrolu ocení.

Konfigurace pomocí DHCPv6 funguje téměř stejně jako pro IPv4. Pomocí DHCPv6 lze navíc stroji předat i informace o DNS serveru, serveru pro synchronizaci času, časové zóně a další. Lze také použít „bezstavové" DHCPv6, které nepřiděluje adresu, ta se získá autokonfigurací, pouze předá uzlu tyto doplňkové informace.

Správnou metodu konfigurace IPv6 adres vám sdělí správce sítě a postup najdete v dokumentaci vašeho operačního systému.

3 Připojení k IPv6 „v nepřátelských podmínkách"

Na síti, která IPv6 nepodporuje nativně, je situace s konfigurací poněkud složitější, nicméně ještě není nic ztraceno. Řada mechanismů byla vytvořena pro období, kdy obě verze protokolu budou na síti existovat současně.

3.1 Oba protokoly současně

Běžnou situací je, že jsme připojeni na síti, která umí obě verze IP, a operační systém podporuje obě verze protokolu. Pokud aplikace potřebuje zjistit IP adresu k zadanému doménovému jménu, pošle DNS dotaz a v odpovědi dostane seznam adres. Jakou verzi protokolu bude preferovat závisí na nastavení aplikace a systému, nicméně doporučené chování je vyzkoušet postupně všechny adresy.

3.2 IPv6 v sítích s převahou IPv4

Pokud chceme získat připojení do IPv6 světa ze sítě, která umí pouze IPv4, přichází do úvahy některý z mechanismů tunelů. Tunel v síti je obecně způsob zabalení dat jednoho protokolu do protokolu jiného, který je v síti podporován. Tunely mohou být vytvořeny mezi koncovými uzly, mezi uzlem a směrovačem, případně mezi směrovači. Mezi hlavní tunelovací mechanismy pro IPv6 přes IPv4 sítě patří 6to4, ISATAP a Teredo.

6to4 používá speciální adresy obsahující IPv4 adresu hraničního směrovače sítě. Vnitřní síť musí podporovat IPv6, hraniční směrovače tunelují IPv6 provoz do IPv4. Lze tak například spojit dvě sítě podporující IPv6 přes síť, která umí pouze IPv4. Uzly vnitřní sítě nevyžadují žádnou speciální konfiguraci. Nevýhodou je závislost na IPv4 adresách, navíc hraniční směrovač musí mít veřejnou IPv4 adresu.

ISATAP neboli Intra-Site Tunnel Addressing Protocol slouží pro IPv6 komunikaci uzlů na lokální síti, která nepodporuje IPv6. Musí jej podporovat uzly lokální sítě, které tunelují IPv6 do IPv4 mezi sebou. Pokud se požaduje připojení do vnějšího IPv6 světa, musí ISATAP zvládnout i hraniční směrovače. Takové připojení pak může být buď nativní, nebo lze ISATAP kombinovat například se 6to4.

Teredo používá sice poměrně neefektivní metody přeposílání dat, zato se umí dostat i přes několikanásobné NATy různých typů. Tím se liší od předchozích mechanismů, které požadovaly veřejné IPv4 adresy a obvykle se s NATy dokázaly sžít jen ve velmi omezené míře. Teredo je postaveno na síti serverů, ke kterým se klienti připojují. Pochází z dílny Microsoftu, a ač jeho dokumentace uvádí, že by se mělo nasazovat jen v situacích, kdy nelze použít nic jiného, ve Windows Vista je připraveno jako standardní tunelovací mechanismus pro IPv6.

4 IPv6 v operačních systémech

IPv6 je podporováno ve většině operačních systémů již několik let. Systémy založené na BSD patřily mezi první volně šiřitelné OS s kvalitní podporou tohoto protokolu. Linuxové distribuce již také běžně obsahují nástroje pro nastavení a správu IPv6. Implementace v Mac OS X vychází ze systému FreeBSD. Samozřejmě jednou z hlavních překážek rozšíření IPv6 mezi uživatele byla podpora v majoritních systémech Windows. Zárodky podpory se vyskytly již ve Windows NT 4.0 a Windows 2000, nicméně implementace produkční kvality začíná na Windows XP se Service Pack 1.

5 Aplikace

Podpora protokolu IPv6 v aplikacích se zlepšuje, nicméně stále není ideální. Co znamená podpora IPv6 pro aplikaci? Aplikace musí pro ukládání adres používat větší datové struktury, je třeba počítat s tím, že k jednomu doménovému jménu DNS

typicky vrátí seznam adres. Navíc i odchozí rozhraní může mít více adres, mezi kterými je třeba vybírat. Je také nezbytné zvládat načítání textové podoby adres z konfiguračních souborů. Pokud aplikace používala knihovní funkce pro manipulaci s adresami, úpravy pro IPv6 jsou obvykle poměrně snadné. Horší situace nastane u programů, které interně závisejí na tvaru IP adresy. U takových může být třeba i kompletní přeprogramování. Naštěstí je takový software v menšině.

Obecně lze říci, že servery a klienty pro běžné síťové služby zvládají IPv6 již několik let, ať už se jedná o přenos pošty (SMTP), přenos souborů (FTP), virtuální terminály (Telnet, SSH), nebo WWW.

I když některé aplikace fungují s IPv6 velmi dobře, narážíme občas na drobné nedostatky. Typicky některé programy nesnesou IPv6 adresu zapsanou v konfiguračním souboru nebo na příkazovém řádku, některé nemají rády adresy zapsané v hranatých závorkách, případně nezvládnou syntax se znakem % pro rozhraní lokální adresy. To ještě nemusí znamenat, že aplikace IPv6 nezvládne, často dostačuje používat doménová jména příslušející daným adresám. Například i Internet Explorer ve Windows XP nepodporuje přímý zápis adresy, přestože doménu na IPv6 adresu správně přeloží a komunikuje po IPv6, zcela to skrývaje před uživatelem.

6 Závěr

Prapůvodní motivací pro vznik protokolu IPv6 bylo vyčerpávání adresního prostoru IPv4. Problém akutního nedostatku IPv4 adres byl sice odsunut do pozadí masovým používáním technik překladu adres, nicméně jejich nevýhody jsou značné. Současný vývoj naznačuje, že IPv6 se v blízké budoucnosti stane běžnou součástí našeho života na síti. Přechod je postupný, nikoli bezbolestný, ale je dobré být připraven, nebo o tom alespoň vědět.

Pokud se o IPv6 chcete dozvědět víc, mezi vhodné zdroje v češtině patří dnes už nepatrně zastarávající, nicméně výborná kniha Pavla Satrapy [5], pro podrobnější základní představu poslouží web [3]. Pro správce sítí lze doporučit aktuální knihu [1].

Literatura

[1] Silvia Hagen. *IPv6 Essentials*. O'Reilly Media, Inc., 2nd edition, 2006. ISBN 0-596-10058-2.

[2] Eva Hladká, Petr Holub, and Michal Procházka. Videokonference za zdí. *Zpravodaj ÚVT*, roč. XVII, č. 5, str. 8–12, 2007. ISSN 1212-0901.

[3] `http://www.ipv6.cz`.

[4] `http://www.abclinuxu.cz/slovnik/nat`.

[5] Pavel Satrapa. *IPv6*. Neocortex, 2002. ISBN 80-8633-01-9. □