Tunelovací mechanismy

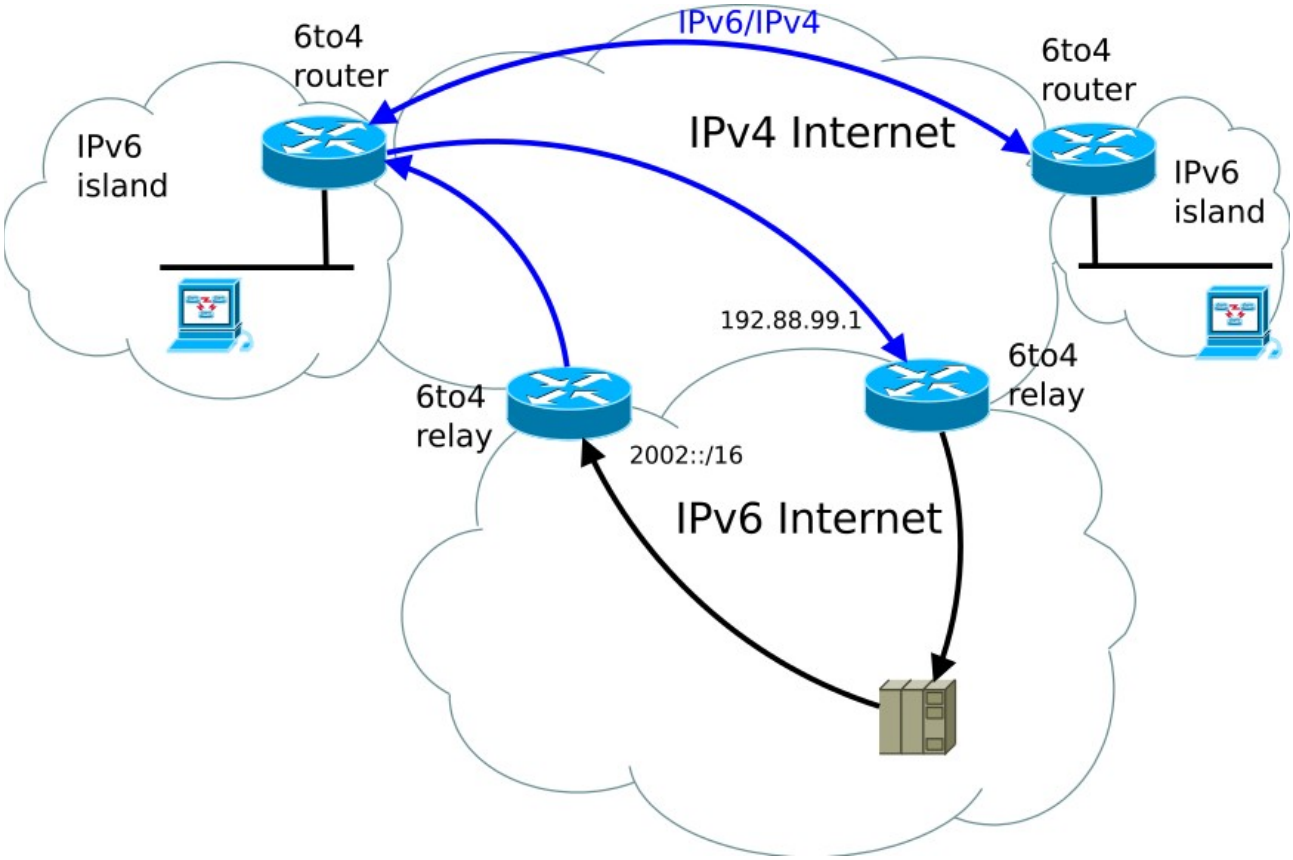
Dnešní díl potěší především ty, které předchozí díly tohoto seriálu dostatečně naladily a mají chuť si protokol IPv6 vyzkoušet v praxi. Jak už bylo řečeno, protokoly IPv4 a IPv6 jsou vzájemně nekompatibilní a protože je jasné, že v současném Internetu prostě není možné oznámit, že od určitého data se IPv4 vypíná a naopak zapíná IPv6, bylo nutné vymyslet nějaké mechanismy, jak tyto protokoly mohou vedle sebe existovat a jak postupně převádět provoz směrem k IPv6.

Dual-stack

Asi každého napadne, že nejjednodušší by bylo prostě do sítě zavést protokol IPv6 a nechat dále vedle něj běžet stávající IPv4 konektivitu. Takováto situace se nazývá dual-stack a jak už to někdy bývá, nejjednodušší řešení bývají i ta nejsprávnější. Snad jedinou malou nevýhodou dual-stacku je fakt, že musíte na jedné fyzické infrastruktuře spravovat dvě logické, ale to jde rozhodně zvládnout. Většina služeb a operačních systémů obvykle preferuje IPv6 spojení před IPv4. Probíhá to tak, že klient s IPv6 konektivitou se nejprve dotáže systému DNS, zdali je služba dosažitelná po IPv6 nebo-li jestli má AAAA záznam. Pokud jej objeví pokusí se sestavit spojení po IPv6 a pokud záznam nenajde nebo spojení selže, dotáže se na A záznam a pokračuje po IPv4. Pokud tedy bude narůstat počet služeb dosažitelných po IPv6, poměr toků v dual-stackových sítí se bude výrazně zvyšovat pro IPv6.

Tunelování

Nicméně toto je bohužel spíše méně obvyklý případ a obvykle máme k dispozici pouze IPv4 konektivitu. Ani v takovém případě ale není nic ztraceno a existují možnosti, jak se do IPv6 světa připojit. Prakticky všechny způsoby využívají mechanismu, který se nazývá tunelování. Obecně řečeno, jde o technologii, která zabalí pakety nějakého protokolu do paketů jiného. V tomto konkrétním případě jde zabalení IPv6 do IPv4, které nám slouží k tomu, abychom překlenuly tu část sítě, která IPv6 nepodporuje. Jako ilustrace nám může posloužit následující obrázek se serveru Wikipedia, který je konkrétně pro tunel 6to4, ale princip je naštěstí dostatečně obecný.



Izolované ostrůvky, které podporují IPv6 (může jít o celé sítě, ale i třeba o jednotlivou stanici) se mohou do světa IPv6 připojit tak, že hraniční router těchto ostrůvků zabalí IPv6 paket do protokolu IPv4 a pošle přes starý Internet dál na tzv. relay. Relay musí být připojena k obou světům a z tohoto paketu vybalí pouze IPv6 část a tu pošle dál. Obráceně, pokud dostane IPv6 paket pro ostrovní síť, zabalí ji do IPv4 a pošle. Jak i obrázek naznačuje, komunikace v různých směrech nemusí jít vždy stejnou cestou. Obvykle je i možné, aby ostrovní sítě spolu komunikovaly na přímo, mimo hlavní IPv6 Internet. Pojďme se tedy podívat na hlavní zástupce tunelování.

6to4 tunelování – ke správnému fungování potřebuje veřejnou IPv4 adresu. Vzhledem k tomu, že většina klientských stanic je v dnešní době obvykle připojena pomocí NATu, je tato technologie určena spíše pro hraniční router. Na druhou stranu, pro síť za routerem je vyhrazen celý prefix délky /48. 6to4 odvozuje svou

IPv6 adresu právě z veřejné IPv4 a pro veškeré adresy je vyhrazen prefix 2002::/16. Například pro adresu 203.0.113.42, je odpovídající IPv6 6to4 prefix 2002:cb00:712a::/48, kde cb00:712a je hexadecimální zápis výše uvedené IPv4 adresy. Na rozdíl od nativní IPv6 konektivity je v operačních systémech je obvykle IPv4 preferováno před 6to4, takže takovýto typ tunelu bude použit především pro služby výhradně založené na IPv6. Pro transport je použit speciální typ protokolu číslo 41, což může způsobovat problémy u některých typů firewallů. 6to4 tunelování je automatický aktivní od verze Windows XP SP2 v případě, že neexistuje nativní (normální) IPv6 adresa a stanice má přiřazenu veřejnou IPv4 adresu. V Linuxových systémech je možné 6to4 zapnou poměrně jednoduchým způsobem. 6to4 podporují v současné době i některé SOHO routery, jako třeba D-Link DIR-815. Od června loňského roku je relay pro 6to4 i v České Republice, provozuje jí sdružení CZ.NIC.

ISATAP tunelování – je speciálním typem tunelování, které zajišťuje IPv6 konektivitu mezi stanicemi v rámci IPv4 interní sítě. To znamená, že se ISATAP tunelování nedá použít mimo rámec organizace, k tomu účelu však může posloužit např. 6to4 tunelování z ISATAP směrovače. ISATAP adresa se dá poznat podle posledních 64 bitů IPv6 adresy, ty budou mít formát :0:5efe :w.x.y.z (kde w.x.y.z je privátní IPv4 adresa) či 200:5efe:w.x.y.z (kde w.x.y.z je veřejná IPv4 adresa). Poslední verze operačního systému Windows mají ISATAP tunelování ve výchozí konfiguraci. Proto lze ve výpisu adres systému nalézt minimálně linkovou lokální ISATAP adresu, která by v případě stanice s privátní IPv4 adresou 192.168.1.2 vypadala takto fe80::5efe:192.168.1.2%13. Dále v případě funkčního ISATAP směrovače, při propagovaném prefixu 2001:db8:0:7::/64, by stanice měla ještě globální ISATAP adresu 2001:db8:0:7:0:5efe:192.168.1.2.

Teredo tunelování – je metoda tunelování, která ke svému fungování nevyžaduje veřejnou adresu a poradí si s překladem adres (kromě symetrického NAT, kde jsou určitá omezení). Z IPv6 rozsahu byl pro Teredo vyhrazen prefix 2001::/32. Teredo adresa by mohla vypadat například takto 2001:0:5ef5:79fd:3409:1033:f5ff:ffd5. Je v ní obsaženo hned několik informací a to IPv4 adresa použitého Teredo serveru, typ klientova NATu, veřejná adresa NATu a číslo UDP portu NATované komunikace. Teredo je aktivní ve výchozí konfiguraci od Windows Vista a podobně jako u 6to4 se pro komunikaci s IPv6 světem využije jen v případech, kdy je cílová služba dostupná pouze po IPv6 a není k dispozici normální IPv6 konektivita. Uživatelé Linuxu a MacOS mohou použít k Teredo tunelování volně dostupnou implementaci s názvem Miredo. I pro Teredo provozuje sdružení CZ.NIC lokální relay a to od dubna tohoto roku. Její adresa je teredo.nic.cz.

Tunel Broker – není žádný konkrétní typ, ale spíše rodina tunelů. Až doposud byly v článku popsány tunelovací techniky, které bylo možné nakonfigurovat pouze na straně klienta a relaye pak už fungovaly v podstatě automaticky, uživatel neví, jak přesně jeho tunel vede. U tunel brokeru se uživatel dohodne s konkrétním provozovatelem tunelu na nastavení. Tím má uživatel jistotu, kam přesně jeho tunel vede a zároveň je komunikace pomocí takovéhoto tunelu obvykle symetrická. Jako příklady provozovatelů tohoto typu tunelu lze uvést Hurricane Electric na adrese http;//tunnelbroker.net či SixXS na adrese http://www.sixxs.net. Nevýhodou druhé jmenované služby je fakt, že proto, aby uživatel obdržel konfigurační údaje k tunelu musí napsat krátkou esej o tom, k čemu tunel potřebuje. Výhodou pro české uživatele naopak je, že tato služba má i lokální relay, kterou od letošního února poskytuje společností Ignum.

Ke všem typům tunelů dlužno podotknout, že rozhodně nejsou myšleny jako definitivní řešení pro přechod na IPv6. Jakékoliv tunelování pochopitelně vede k degradaci kvality služby a to například tím, že ke každému paketu je přibalována hlavička dalšího protokolu a že routing z hlediska tunelujícího protokolu nemusí být vůbec výhodný pro protokol jenž je tunelován.

Tímto jsme probrali technologie pro připojení sítí pouze s IPv4 do IPv6. V příštím díle se budeme zabývat bezpečností a zároveň si povíme, jaké existují mechanismy pro vyřešení opačného problému tedy pro připojení sítí pouze s IPv6 protokolem do IPv4.

Autor:
Ondřej Filip, výkonný ředitel sdružení CZ.NIC, správce národní domény .CZ