Computerworld, 8. 10. 2011

Silné a slabé stránky protokolu IPv4

Každou chvíli se dozvídáme z médií, že síť sítí rychle roste. Každým dnem se k Internetu připojí obrovské množství uživatelů, vznikají nové služby, rozšiřuje se a zkvalitňuje síťová infrastruktura. Počet připojených zařízení se také zvyšuje. Už se nejedná jen o klasické počítače, ale připojeny jsou televize, blue-ray přehrávače, telefony, herní konzole, ledničky, kamery, domácí čidla a podobně. Pokud se nad tímto raketovým růstem zamyslíte, musí se vám nutně zdát, že lidé, kteří Internet před desítkami let navrhli, museli mít obrovskou předvídavost a genialitu. Jenže i oni byli jen lidé a tak je i v návrhu Internetu bohužel jedna nedokonalost. A ta právě spočívá v tom, že počet zařízení, které je možné připojit, je omezen. Úplně první adresní prostor byl navržen tak, že počáteční číslo IP adresy označovalo síť a zbylé tři vyjadřovaly číslo daného počítače v síti. To tedy znamenalo, že by takových sítí mohlo být maximálně 256, což samozřejmě přestalo velmi rychle stačit a tak záhy přišla první změna.

Rozdělení do tříd nepomohlo

Členění adresního prostoru bylo v roce 1981 změněno tak, že všechny ty více než čtyři miliardy adres se rozdělily do pěti základních skupin, tzv tříd. Třída A byly adresní bloky pro velké organizace. Velikost takových bloků byla 16777216 a bylo jich pouze 127. Tyto adresy se poznaly podle toho, že ve dvojkové soustavě byl jejich nejvýznamnější bit 0. Třída B byla určena středním organizacím a velikost jejich bloků byla 65536 a takovýchto bloků bylo 16384; ve dvojkové soustavě tyto adresy začínaly prefixem 10. Bloky adresní třídy C měly velikost 256 adres a takových bloků bylo 2097152. Tyto adresy byly uvozeny 110. Třídy D a E už nebyly (a nejsou dodnes) určeny pro adresování běžného Internetového provozu. Adresy třídy D začínají 1110 a jsou určeny pro skupinové adresování nebo-li multicast. Poslední třída E začínající na 1111 je vyhrazena pro budoucí použití. Následující tabulka celou situaci rekapituluje.

Třída	Uvozující bity	Teoretický počet sít	Počet adres v síti	Adresní rozsah
Třída A	0	128	16777216	0.0.0.0 – 127.255.255.255
Třída B	10	16384	65536	128.0.0.0 – 191.255.255.255
Třída C	110	2097152	256	192.0.0.0 – 223.255.255.255
Třída D	1110	nedefinováno	nedefinováno	224.0.0.0 – 239.255.255.255
Třída E	1111	nedefinováno	nedefinováno	240.0.0.0 – 255.255.255.255

Poměrně záhy se ukázalo, že ani toto členění není optimální. Velké množství organizací vyžadovalo více než 256 připojených počítačů a proto žádaly adresní bloky třídy B. Protože těchto bloků je jen 16384, velmi rychle začaly docházet. Tento jev byl nazván „class B exhaustion“.

A tak bylo opět nutné změnit adresní schéma. K tomu došlo v roce 1993, kdy třídy A, B a C byly zrušeny a nahrazeny novým systémem „Classless Inter-Domain Routing (CIDR)“. Tento nový systém spočíval v tom, že členění adresy na číslo sítě a číslo stroje začalo být dynamické. To, jaká část adresy bude použita na číslo sítě, začala vyjadřovat tzv. síťová maska, která se zapisuje buď podobně jako IP adresa čtveřicí dekadických čísel například 255.255.255.0 (ve dvojkové soustavě vždy několik jedniček následovaných nulami, tedy v tomto případě 11111111111111111111111100000000) nebo pouze jako číslo vyjadřující, kolik číslic ve dvojkové soustavě (bitů) vyjadřuje číslo sítě, tedy například /24. Tedy 172.16.34.23/255.255.0.0 = 172.16.34.23/16 je adresa počítače v síti 172.16.0.0/16, což je síť, která může obsahovat až 65536 strojů.

Název vložáku - „Zpomalovače“ CIRD a NAT

CIDR dramaticky zpomalil ubývání adresního prostoru a jeho správci si mohli na chvíli oddychnout. Nicméně i tak bylo zřejmé, že adresní prostor záhy dojde a tak byla vynalezena ještě další technologie, která má jeho ubývání bránit. Tato technologie se nazývá NAT a je založena na poměrně jednoduchém pozorování, že rozhodně ne všechny stroje připojené k Internetu mají stejnou funkci. Některé převážně poskytují služby, to jsou tzv. servery, a jiné připojují běžné uživatele k Internetu, tzv. klienti. Drtivá většina služeb Internetu je postavena na principu, že klient iniciuje spojení se serverem, pošle mu dotaz a server pak odpovídá. Iniciace spojení probíhá tak, že klient si zvolí tzv. číslo portu, což je jakési pseudonáhodné číslo velikosti 1 až 65535 a provede spojení s IP adresou serveru a jeho číslem portu, který je pro každou službu dán. Protokol HTTP, který se používá pro přenos WWW stránek, má například číslo 80. Spojení je tedy určeno čtveřicí čísel: zdrojová adres, zdrojový port, cílová adresa a cílový port. Čísla na straně serveru jsou daná a nelze s nimi hýbat, ale autory technologie NAT napadlo, zda-li je nutné, aby každý klient měl nutně svou zdrojovou IP adresu. Výsledek potom vypadá následovně. Větší skupina počítačů používá jakési „falešné“ adresy z nějakého vyhrazeného rozsahu. Tyto adresy nejsou z Internetu dosažitelné a může je ve svých privátních sítích používat i kdokoliv jiný. Tato skupina je připojena do Internetu pomocí zařízení (směrovače, routeru), které má alespoň jednu svou „pravou“ IP adresu. Pokud se tedy klient z této skupiny chce připojit k nějaké službě, pošle požadavek na spojení se svou „falešnou“ adresou a číslem

portu. Směrovač nemůže takovýto požadavek přímo přeposlat do Internetu, protože ony „falešné“ IP adresy nejsou v Internetu dostupné, a tak provede překlad a klientovu adresu a port nahradí svou „správnou“ IP adresou a svým číslem portu. Fakt, že tento překlad provedl, si musí zapamatovat, protože až přijde od serveru odpověď na zdrojovou adresu a port, musí ji být schopen přeposlat zpět klientovi opět na jeho původní „falešnou“ adresu a port. Omezením této technologie je výkon a kapacita směrovače, který si musí pamatovat a prohledávat všechna otevřená spojení, a také počet portů, které má směrovač k dispozici. Pokud má totiž klient svou IP adresu, může otevřít zhruba 65 tisíc spojení. V případě NATu tento počet sdílí s ostatními připojenými klienty. Na druhou stranu hlavní výhodou NATu je, že větší počet klientských stanic využívá pouze jednu IP adresu. Jakkoliv NAT vypadá poněkud komplikovaně, v dnešním Internetu je takto připojené obrovské množství klientských stanic a tato technologie opět významně zvýšila úsporu adresního prostoru.

Přerozdělovací politika

Nicméně ani všechny tyto změny v adresování nepomohly a adresní prostor nám rychle ubývá. Asi nejvíce citovanou analýzu na toto téma provedl Geoff Huston z organizace APNIC, který na svých stránkách http://ipv4.potaroo.net ukazuje, kdy nám při současném způsobu přidělování zhruba IP prostor dojde. Nejde o jedno číslo, protože přidělování adresního prostoru je hierarchické. Veškeré IP adresy drží americká organizace IANA. Ta je přiděluje ve velkých blocích pěti regionálním organizacím, tzv. Regional Internet Registry (RIR). Regiony jsou Severní Amerika, Jižní Amerika, Asie-Pacific, Afrika a Evropa-střední východ. Tyto RIRy přidělují adresy jednotlivým poskytovatelům a teprve ti je přidělují koncovým uživatelům. Určit, kdy tedy dojdou adresy koncovým uživatelům je nemožné, protože to bude u každého poskytovatele jiné, nicméně v době psaní tohoto článku ukazovala Hustonova analýza, že u IANA dojdou adresy v květnu 2011 a RIRům pak na začátku roku 2012. To, že dojdou adresy samozřejmě neznamená konec Internetu, ale rozhodně se výrazně zkomplikuje připojování nových uživatelů, omezí se možnosti vstupu nových poskytovatelů na trh a podobně.

Zatím jedinou známou možností, jak se s problémem vypořádat, je přechod na protokol IPv6, který mimo jiné významně rozšiřuje adresní prostor, ale o tom už v dalším díle toho seriálu.

O autorovi:
Ondřej Filip, výkonný ředitel sdružení CZ.NIC, správce české národní domény .CZ