Portál pre odborné publikovanie ISSN 1338-0087

Model OSI a zavádění IPv6 v počítačových sítí

Hanáček Adam · Informačné technológie

07.08.2013

Článek se zabývá aktuální problematikou související s přechodem z protokolu IPv4 na protokol IPv6 v počítačových sítích. Úvod článku poskytuje celkový pohled na historii a původní určení počítačových sítí. První část práce pak popisuje jednotlivé vrstvy modelu OSI a rozdíly oproti celosvětově používaném modelu TCP/IP. Dále je popsána aktuální situace a pravděpodobný průběh přechodu z protokolu IPv4 na IPv6. Na závěr je probrána vhodnost délky síťové adresy IPv6.

Úvod

“Počítačová síť je soubor zařízení a pravidel, která slouží pro přenos dat mezi počítači, které se skládají z různých stavebních bloků: počítačů, přepínačů, kabelů a tak dále.“ [1] První počítačové sítě se začaly objevovat již v 60. letech 20. století. Tehdy však ještě nikdo netušil, jak velký bude rozvoj počítačových sítí v 80. letech, kdy vzniklo více operačních systémů s vlastními protokoly pro komunikaci v rámci své sítě. Ovšem právě z důvodu odlišnosti protokolů nebylo možné propojení různých operačních systémů mezi sebou. Sítě tedy byly uzpůsobeny pro komunikaci jen v rámci jednoho podniku.

Z toho důvodu byl vytvořen otevřený síťový systém OSI (Open Systems Interconnection), který byl přijat roku 1984 mezinárodní normou ISO (International Standard Organization) a stal se v budoucnu základním kamenem pro počítačové sítě. V Internetu je však nutné přidělovat adresy pro identifikaci sítí a počítačů, a právě to zajišťuje centrální autorita IANA (Internet Assigned Numbers Authority), která přiděluje velké bloky adres regionálním registrům (Regional Internet Registry, RIR). Těch je pět a na jejich počtu se nejspíš hned tak něco nezmění. Zeměkouli mají rozdělenu následovně [2]:

- AFRINIC Afrika
- APNIC Asie a Pacifik
- ARIN Severní Amerika
- LACNIC Latinská Amerika
- RIPE NCC Evropa a Blízký východ

Pro směrování dat v Internetu je stále nejrozšířenější protokol IPv4. Při vzniku Internetu se však počítalo pouze s rozšířením na univerzitách případně do několika firem. Nikdo nepředpokládal takové rozšíření Internetu, které začalo již v 80. letech.

Proto se zdálo být 32 bitů, které umožňuje připojit až 2^{32} -1 (přibližně 4,3 * 10^{9}) počítačů pro adresaci jednotlivých zařízení, více než dostačující. V současné době je však zmíněných 2^{32} -1 připojitelných zařízení pomocí IPv4 nedostatečný, proto se pomalu přechází na protokol IPv6, který využívá 128 bitů pro adresaci zařízení. Umožňuje tedy připojit až 2^{128} -1 (přibližně 3,4 * 10^{38}) počítačů. Článek je zaměřen nejen na podrobný popis modelu OSI, ale také pojednává o optimálnosti zvýšení počtu připojitelných zařízení z 2^{32} -1 na 2^{128} -1.

Model OSI

Jak již bylo naznačeno v úvodu, model OSI byl vytvořen z důvodu nekompatibility počítačových sítí mezi jednotlivými výrobci. "Systém odesílající požadavek musí dodržet tyto čtyři kroky (založené na specifických funkcích modelu OSI) [3]:

1. Adresovat požadavek
2. Přiřadit mu určitý protokol
3. Modulovat ho
4. Předat ho po fyzickém médiu"

Model OSI je složen ze sedmi vrstev, které stanovují způsob manipulace s daty. V rámci modelu OSI slouží aplikační, prezentační a relační vrstva pro zpracování dat a zbylé vrstvy jsou určeny pro vlastní přenos dat. Každá vrstva komunikuje pouze se sousedními vrstvami, přičemž každá nižší vrstva poskytuje služby své vyšší vrstvě. Při posílání zprávy putují data od nejvyšší vrstvy po nejnižší. Žádná vrstva nemění obsah zprávy, ale jednotlivé vrstvy přidají k datům svou hlavičku, další informaci nebo zpracují data (modulace, šifrování).

7. Aplikační vrstva

Aplikační vrstva je nejvyšší v modelu OSI. Aplikační vrstvu tvoří pouze obecné mechanismy, které využívají aplikace pro odesílání nebo příjem dat po síti. Jinými slovy se jedná o rozhraní, které využívají aplikace pro práci s daty po síti. Mezi nejznámější používané protokoly patří FTP pro přenos souborů, HTTP pro přenos hypertextových stránek, TELNET jako síťový virtuální terminál nebo SNMP pro vzdálenou správu síťových zařízení.

6. Prezentační vrstva

Úkolem prezentační vrstvy je převod dat do podoby srozumitelné pro příjemce, případně zajistit ochranu dat proti zneužití. Patří sem tedy komprese, dekomprese, šifrování nebo dešifrování dat předaných aplikační vrstvou.

5. Relační vrstva

Relační vrstva se stará o vytvoření relace mezi odesílatelem a příjemcem. V hlavní řadě zajišťuje začátek, konec, případně obnovu spojení. Mimo to umožňuje také správu přístupu -tedy přihlašování, odhlašování a kontrolu hesla uživatele.

4. Transportní vrstva

Transportní vrstva zajišťuje hlavní aspekty přenosu dat mezi dvěma procesy. Rozděluje zprávu na stejně dlouhé úseky (segmenty nebo datagramy) a naopak. Při přenosu zprávy pohlíží na síť tak, jako by byla přímo spojena s koncovým zařízením. Procesy zde spolu komunikuji prostřednictvím portů, což je číslo v rozmezí 1-65535, které identifikuje konkrétní aplikaci. Mezi nejčastěji používané protokoly v transportní vrstvě jsou TCP (Trasmission Control Protocol) pro spolehlivý přenos dat nebo UDP (User Datagram Protocol) pro rychlý, ale nespolehlivý přenos dat. "Základní přenosovou jednotkou na transportní vrstvě je tedy buď TCP segment nebo UDP datagram." [4]

3. Síťová vrstva

Transportní vrstva tedy využívá komunikaci mezi procesy, kdy pohlíží na síť tak, jako by byla přímo spojena s koncovým zařízením. Spojení však přímé není a je nutné vybrat nejvhodnější cestu ke koncovému zařízení a data směrovat, o což se stará síťová vrstva s pomocí logických adres. Ty jsou přiřazeny administrátorem. Síťová vrstva vytváří ze segmentů pakety (datagramy) a přidá k nim adresu zdroje a cíle komunikace. Na této vrstvě pracuje router (směrovač).

2. Linková vrstva

Na rozdíl od síťové vrstvy linková vrstva pracuje s MAC (Media Access Control) adresami, které jsou přiděleny přímo výrobcem, a řeší přenos mezi přímo sousedícími stanicemi. Převádí pakety na rámce, a tím se opět větší úseky rozdělí na více úseků o stejné délce. Rámce pak obsahují příznak začátku rámce, hardwarovou adresu cílového zařízení, hardwarovou adresu zdrojového zařízení, délku paketu, vlastní paket a nakonec kontrolní součet. Na straně příjemce je pak úkolem linkové vrstvy zajistit správné seřazení rámců a požádat o opětovné vyslání rámce v případě, že byl poškozen. Na linkové vrstvě pracují bridge (mosty) a switche (přepínače).

1. Fyzická vrstva

Fyzická vrstva nakonec zajišťuje samotný přenos dat a řeší napěťové úrovně, časování, konektory, rozhraní a také konverzi přenášených bitů (A/D a D/A převodníky). Patří sem huby, opakovače a síťové adaptéry.

Model OSI a TCP/IP

Ačkoli referenční model OSI je nejlépe známý model vrstveného síťového zásobníku, není jediný. V celosvětové síti Internet se používá model TCP/IP. Model OSI má 7 vrstev (aplikační, prezentační, relační, transportní, síťovou, linkovou a fyzickou), zatímco architektura TCP/IP pouze 4 (aplikační, transportní, síťovou a vrstvu síťového rozhraní). TCP/IP slučuje vrstvu aplikační, prezentační a relační do jedné s názvem aplikační vrstva. Dále slučuje linkovou a fyzickou vrstvu do jedné s názvem vrstva síťového rozhraní. Síťová vrstva bývá někdy v českých textech nazývána internetovou vrstvou (internet layer).

Základním protokolem síťové vrstvy je IP protokol, který zajišťuje přenos datagramu na základě síťových IP adres obsažených v jejich záhlaví. Datagramy putují sítí nezávisle na sobě a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. IP

protokol poskytuje vyšším vrstvám síťovou službu bez spojení. Doručení datagramu tedy není zaručeno a spolehlivost musí zajistit vyšší vrstvy (TCP, aplikace). Hlavní rozdíl TCP/IP oproti modelu OSI je v převedení spolehlivosti přenosu dat až na transportní vrstvu, což zajistilo zvýšení rychlosti přenosu. [3] V současnosti se nejčastěji používá protokol IPv4, ale postupně se přechází na protokol IPv6.

Pravděpodobný průběh přechodu z IPv4 na IPv6

IP (Internet Protocol) náleží síťové vrstvě a používá se pro jednoznačnou identifikaci počítačů v síti. "Protokol je založen na principu hostitelů a sítí. Hostitelem je jakékoli zařízení v síti, které je schopné odesílat a přijímat pakety IP. Hostiteli proto mohou být směrovače, pracovní stanice, servery či každé zařízení s adresou IP."[5] "Balík protokolů TCP/IP definuje jistá pravidla k přiřazování IP adres."[6] Jak již bylo zmíněno v úvodu hlavním důvodem zavádění IPv6 je masivní nárůst počtu možných adres, které lze přidělit a to z 232 -1 až na 2128 -1. Zmíněný přechod by však nenastal, kdyby nebyl nezbytně nutný. Adresy IPv4 jsou již téměř všechny obsazeny a nastal nástup přidělování IPv6 adres. Důvodem tak pozdního zavedení IPv6 je zřejmě fakt, že hlavní výhoda nového protokolu spočívá pouze v rozšíření adresního prostoru a neexistoval dostatečný tlak na výrobce, dodavatele Internetu ani uživatele pro dřívější přechod na IPv6.

Dalším důvodem tak pozdního nasazení je i jeho náročné zavedení do praxe. Nestačí pouze přenastavit síťové zařízení, ale musí v první řadě existovat samotná podpora IPv6. Starší zařízení samozřejmě IPv6 nepodporují. Přechod tedy nebyl možný ze dne na den a byl zvolen pozvolný přechod. V současné době se počet připojených domén pomocí IPv6 pohybuje pouze okolo 18%. Z výsledků zveřejněných na [7] lze odhadnout budoucí nástup IPv6. Jestliže tedy bude přechod probíhat podobně jako doposud, tak v roce 2015 bude využívat IPv6 přibližně 28% domén a v roce 2020 bude využívat IPv6 53% domén. Je však nutné zdůraznit, že domény využívající IPv6 stále podporují i starý protokol IPv4. [7] Jiná situace je ovšem u koncových uživatelů. Pouze přibližně 1,60% uživatelů využívá nový protokol IPv6, přičemž ze zdrojů [8][9][10] je možné odhadnout, že v roce 2015 bude IPv6 využívat 3,2% uživatelů a v roce 2020 bude IPv6 využívat 8,45% uživatelů.

Zatížení sítě protokolem IPv6

Jak lze odvodit z výše zmíněného, při přenosu každého paketu se zvýší délka jeho hlavičky z 32 bitů na 128 bitů. Vzhledem k velmi vysokým přenosovým rychlostem však nelze očekávat problémy způsobené zahlcením sítě jako důsledek prodloužení délky hlavičky.

Vhodnost délky síťové adresy v protokolu IPv6

Nedostatečnost 32 bitové délky pro adresaci sítě je již dlouho zřejmá. Otázkou však zůstává, jestli je optimální skok až na 128 bitů a nestačilo by pouze 64 bitů. Počet možných adresovatelných zařízení při použití staré IPv4 je přibližně $4,3 * 10^9$, což reálně nevychází ani jedna IP adresa na osobu. Při použití 64 bitů je celkový počet IP adres 2^{64}-1 a to se rovná $18,447 * 10^{18}$. Za předpokladu, že na Zemi žije přibližně $7 * 10^9$ lidí, vychází přibližně $2,635 * 10^9$ IP adres na osobu. Musí se ovšem počítat s tím,

že při vytváření podsítí jsou nulové bity určené pro adresaci sítě a jedničkové pro všesměrové vysílání. Dále je nutné předpokládat budoucí nárůst populace a zvolit určitou rezervu pro využití IP adres v serverech, směrovačích a pro hostitele.

Mimo to je také třeba předpokládat využití IP adres pro hodinky, lednice, televize atd. Ovšem i přes předpoklad trojnásobného nárůstu počtu obyvatel a zvolení dostatečné rezervy pro úbytek způsobený tvorbou podsítí a využití IP adres v jiných zařízeních by bylo možné předpokládat až $6,588 * 10^8$ IP adres na osobu, což je více než dostačující. Při použití IPv6 je však celkový počet adres na osobu $4,86 * 10^{28}$. Důvod tak velké rezervy zřejmě vychází z předchozího poučení z 80. let, kdy se také zdála být délka IPv4 naprosto dostatečná, a proto byl nyní pro jistotu zvolen možná až příliš velký adresní prostor. Nicméně vzhledem k velmi vysokým nákladům, které stojí přechod na IPv6, je tato volba pochopitelná.

Závěr

Hlavní část práce popisuje nejen pravděpodobný průběh přechodu na protokol IPv6, ale také vhodnost 128 bitové délky protokolu. Přechod na IPv6 trvá již spoustu let a s jistotou lze říci, že ještě spoustu let potrvá. Reálná délka 128 bitů se zdá být zbytečná a plně dostačující by byla délka 64 bitů, nicméně vzhledem k velmi vysokým přenosovým rychlostem nepředstavuje 128 bitů pro adresaci počítačů v síti žádný problém. Proto tak masivní až možná zbytečně velké rozšíření adresního prostoru nelze označit za chybu. Rychlost zavádění IPv6 lze jen stěží odhadnout. Teoretický předpoklad budoucího vývoje je znázorněn v kapitole “Pravděpodobný průběh přechodu z IPv4 na IPv6“, ovšem jedná se pouze o odhad, který může být od skutečnosti odlišný. I nově přidělené adresy však podporují starší protokol IPv4.

Použitá literatura

1. SOSINSKY, Barrie. Počitačovésítě. 1. vyd. Brno: Computer Press a.s, 2010. ISBN 978-80-251-3363-7.
2. SATRAPA, Pavel. Internetovýprotokol IPv6.Praha 6: CZ.NIC, z. s. p. o., 2011. ISBN 978-80-904248-4-5.
3. OSTERLOH, Healther. TCP/IP Kompletníprůvodce.Praha 8: SoftPresss.r.o, 2003. ISBN 80-86497-34-8.
4. DOSTÁLEK, Libor a Alena KABELOVÁ. Velkýprůvodceprotokoly TCP/IP a systémem DNS. Brno: Computer Press a.s., 2008. ISBN 978-80-251-2236-5.
5. BIGELOW, Stephen J. Mistrovství v počítačových sítí. Brno: ComputerPress, a.s., 2004. ISBN 80-251-0178-9.
6. ODOM, Wendell. Směrování a přepínání sítí. Brno: ComputerPress, a.s., 2009. ISBN 978-80-251-2520-5.
7. IPv6 domény. Statistiky CZ [online]. 2013 [cit. 2013-07-22].Dostupné z: https://stats.nic.cz/stats/ipv6_domains/
8. IPv6. Cloud Computing, Enterprise, Mobile, Security Solutions [online]. 2013 [cit. 2013-07-24].Dostupné z: http://www.akamai.com/ipv6
9. IPv6. IPv6 – Google [online]. 2013 [cit. 2013-07-24].Dostupné z: http://www.google.com/ipv6/statistics.html
10. IPv6 Users by Country. APNIC – Home [online]. 2013 [cit. 2013-07-24]. Dostupné z:

http://labs.apnic.net/dists/v6dcc.html