WrapSix aneb nebojme se NAT64

Michal Zima
zima@wrapsix.cz

EurOpen, 14. května 2013

NAT64

- je jedním z mnoha přechodových mechanismů pro IPv6
- nahrazuje koncept NAT-PT
- hlavní RFC6144–6147
- snaží se obejít nekompatibilitu mezi IPv4 a IPv6 pomocí prostředníka

Ostatní přechodové mechanismy

	Infrast.	Řešení koexistence IPv4 a IPv6
6in4	IPv4	dual-stack
6to4	IPv4	dual-stack
6rd	IPv4	klientské tunely
6over4	IPv4	osamocené IPv6 uzly
ISATAP	IPv4	totéž, ale nevyžaduje IPv4 multicast
4rd	IPv6	klientské tunely
DS-Lite	IPv6	IPv4 podsítě (+ dual-stack)

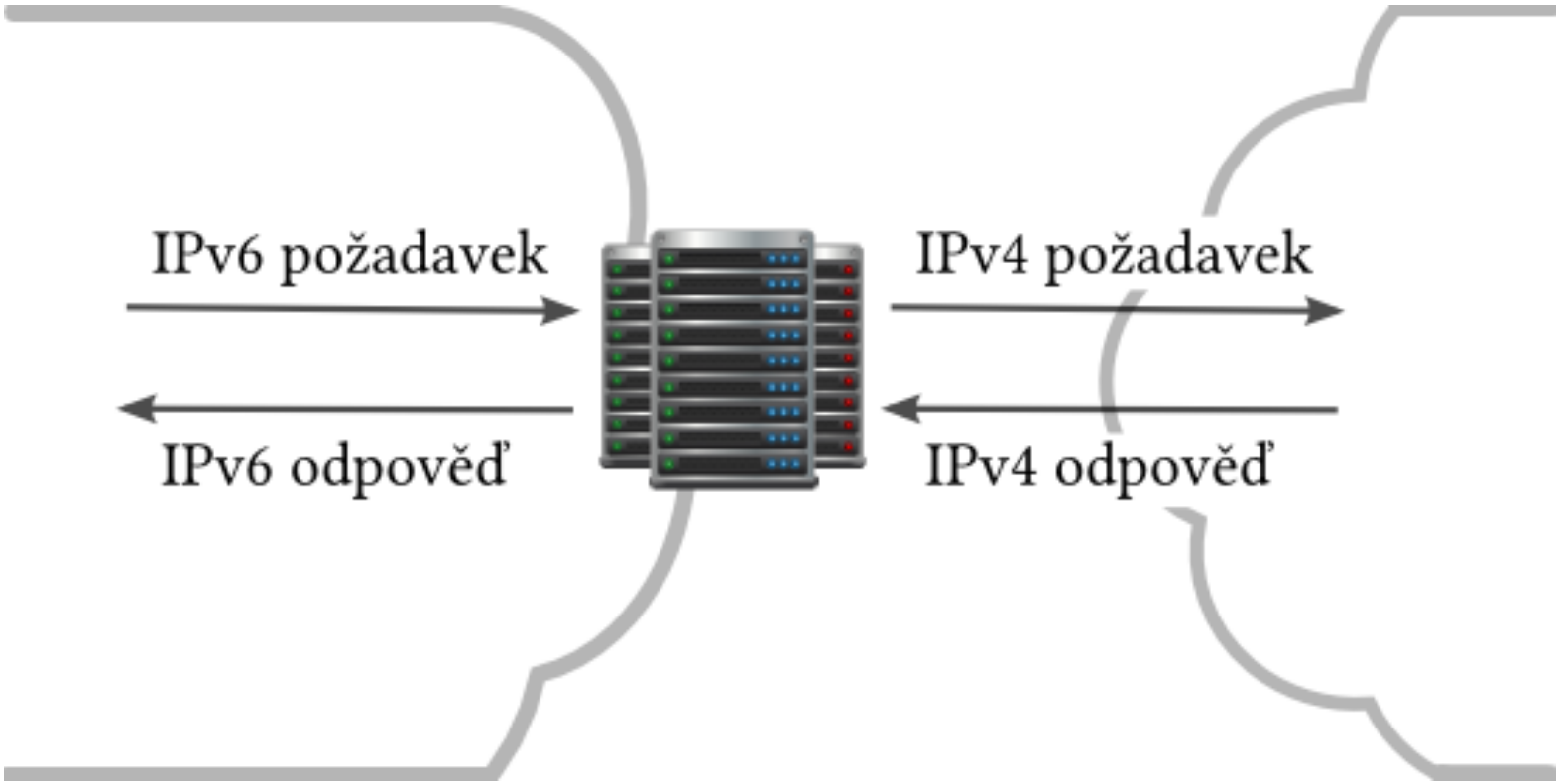
Co tedy požadujeme

- přechodový mechanismus pro IPv6 infrastrukturu
- přechodový mechanismus i pro osamocené uzly, ne jen podsítě
- netlačit klienty k dalšímu nákupu HW
- co nejméně omezení

Co dostáváme

- NAT64, který překládá provoz z IPv6 do IPv4 a zpátky
- podle množství dostupných IPv4 adres můžeme chtít:
  - bezstavový NAT64
  - stavový NAT64

NAT64



Bezstavový NAT64

- má velmi nízkou režii
- nemá žádný problém se spojeními navazovanými z IPv4 sítě
- ideální například pro sítě zahrnující pouze servery – vyžadující staticky přidělené IPv4 adresy

Stavový NAT64

- umožňuje sdílet IPv4 adresy – jako běžný NAT
- ideální zejména pro běžné sítě s koncovými klienty, kde je IPv4 adres výrazně méně než klientů

Způsob komunikace do IPv4

- IPv4 adresy se mapují do vyhrazeného IPv6 prefixu
- IANA vyhradila pro tento účel 64:ff9b::/96
- příklad: 147.228.60.10 → 64:ff9b::93e4:3c0a
- pro testování apod. lze použít i zápis 64:ff9b::147.228.60.10 – operační systém to zpravidla umí zpracovat

DNS64

- základní prostředek pro získávání mapovaných IPv6 adres
- pokud jméno má veden AAAA záznam (s IPv6 adresou), je vrácen ten
- pokud ne, tak se provede mapování IPv4 adresy z A záznamu do nového AAAA záznamu

DNS64

- zasahování do DNS narušuje integritu DNSSEC zabezpečení
- DNSSEC validaci proto provádí vždy DNS64 server
  - centrální (ISP)
  - koncového uživatele

Překlad IPv6 $\leftrightarrow$ IPv4

- musí být co nejtransparentnější pro obě strany
- při výměně hlaviček protokolů se zachovává maximum voleb (kromě těch, které nemají protějšek)
- v provozu je velmi důležité zejména správné uchopení fragmentace

Fragmentace v IPv4

- fragmentovat může kterýkoli uzel po cestě paketu
- řídí se nastavením bitu „Don't fragment“ v hlavičce
- neprůchozí nefragmentovatelný paket vyvolává ICMP chybu
- oficiální minimální MTU je 68 B

Fragmentace v IPv6

- fragmentace je záležitost pouze odesílatele
- pokud je paket příliš velký, je o tom informován ICMPv6 paketem
  - Path MTU discovery (PMTUd)
- oficiální minimální MTU je 1280 B

Fragmentace v NAT64: 6 $\rightarrow$ 4

- nastavením bitu „Don't fragment“ se simuluje chování běžné pro IPv6
- odesílatel je schopný se s úzkou cestou standardně vypořádat
- pro již fragmentované pakety se povoluje další fragmentace

Fragmentace v NAT64: 4 $\rightarrow$ 6

- pakety mohou být pro IPv6 síť příliš velké
  - nižší MTU
  - o 20 B větší hlavička
- NAT64 figuruje jako poslední IPv4 uzel a první IPv6 uzel na cestě $\Rightarrow$ pokud smí, přizpůsobí paket podmínkám IPv6 sítě

Speciální pakety

- překládá se maximum, co jde
- zejména chybové ICMP zprávy, vč. vnořených paketů
- zatím je def. překlad pro TCP, UDP a ICMP

NAT64 prakticky

- je potřeba DNS64 server a NAT64 brána
- jako DNS64 dobře poslouží BIND
- pro bránu je vhodné vyhradit samostatný server

DNS64

- BIND 9.8.0 a novější
- stačí jeden řádek v konfiguraci, v sekci `options`:
  - `dns64 64:ff9b::/96;`

NAT64

- podle množství provozu zvolíme:
  - běžný PC HW, 1× NIC – desítky tisíc pps
  - výkonnější serverový HW, 2× NIC – stovky tisíc pps
  - dedikovaný HW optimalizovaný pro NAT64 – line-rate (tzn. rychlost linky při nejmenších paketech – 48 B)
- pro první kategorii si lze vybírat z řady řešení

WrapSix

- open-source NAT64 brána
- pokrývá všechny tři kategorie
- běží na Linuxu, nepotřebuje žádné knihovny ani úpravy jádra

Zprovoznění

- nutné přidělit IPv4
- je možné zvýšit minimální MTU v síti (výchozí je konzervativní nastavení 1280 B)
- nastavení směrování prefixu (výchozí je 64:ff9b::/96) na bránu

Dlouhodobější pozorování

- brána samotná funguje bez problémů
- její využívání sítí se dobře řídí na úrovni DNS64
- k vypuštění IPv4 ze sítě je však o něco delší cesta

Problémy

- některé aplikační protokoly (např. FTP) přenášejí uvnitř paketů IP adresy
  - lze relativně jednoduše vyřešit přidáním podpory pro jejich specifický překlad
  - u WrapSixu work-in-progress
- ne všechny aplikace používají ke svému provozu DNS

Aplikace nepoužívající DNS

- typicky hry, eventuálně i běžné aplikace, kterým jen uživatel nepředá jméno, ale přímo adresu
- tři možná řešení:
  - hacknout každou takovou aplikaci – většina však nebude open-source + příliš mnoho práce
  - upravit příslušné knihovní funkce – nepříliš kompatibilní s mobilitou zařízení (přesun do sítě bez NAT64, ale s IPv4 konektivitou)
  - WrapSix Klient (nebo alternativa) – neupravuje aplikace, ani jádro či knihovny

Princip WrapSix Klienta

- programy chtějí IPv4, ale venku není
- budeme v systému emulovat IPv4
- pakety, které přijmeme, přeložíme a pošleme na NAT64
- odpovědi přeložíme zpátky a předáme aplikaci

Shrnutí

- WrapSix spolehlivě překládá (v současnosti) až 1 Gb provozu
- jeho klientská část zase zprostředkovává spojení pro aplikace mimo dosah DNS64
- uživatel by při migraci sítě na tuto kombinaci neměl pocítit žádné omezení
- můžeme tedy seriózně zvažovat odstranění IPv4

Děkuji za pozornost