
5. Politika přidělování adres a různá doporučení

- Speciální případ – prefixy /127
- Prefixy pro organizace - /48 nebo více?
- Prefixy pro sítě – proč /64 a nic jiného?
- Doporučení RIR (ARIN, RIPE)

Using 127-bit IPv6 Prefixes on Inter-Router Links

- [draft-kohno-ipv6-prefixlen-p2p-02.txt](#)

- **Abstract**

On inter-router point-to-point links, it is useful for security and other reasons, to use 127-bit IPv6 prefixes. Such a practice parallels the use of 31-bit prefixes in IPv4 [RFC3021]. This document outlines some of these reasons and specifies that 127-bit IPv6 prefix lengths must be supported on such links.

Komentář

- Týká se zejména backbone sítí:
 - p2p spoje bez ND/NC (SONET)
 - Problém ping-pong (řeší sice [RFC 4443](#), ale většinou není implementováno)
 - routery nemají rozhraní koncových sítí, pak je globální prefix jen na spojích mezi routery
 - Problém útoků na přeplnění ND cache (lze řešit ACL na vstupech do sítě)
- Z řady praktických důvodů je žádoucí mít globální adresy na spojích mezi routery
- Prefix /127 řeší tyto problémy

Komentář

- Jak je to vlastně s délkou Interface ID v globální adrese?
 - Lze použít jinou délku než 64?
- RFC 2373 IP Version 6 Addressing Architecture (1998, aktualizováno RFC 3513, 4291) definuje délku IID 64 bitů:
 - All global unicast addresses other than those that start with binary 000 have a 64-bit interface ID field (i.e., $n + m = 64$), formatted as described in section 2.5.1 (mod. EUI-64). Global unicast addresses that start with binary 000 have no such constraint on the size or structure of the interface ID field.
 - Mnohé další RFC z toho vycházejí, pokud nebude IID 64 bitů, nebudou fungovat (např. SLAAC, DHCPv6, SEND, 6to4)

Komentář

- Podmínky použití /127:
 - HW musí podporovat routing prefixů delších než /64 (některé Broadcom čipy nepodporují)
 - Nemá smysl, pokud je na routeru inzerován prefix koncové sítě /64 nebo kratší a není p2p spoj bez ND (čili pokud se používá Ethernet nebo MPLS)
 - Musí být vypnutelný Subnet Router Anycast – změna [RFC3627](#) na „Use of /127 Prefix Length Between Routers *Running Subnet-Router Anycast* Considered Harmful,,
 - Juniper, Cisco automaticky

A Scalable Addressing Allocation Architecture for IPv6

- [draft-azingerg-scappable-addressing](#)
- The good news is that IPv6 has started growing at a significant rate. The bad news is that IPv6 has started growing at a significant rate.
- Růst počtu inzerovaných prefixů větší než o 50% ročně (pokud by pokračoval v tomto exponenciálním trendu, bude v roce 2040 1,5 miliard prefixů)

Doporučení

■ Agregace

- The assignment of prefixes is intended to roughly follow the underlying Internet topology so that aggregation can be used to facilitate scaling of the global routing system.

■ Problémy:

- multi-homing (nejdelší PI prefix /48)
- traffic engineering
- změna providera bez změny prefixu

■ Doporučení:

- Přidělovat zásadně jen 2^n , nikdy více disjunktních prefixů
- Jinak jako CIDR pro IPv4

IPv6 Address Assignment to End Sites

- [draft-ietf-v6ops-3177bis-end-sites](#)
- Update [RFC 3177](#) (2001)
- Původní doporučení:
 - /48 obecně, s výjimkou velkých uživatelů
 - /64 pokud je jisté, že bude vyžadován právě jeden subnet a nikdy více
 - /128 pokud je napojeno jediné zařízení
- Typické příklady:
 - Koncový uzel připojený přes PPP dostane /128 ze sdíleného prefixu /64
 - Mobilní zařízení se sítí (auto, mobil) dostane /64
 - Domácí síť dostane /48
 - Malá firma dostane /48
 - Velká firma dostane /47 nebo kratší prefix

Komentář RFC 3177

Důvody zavedení doporučené délky prefixu /48:

- Jednotná délka prefixu pro koncové sítě zjednodušuje přechod mezi ISP a přechod na PI.
- Prefix délky /48 dovoluje všem prakticky neomezený růst sítě bez nutnosti realokace prefixů od ISP nebo používání NAT.
- Zjednodušuje správu reverzních DNS záznamů.
- Dovoluje využít 6to4 pro nouzovou konektivitu a beze změny vnitřní struktury (6to4 adresa má prefix 2002:IP:V4::/48, dalších 16 bitů lze použít na subnet).

Komentář RFC 3177

- **Není to mrhání adresovým prostorem?**
 - Prefix 001/3 (2xxx:: a 3xxx::) dovoluje 2^{45} unikátních prefixů, tj. 35,184,372,088,832 prefixů
 - H poměr ([RFC 1715](#)) – reálné využití adresového prostoru, obvykle 0.24-0.26
 - $H = \log_{10}(178\ 000\ 000\ 000)/45 = 0.25$
 - Při „standardním“ zaplnění lze bez problémů pokrýt 178 miliard unikátních prefixů (v roce 2050 je očekávána populace 10 mil., čili každý člověk může mít 17,8 prefixů délky /48)

Změny doporučení RFC3177

- Nepřidělovat /128, vždy minimálně /64
- Pevné délky doporučených prefixů (48 a 64) vedly k zadrátovaným implementacím (návrat ke classfull A/B/C), což nebylo záměrem, zdůraznit CIDR
- Stejný prefix délky /48 pro domácí sítě a velké sítě se ukazuje jako nepotřebný a komplikující:
 - Domácí sítě jsou obvykle ve vysokém počtu napojeny na stejného poskytovatele, prefix poskytovatele /32 dovoluje napojit 65535 sítí /48, což je málo
 - Domácí sítě sice mohou mít subnety (a je žádoucí to dovolit), nicméně 65535 subnetů je příliš
- **Doporučení:** volit pro **domácí sítě** delší prefix (např. /56)
- **Varování:** vzhledem k zápisu adres a reverznímu DNS není příliš vhodné volit jiné délky než násobek 4, lépe 8.

RIR

■ ARIN

- Návrh na doplnění pravidel
 - Standardně /48
 - Pokud má organizace více lokalit, do 10 lze přidělit /44, při větším počtu i /40

■ RIPE

- ripe-481 <http://www.ripe.net/ripe/docs/ripe-481.html>
 - LIR, ISP standardně /32
 - PI nejdelší /48
 - Doporučení pro LIR/ISP, při kratším prefixu než /48 pro jednu lokalitu zdůvodnění

Bod 6. Adresní plán

- Jak hospodařit s přiděleným prefixem /48?
- Předpoklad: prostředí metropolitních nebo campusních sítí (větší sítě propojovací i koncové)
- Požadavky:
 - Agregace (inzerce co nejkratších prefixů), čili zhruba podle fyzické topologie.
 - Dovolit růst, čili ponechat rezervy mezi alokacemi pro růst sítí (počet subnetů, ne počet uzlů).

Jak v praxi

- Máme IPv4 adresy a prefixy
 - Pokud jsou „rozumné“, lze použít jako základ pro alokaci IPv6 prefixů
 - Pokud ne, pak je lepší začít z čisté vody
- Příklad VUT:
 - Fakulty mají obvykle několik nesouvisejících IPv4 prefixů
 - Fakulta dostane /56 (čili 256 subnetů délky 64) číselně odpovídající prvnímu přidělenému IPv4 prefixu délky /24, dalších 15 se ponechá v rezervě

Jak dělit?

- Teoreticky známý a vyřešený problém ([Buddy systém](#)), jinak viz [ripe-343](#)
- Dělíme na poloviny a přidělujeme postupně vždy počáteční z dané poloviny (zbytek rezerva na růst)
- Sekvence alokací pro /48 děleno po /56 (doporučené dělení):
 1. 0, 128,
 2. 64, 192,
 3. 32, 96, 160, 224
 4. 16, 48, 80, 112, 144, 176, 208, 240
 5. 8, 24, ...
- Redukce fragmentace: pokud se předcházející blok blíží k zaplnění, tak tento nepřidělovat a ponechat jako rezervu

Praktický příklad

- Máme 3 areály A, B, C, A má 3 instutice a,b,c, B má 1 d, C má 4 e,f,g,h
 - počet nepřekročí 256, každá tedy dostane počátečně jeden /56, celkem potřebujeme 8 + infrastrukturu, rozdělíme tedy po 16 a rezervujeme pro každou 16 bloků /56
 - areály je třeba agregovat, rozdělíme blok na čtyři díly
 - areál A bude PFX:0000::/56 až PFX::3F00::/56
 - areál B bude PFX:4000::/56 až PFX::7F00::/56
 - areál C bude PFX:8000::/56 až PFX::BF00::/56
 - A.a dostane PFX:0000::/56, A.b – PFX:1000::/56, A.c – PFX:2000::/56
 - B.d dostane PFX:4000::/56
 - C.e dostane PFX:8000::/56, C.f – PFX:9000::/56, C.g – PFX:A000::/56, C.h – PFX:B000::/56

Příklad

- Za každým přidělením je rezerva 15 bloků /56
- pokud naroste počet institucí v areálu, posune se dělení o stupeň dále, rezerva bude jen 7 bloků:
 - A.m dostane PFX:0800::/56
 - atd.
- Pro infrastrukturu lze vyhradit poslední blok, spojky s prefixem **délky /64** začít naopak od konce:
 - PFX:FF00::/56
 - Kdo má více spojek než 255?
 - ND funguje i na NBMA sítích (Frame-Relay, ATM), problém ping-pong v koncových a metropolitních sítích nenastává (je to problém p2p sítí bez ND - PPP, Sonet, řeší ho aktuální ICMPv6 dle RFC4443 podle draft-ietf-ipngwg-p2p-pingpong, ale není většinou implementováno)

Další trendy

- Univerzální pravidlo – použij prefix /64
- Co s ND útoky a ping-pong?
 - implementovat RFC4443 (plné ND a neposílat pakety zpátky po stejném if odkud přišel) na p2p PPP
 - mnozí si spojují ND jen s link-layer adresou, to je omyl, ND má mnoho funkcí, v tomto případě je nutná detekce existence souseda, získání link-layer adresy je tady jen volitelným parametrem
 - 6loWPAN ND Optimization
 - preregistrace link-adresy v NC
 - nesystémové použití /127
- Pozn.: i když použijeme ručně konfigurované fixní adresy (třeba i link-local), na Ethernetu ND vždy běží a NC existuje!