Autokonfigurace IPv6 v lokální síti

Ondřej Caletka

cesnet

6. června 2018

Teoretický úvod

cesnet

IPv4 v lokální síti

- jedna adresa na rozhraní
- ruční konfigurace adres a směrování, později BOOTP a DHCP
- objevování sousedů samostatným protokolem ARP
- závislost na všesměrovém vysílání
  - multicast byl vyvinut později

cesnet

Problémy IPv4 v lokální síti

- broadcast storms – intenzivní všesměrové vysílání
  - velká zátěž pro všechny uzly
  - vyčerpání velké části kapacity linek
- stavové DHCP
  - síť si musí pamatovat, kterou adresu kdo použil
  - lze získat pouze jednu adresu
  - identifikátorem je adresa spojové vrstvy konkrétního rozhraní
- porušení vrstvového modelu
  - protokol aplikační vrstvy konfiguruje síťovou vrstvu

cesnet

Adresování v IPv6

síťová část

- 3 bity druh adresy (unicast, multicast – prefix /3)
- 9 bitů identifikace RIR (prefix /12)
- 17 – 20 bitů identifikace LIR (prefix /29 – /32)
- 16 – 27 bitů identifikace koncového uživatele (prefix /48 – /56)
- 8 – 16 bitů identifikace podsítě (prefix /64)

identifikátor rozhraní

- určuje zařízení v podsíti
- náhodné číslo
- dříve odvozované z MAC adres

- záměrně extrémně řídký adresní prostor
- síťová zařízení mají zakázáno *předpokládat* určitou délku prefixu

cesnet

Druhy IPv6 adres

`::1/128` loopback

`2000::/3` globální unikátní

`fe80::/10` linkové lokální

- dosah pouze v rámci linky
- je třeba doplňovat názvem rozhraní (`fe80::2%eth0`)

`fc00::/7` unikátní lokální

- v praxi `fdxx:xxxx:xxxx::/48` (40 bitů náhodných)
- snaha eliminovat kolidující IP rozsahy

`ff00::/8` skupinové – čtvrtý znak určuje dosah

`ff02::/16` linka
`ff08::/16` organizace
`ff0e::/16` globální

cesnet

IPv6 v lokální síti

- více adres na rozhraní
- link-local IPv6 adresa k dispozici nezávisle na okolí
- objevování sousedů součástí ICMPv6
  - s využitím linkového multicastu
- objevování směrovačů součástí ICMPv6
  - lze použít i pro konfiguraci IP adresy

cesnet

Objevování IPv6 sousedů

- funkce ICMPv6 protokolu
- odpovídá ARP zprávám

  Neighbor solicitation Kdo má danou IPv6 adresu?
  Neighbor advertisment Já mám takovouto IPv6 adresu!
- šíří se multicastem do **skupiny pro vyzývaný uzel**
  - adresa `ff02::1:ffxx:xxxx`
  - posledních 24 bitů shodných s IPv6 adresou
  - navrženo, aby:
    - počet počítačů ve skupině byl blízký jednomu
    - počet skupin, ve kterých musí být jeden počítač, byl blízký jedné
  - síť má data k **efektivnímu doručování zpráv** bez nutnosti všesměrového vysílání

cesnet

Připojení do sítě krok za krokem

1. vytvoří se link-local adresa `fe80::<interface id>`
2. přihlásí se multicastová skupina pro vyzývaný uzel
3. ověří se unikátnost link-local adresy
4. pošle se výzva směrovačům

cesnet

Link-local adresy

- prefix `fe80::` spojený s identifikátorem rozhraní
- jsou k dispozici vždy, na každém aktivním rozhraní
- platí pouze s uvedením rozhraní (*scoped address*)
- používají se pro následnou servisní komunikaci
- je možné je používat k libovolné komunikaci v rámci linky
- vždy jde o přímo připojená zařízení, nelze komunikovat přes směrovač
  - zároveň jde o jediné adresy, které jsou **garantovaně přímo připojené**

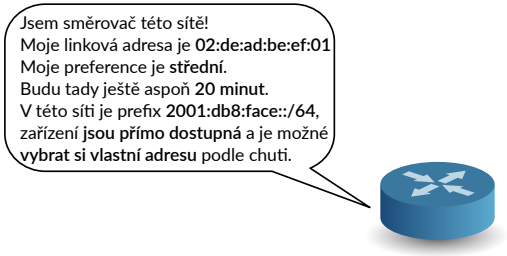
cesnet

Objevování IPv6 směrovačů

Router solicitation Je v této síti nějaký směrovač?

Router advertisment Já jsem směrovač a mám toto nastavení.

- funkce ICMPv6 protokolu
- směrovač pravidelně zasílá do sítě:
  - svou adresu spojové vrstvy, životnost a preferenci
  - volitelně informace o prefixech a jejich dostupnosti
  - další volby (MTU, směrování, adresy DNS serverů)
- všechna zařízení nastavují směrování



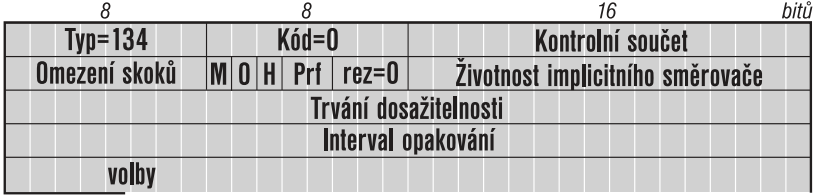
cesnet

Reakce na ohlášení směrovače

- směrovač je přidán do seznamu směrovačů
  - ve směrovací tabulce se objeví výchozí brána
  - předpokládá se, že směrovačů může být víc
  - koncový systém automaticky vyhodnocuje (ne-)dostupnost směrovače
- časovače životnosti se resetují
- příznaky pro DHCPv6

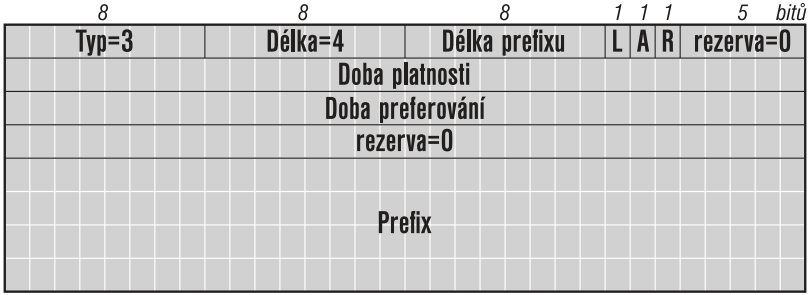
  Managed spustí získávání adresy pomocí DHCPv6

  Other config informuje o přítomnosti bezestavového DHCPv6



Obrázek: Pavel Satrapa – IPv6, 3. vyd., CZ.NIC Praha 2011

Zpracování volby síťového prefixu



on-Link prefix se do směrovací tabulky zapíše jako přímo dostupný

Autonomous prefix se použije pro bezestavovou autokonfiguraci (SLAAC)

Obrázek: Pavel Satrapa – IPv6, 3. vyd., CZ.NIC Praha 2011

cesnet

rdisc6 eth0

```
Dožaduji se ff02::2 (ff02::2) na eth0…

Hop limit                 :           64 (      0x40)
Stavová konfigurace adres :          Ano
Stavová další konfigurace :          Ano
Přednost routeru          :       střední
Životnost routeru         :         1800 (0x00000708) sekund
Doba dosažitelnosti       :     neurčeno (0x00000000)
Doba pro znovuvyslání     :     neurčeno (0x00000000)
 Linková adresa zdroje    : D8:58:D7:00:0B:1D
 MTU                      :        1500 bajtů (platné)
 Předpona                 : 2001:db8:1::/64
  Doba platnosti          :         7200 (0x00001c20) sekund
  Upřednostňovat po dobu  :         1800 (0x00000708) sekund
 Rekurzivní DNS server    : 2001:db8:1::1
  Životnost DNS serveru   :         1200 (0x000004b0) sekund
 od fe80::da58:d7ff:fe00:b1d
```

ip -6 route

```
2001:db8:1::/64 dev eth0 proto ra metric 203 mtu 1500 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev wlan0 proto kernel metric 256 pref medium
default via fe80::da58:d7ff:fe00:b1d dev eth0 proto ra metric 203
        mtu 1500 pref medium expires 1709sec
default via fe80::da58:d7ff:fe00:b1d dev wlan0 proto ra metric 302
        mtu 1500 pref medium expires 1651sec
```

- přímo dostupný prefix pro ohlášky s příznakem L
- přímo dostupné *link-local* adresy na všech rozhraních
- výchozí cesta směrovačem
  - prostřednictvím *link-local* adresy
  - s omezenou životností podle ohlášky

cesnet

Konfigurace IP adresy

- **nezávislá na nastavení směrování**
- různé způsoby se **vzájemně nevylučují**
- výsledkem je vždy **jen IP adresa** (/128)
  - „maska podsítě“ je nastavena z ohlášení směrovačů

SLAAC bezestavová autokonfigurace
- aktivováno příznakem `A` ve volbě prefixu
- k síťovému prefixu se připojí identifikátor rozhraní

DHCPv6 přidělení **jedné** IPv6 adresy
- aktivováno příznakem `M` v ohlášení směrovače
- proces obdobný DHCPv4, ale bez nastavení masky a brány

cesnet

ip -6 addr

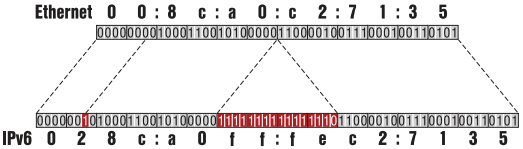
```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 state UNKNOWN qlen 1000
    inet6 ::1/128 scope host
2: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP qlen 1000
    inet6 2001:db8::cafe/128 scope global
       valid_lft forever preferred_lft forever
    inet6 2001:db8::e8b:fdff:fe60:e9b/64 scope global dynamic
       noprefixroute valid_lft 7051sec preferred_lft 1651sec
    inet6 fe80::e8b:fdff:fe60:e9b/64 scope link
       valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP qlen 1000
    inet6 2001:db8:1::cafe/128 scope global
       valid_lft forever preferred_lft forever
    inet6 2001:db8:1::f21f:afff:fe4a:5c54/64 scope global dynamic
       valid_lft 7109sec preferred_lft 1709sec
    inet6 fe80::f21f:afff:fe4a:5c54/64 scope link
       valid_lft forever preferred_lft forever
```

Tvorba identifikátoru rozhraní

1. vázaný na adresu spojové vrstvy
2. náhodné číslo bez vztahu k HW
3. v čase proměnlivé náhodné číslo
   - RFC 4941 privacy extensions
   - nejčastější chování klientských zařízení
   - náročné na správu i kapacity
4. v čase stabilní náhodné číslo
   - RFC 7217 stable private IPv6
   - v dané podsíti je adresa stabilní, v jiných sítích zcela jiná

Nejčastější varianty

Windows	3 + 2
Linux	3 + 1
Linux – dhcpcd	4
Embedded HW	1



Obrázek: Pavel Satrapa – IPv6, 3. vyd., CZ.NIC Praha 2011

cesnet

DHCPv6

- obdoba tradičního protokolu z IPv4
- identifikace nodů pomocí DHCP Unique IDentifier
  - unikátní identifikátor **pro celý počítač**
  - nezávislý na konkrétním síťovém hardwaru (funguje i třeba nad PPP)
  - obvykle vygenerovaný při prvním startu OS
  - obtížně měnitelný
- nepovinná podpora, záměrně **nepodporováno v OS Android**

Stavové DHCP	server spravuje databázi zápůjček
Bezestavové DHCP	jednoduchý dotazovací protokol pro nejrůznější konfigurační volby (DNS, NTP, proxy,…)

cesnet

Výhody DHCPv6

- možnost používat krátké adresy
- možnost přidělovat **celé prefixy** pro domácí síť
- široká podpora pro bezestavový režim (širší než pro volby směrovačů)

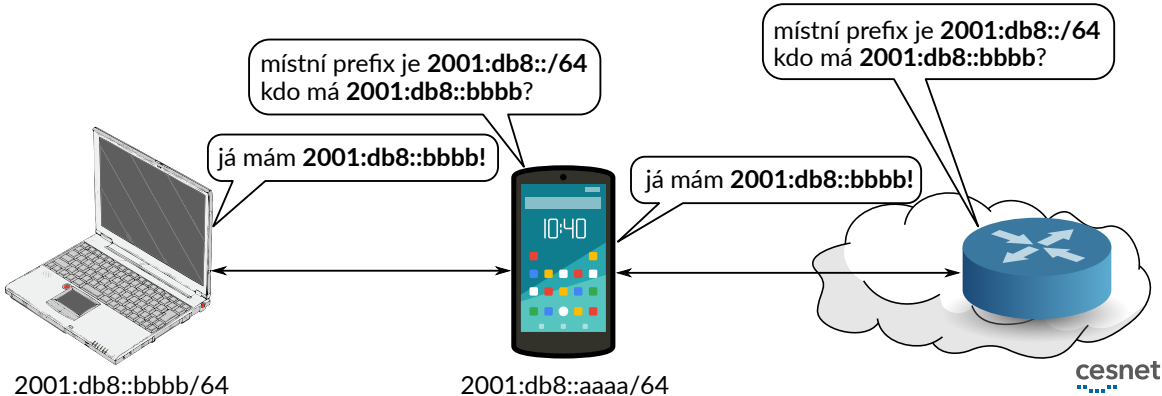
Nevýhody DHCPv6

- problematická identifikace stanic, neslučitelná s IPv4
- přiděluje pouze **jednu** IPv6 adresu
- podpora není vyžadována pro koncové zařízení

cesnet

Proč nestačí jedna IPv6 adresa?

- **virtualizace**
- přechodové mechanizmy (464XLAT)
- **tethering** (pseudobridge / Proxy NDP)



Praktické zkušenosti

cesnet

Problematický multicast

- nejasné standardy, speciálně pro linkový multicast
- ohromné množství stavů, které síť musí držet → DoS potenciál
- většina síťových zařízení přistupuje k linkovému multicastu jako k broadcastu
- chyby v klientských zařízeních

Příklad chybné signalizace multicastu

- mobil po probuzení neodešle MLD zprávy o členství ve skupinách
- přepínač během spánku začal filtrovat skupinu pro vyzývaný uzel
- směrovač potřebuje obnovit záznam v tabulce sousedů
- NDP zprávy jsou přepínačem zahozeny

cesnet

Velká spotřeba baterie

- problém velkých Wi-Fi sítí
- každé nové zařízení pošle výzvu směrovači
- směrovač odpoví všem zařízením v síti
- všechna zařízení upraví svou konfiguraci

Zmírňování následků

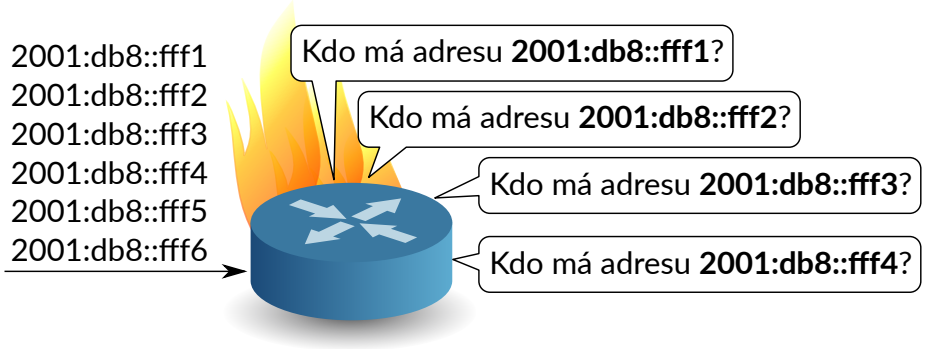
- ohlášení pouze konkrétnímu zařízení
- omezení četnosti pravidelných ohlášek
- filtrování multicastů ve firmwarech zařízení (**špatný nápad**)
  - typicky optimalizované pro funkci IPv4
  - často vede k vypršení platnosti směrovače a nefunkčnosti IPv6

cesnet

RFC 7772 – Reducing Energy Consumption of Router Advertisements

Příliš velký adresní prostor

- většina adres je neobsazených
- objevování sousedů je netriviální úloha
- stačí poslat data na neobsazené IPv6 adresy
- v praxi menší problém, než se předpokládalo



cesnet

Nezabezpečená spojová vrstva

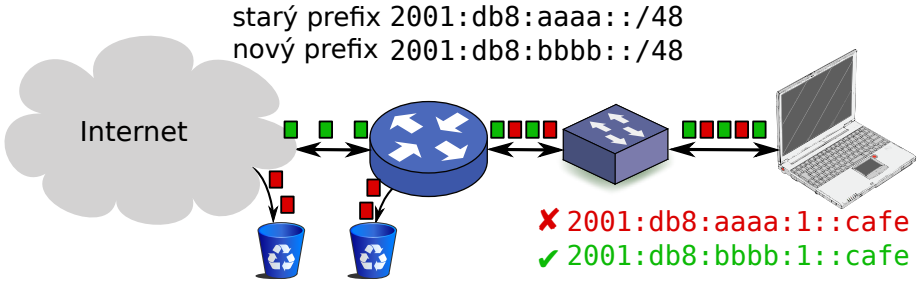
- **stejný problém jako u IPv4**
- kdokoli se může prohlásit směrovačem
- kdokoli může ukrást něcí adresu
- protiopatření **nejsou dokonalá**
- standardy jako SeND (*Secure Neighbor Discovery*) nejsou běžně podporovány
- ideálním řešením je **mikrosegmentace**
  - nepřipustit sdílení spojové vrsty
  - směrovače namísto přepínačů
  - obtížná kompatibilita s IPv4

Wilhelm Boeddinghaus – IPv6 in Enterprise Network: Advanced Topics

cesnet

Potíže při předadresování

- mezi adresou a branou není přímá vazba
- brána musí aktivně anulovat starou adresu, jinak bude koncové zařízení používat starou adresu nadále
- problém např. při ztrátě napájení CPE



cesnet

Potíže při přeadresování

- teoreticky vyřešeno pravidlem novým pravidlem výběru zdrojové adresy
- k uplatnění daného pravidla musí zařízení evidovat, který směrovač ohlašoval které prefixy, což **není povinné**

Výběr adresy odesílatele podle RFC 6724

Pravidlo 5.5: Preferuj adresy z prefixů ohlašovaných použitou bránou.
Pokud je prefix adresy A přidělen použitou branou a prefix adresy B je přidělen jinou branou, preferuj adresu A. Obdobně, je-li prefix adresy B přidělen použitou branou a prefix adresy A jinou branou, preferuj adresu B.

cesnet

Shrnutí

cesnet

Shrnutí

- existuje **jediný způsob** automatické konfigurace směrování
- jako brány vždy vystupují **link-local adresy**
- konfigurace adres je **zcela nezávislá** na konfiguraci směrování
- DHCPv6-only se hodí jen do uzavřené, kontrolované sítě
- multicast nefunguje tak dobře, jak se čekalo
- **mikrosegmentace** eliminuje zranitelnosti spojové vrstvy

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**

Prezentace je již nyní k dispozici ke stažení.