5 Objevování sousedů (Neighbor Discovery)

Jedním z dobře známých problémů počítačových sítí je zjištění linkové adresy partnera. Počítač potřebuje poslat někomu data, zná jeho IP adresu, podle ní také ví, že spolu sídlí v jedné lokální síti (řekněme Ethernetu). Aby mu však mohl odeslat paket, potřebuje znát právě cílovou ethernetovou adresu.

IPv4 k tomuto účelu používá samostatný protokol nazvaný Address Resolution Protokol (ARP). V zásadě funguje tak, že odesílající rozešle na všesměrovou IP adresu 255.255.255.255 (všechny stroje v lokální síti) ARP dotaz „Kdo z vás má IP adresu XY?“ Šťastný vlastník mu pak odpoví „To jsem já a moje ethernetová adresa je HyChyKyRyDyTyNy.“

U IPv6 se rozhodli dotyčný mechanismus definovat přímo jako jednu ze základních součástí IP. A když už byli v té revoluci, rovnou vytvořili obecnější nástroj, který kromě hledání linkových adres řeší ještě celou řadu dalších problémů. Výsledek nazvali *objevování sousedů (Neighbor Discovery, ND)*. Slouží k následujícím účelům:

- zjišťování linkových adres uzlů ve stejné lokální síti
- rychlé aktualizace neplatných položek a zjišťování změn v linkových adresách
- hledání směrovačů
- přesměrování
- zjišťování prefixů, parametrů sítě a dalších údajů pro automatickou konfiguraci adresy
- ověřování dosažitelnosti sousedů
- detekce duplicitních adres

Vše je definováno v RFC 4861: *Neighbor Discovery for IP version 6*. Pro svou činnost využívá pěti typů ICMP zpráv, dvě další k nim přidává zabezpečení nazvané SEND. Jejich přehled najdete v tabulce 5.1. V této kapitole popíši jen aspekty související se zjišťováním linkových adres a testováním dosažitelnosti. Automatické konfiguraci (do níž spadá většina ostatních součástí objevování sousedů) věnuji samostatnou kapitolu.

Objevování sousedů	
výzva směrovači	router solicitation
ohlášení směrovače	router advertisement
výzva sousedovi	neighbor solicitation
ohlášení souseda	neighbor advertisement
přesměrování	redirect
SEND	
žádost o certifikační cestu	certification path solicitation
ohlášení certifikační cesty	certification path advertisement

Tabulka 5.1: Typy ICMP zpráv pro objevování sousedů

5.1 Hledání linkových adres

Zjišťování linkové adresy na základě IP se velmi podobá klasickému ARP. Změnily se vlastně jen názvy a především adresa, na kterou tazatel zasílá svůj dotaz.

adresa vyzývaného uzlu

Pro potřeby objevování sousedů byl definován hlouček skupinových adres, na něž se rozesílají dotazy. Všechny mají společný prefix

ff02:0:0:0:0:1:ff00::/104

Uzel, který hledá linkovou adresu pro určitou IPv6 adresu, vezme posledních 24 bitů z hledané IP adresy a připojí je za výše uvedený prefix. Tím získá skupinovou adresu, na kterou zašle svůj dotaz. Takže pokud například hledá linkovou adresu pro

2001:db8:1:1:022a:fff:fe32:5ed1

bude se ptát na skupinové adrese

ff02::1:ff32:5ed1

V terminologii IPv6 se takové adrese říká *adresa pro vyzývaný uzel (solicited node address)*. Skutečnost, že z hledané adresy se přebírá jen spodních 24 bitů, zmenšuje počet skupin, v nichž každý počítač musí být členem. Pokud si vzpomenete na kapitolu 3 na straně 55, IP adresy jsou konstruovány tak, že spodních 64 bitů vychází z identifikátoru rozhraní a k nim je připojen prefix pro horních 64 bitů. Totéž rozhraní může být zařazeno do několika sítí s různými prefixy, nicméně závěrečnou část adresy bude mít stále stejnou. To znamená, že všechny jeho IP adresy budou mít stejnou adresu vyzývaného uzlu.

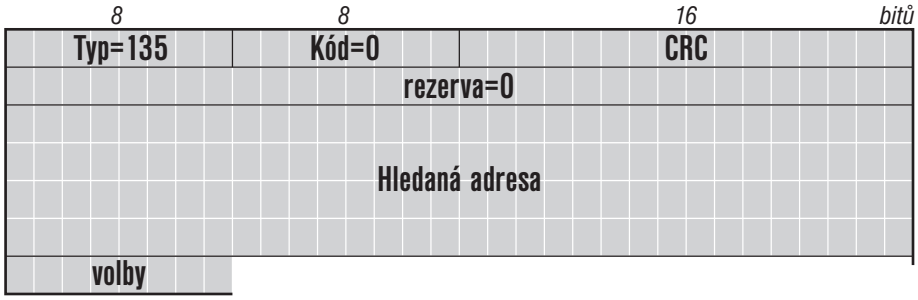
Aby objevování sousedů fungovalo, musí počítač při inicializaci IP pro síťové rozhraní vstoupit do všech skupin odpovídajících adresám vyzývaného uzlu pro všechny adresy přidělené rozhraní. Díky popsanému mecha-

nismu bude zpravidla jen jedna, protože vychází z identifikátoru rozhraní, který bývá ve všech adresách stejný[1]. Na druhé straně jsou závěrečné tři bajty dostatečně dlouhé na to, aby ve skupině pro vyzývaný uzel byl zpravidla každý sám. I ve velmi velkých sítích najdete jen vzácně dvojice karet se shodnou hodnotou poslední trojice bajtů. To v praxi znamená, že při hledání linkové adresy nejsou zbytečně obtěžováni ostatní a zpravidla se osloví jen samotný její vlastník.

hledání adresy

Pokud tedy počítač (dále mu budeme říkat „vyzyvatel“) shání linkovou adresu jiného, u nějž zná pouze IP adresu, postupuje následovně: Z cílové IP adresy vytvoří výše popsaným postupem skupinovou adresu vyzývaného uzlu. Na ni pošle speciální typ ICMP zprávy nazvaný *Výzva sousedovi*. Pokud je počítač s danou IP adresou aktivní, bude zapojen do příslušné skupiny a výzvu obdrží. Reaguje na ni *Ohlášením souseda*, které pošle vyzyvateli a které obsahuje informace o jeho linkové adrese.

Každý uzel by si měl udržovat interní datovou strukturu nazvanou *cache sousedů*, ve které má uloženy jejich linkové adresy. Na základě příchodu ohlášení souseda si do této cache zanese novou položku s jeho IP adresou a odpovídající linkovou adresou.



Obrázek 5.1: Výzva sousedovi

výzva sousedovi

Formát *Výzvy sousedovi* znázorňuje obrázek 5.1. V podstatě obsahuje jedinou informaci – *Hledanou adresu (Target address)*, k níž odesilatel výzvy shání linkovou. K datagramu může připojit volbu, která ohlašuje jeho vlastní linkovou adresu, aby adresát výzvy rovnou věděl, kam má odpovědět.

Obrázek 5.2: Volba *Linková adresa odesilatele*

[1] Pokud ale stroj používá adresy zachovávající soukromí, mají jeho adresy různé spodní poloviny a tím pádem bude členem více vyzývaných skupin.