

IPv4 překlad adres (NAT)

Tato prezentace seznamuje studenty s problematikou překladu IP adres (NAT – Network Address Translation) v prostředí IPv4. Vysvětluje základní motivaci k nasazení NAT, představuje různé typy NAT (SNAT, DNAT, PAT), ukazuje jejich fungování a vliv na komunikaci. Rozebírá také hlavní výhody i nevýhody NAT a nastiňuje vztah mezi NAT a IPv6.

Úvod do NAT

Motivace pro NAT

- Vyčerpání veřejných IPv4 adres – díky NATu mohou desítky až stovky zařízení sdílet jedinou veřejnou IPv4 adresu.
- Skrytí vnitřní sítě (soukromé adresy RFC 1918) – z hlediska internetu se jeví, jako by celý provoz šel z jedné veřejné IP.

Základní princip

- NAT zařízení (typicky router nebo firewall) přepíše IP adresu v IP hlavičce a udržuje tabulku spojení, aby data mohla proudit správným směrem zpět.

Typy NAT

Statický NAT (One-to-One)

- Každá soukromá adresa je napevno namapována na veřejnou adresu.
- Používá se, pokud potřebujete mít veřejně dostupný server (např. webový server) a chcete mu přiřadit veřejnou IP.
- Nevýhoda: potřeba mít dostatek veřejných IP adres.

Dynamický NAT

- Skupina (pool) veřejných adres přidělována dynamicky vnitřním hostům.
- Stále se vyžaduje dostatečné množství veřejných IP, ale ne fixní mapování.

Overloading – PAT (Port Address Translation)

- Nejčastěji využívaný typ NAT (označován jako NAT s překladem portů).
- Mnoho vnitřních soukromých adres sdílí jednu veřejnou IP s různými porty.
- Efektivní řešení – dovolí stovkám zařízení fungovat „navenek“ s jedinou veřejnou IP adresou.

Základní pojmy

Inside (vnitřní) vs. Outside (vnější)

- **Inside local address:** adresa zařízení v soukromé síti.
- **Inside global address:** adresa, pod kterou je zařízení vidět zvenku (veřejná).
- **Outside local address:** adresa cílového serveru z pohledu vnitřní sítě (obvykle shodná s outside global).
- **Outside global address:** reálná veřejná adresa cílového serveru.

NAT tabulka

- Zařízení si ukládá mapování (např. 192.168.0.10:12345 ↔ 203.0.113.5:56789), aby vědělo, kam přeposlat odpovědi.

Příklad Overload NAT (PAT)

Schéma

- Uživatel má PC s adresou 192.168.1.100 (port 50000).
- Router má vnější IP 198.51.100.10.
- Při odchozí komunikaci do internetu router zapíše do NAT tabulky:
 - **Inside local** 192.168.1.100:50000 → **Inside global** 198.51.100.10:62000 (příklad portu).
- Vnější server 1.2.3.4 vrátí data na 198.51.100.10:62000, router ví, že to patří PC 192.168.1.100:50000.

Poznámka

- Port je klíčový pro rozlišení více stanic, které sdílí stejnou veřejnou IP.

Výhody a nevýhody NAT

Výhody

- Šetření veřejných IPv4 adres.
- Základní skrytí vnitřní sítě (z hlediska bezpečnosti to není plnohodnotný firewall, ale ztěžuje přímý přístup zvenku).
- Snadné připojení více zařízení k internetu bez nutnosti nákupu více veřejných IP.

Nevýhody

- Narušení end-to-end principu internetu (každý host nemá globálně jedinečnou IP).
- Komplikace pro některé aplikace (VoIP, P2P, IPsec VPN), které potřebují přímé spojení.
- Musí se řešit NAT traversal (UPnP, NAT-PMP, manuální port forwarding) pro příchozí spojení.

Port Forwarding (DNAT)

Definice

- Umožňuje mapovat konkrétní port (např. 80) na vnitřní server (např. 192.168.0.50:80).
- Též nazýváno DNAT (Destination NAT), protože se mění cílová adresa nebo port.

Příklad

- Mám server s privátní adresou 192.168.0.50, chci, aby byl dostupný z internetu na portu 80.
- Na routeru nastavím forward: **Outside global** 198.51.100.10:80 → **Inside local** 192.168.0.50:80.
- Uživatel z internetu zadá 198.51.100.10, zobrazí se stránka z vnitřního serveru.

NAT a IPv6

Budoucnost NATu

- IPv6 díky obrovskému adresnímu prostoru eliminuje nutnost NAT k šetření adres.
- Nicméně v praxi se někdy používá i NAT66 (z bezpečnostních/důvodů správy), ale není to tak rozšířené ani nutné jako u IPv4.

Dual-stack sítě

- Mnoho sítí provozuje současně IPv4 NAT (kvůli vyčerpání IPv4) a zároveň IPv6 (napřímo bez NAT).

Shrnutí

NAT (Network Address Translation) je klíčový mechanismus, který umožňuje sdílet omezené množství **veřejných IPv4 adres** v době jejich nedostatku.

Existují **různé typy**: statický NAT, dynamický NAT a nejčastěji používaný **PAT (Overload)**, který dovoluje mnoha zařízením používat **jedinou veřejnou IP** s odlišením přes porty.

DNAT / Port forwarding je způsob, jak z internetu zpřístupnit služby ve vnitřní síti.

NAT **má i nevýhody** – narušuje end-to-end princip a může ztěžovat provoz aplikací, které vyžadují přímou komunikaci.

S příchodem **IPv6** lze NAT z velké části nahradit nativní adresací, avšak IPv4 NAT stále zůstává důležitý v mnoha sítích.

Kontrolní otázky

1. Proč se NAT prosadil a jaký problém v IPv4 částečně řeší?
2. Jaký je rozdíl mezi statickým NATem a PAT (Port Address Translation)?
3. Co se rozumí pojmy *Inside local address* a *Inside global address*?
4. Jak funguje „port forwarding“ a v jaké situaci se používá?
5. Jaké problémy může NAT způsobovat pro některé síťové aplikace (např. VoIP, P2P)?
6. Proč se v IPv6 předpokládá menší potřeba NAT a proč přesto v určitých případech zůstává?

Doporučená literatura

- 1. Tanenbaum, A. S., Wetherall, D.:** *Počítačové sítě*, 5. vydání (česky) – Kapitoly o IPv4, NAT.
- 2. Kurose, J. F., Ross, K. W.:** *Computer Networking: A Top-Down Approach* – Část o NAT a protokolech v IPv4.
- 3. Cisco Networking Academy:** *CCNA materiály* – Přehledná vysvětlení konfigurace NAT/PAT.
- 4. RFC 3022** – *Traditional IP Network Address Translator (Traditional NAT)*.
- 5. Oficiální dokumentace výrobců routerů** (např. Cisco, MikroTik) – Praktická konfigurace NATu a příklady.