Počítačové sítě 2

Jan Outrata

KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLOMOUCI

přednášky

Network Address Translation (NAT)

Úvod

- pro (tzv. koncovou, přímou) komunikaci v IP síti, např. Internetu, potřebuje zařízení **IP adresu** – unikátní v celé síti
  - IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP), vyčerpaný omezený celkový adresní prostor
  - částečné řešení: dynamické adresy jen pro aktuálně připojená odpojovaná zařízení – např. v mobilních sítích, v LAN DHCP
  - (trvalé?) řešení: IPv6 – „neomezený“ adresní prostor, ale pomalý přechod z IPv4
  - „trvalé“ „řešení“?!: **Network Address Translation (NAT)**

Úvod

- pro (tzv. koncovou, přímou) komunikaci v IP síti, např. Internetu, potřebuje zařízení **IP adresu** – unikátní v celé síti
  - IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP), vyčerpaný omezený celkový adresní prostor
  - částečné řešení: dynamické adresy jen pro aktuálně připojená odpojovaná zařízení – např. v mobilních sítích, v LAN DHCP
  - (trvalé?) řešení: IPv6 – „neomezený“ adresní prostor, ale pomalý přechod z IPv4
  - „trvalé“ „řešení“?!: **Network Address Translation (NAT)**

= **překlad IP adres** = přepisování v IP paketech libovolných adres v LAN na přidělené adresy v síti ISP a opačně – **basic (one-to-one) NAT**, mnoho RFC

- původně pro odstranění potřeby změny adres při změně (sítě) ISP
- téměř výhradně pro IPv4 (ale pro IPv6 experimentální Network Prefix Translation, NPTv6)

Úvod

- pro (tzv. koncovou, přímou) komunikaci v IP síti, např. Internetu, potřebuje zařízení **IP adresu** – unikátní v celé síti
  - IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP), vyčerpaný omezený celkový adresní prostor
  - částečné řešení: dynamické adresy jen pro aktuálně připojená odpojovaná zařízení – např. v mobilních sítích, v LAN DHCP
  - (trvalé?) řešení: IPv6 – „neomezený“ adresní prostor, ale pomalý přechod z IPv4
  - „trvalé“ „řešení“?!: **Network Address Translation (NAT)**

= **překlad IP adres** = přepisování v IP paketech libovolných adres v LAN na přidělené adresy v síti ISP a opačně – **basic (one-to-one) NAT**, mnoho RFC

- původně pro odstranění potřeby změny adres při změně (sítě) ISP
- téměř výhradně pro IPv4 (ale pro IPv6 experimentální Network Prefix Translation, NPTv6)

- pro LAN vyhrazené **rozsahy IPv4 adres pro privátní sítě** (RFC 1918): 10./8, 172.16./12, 192.168./16 – pakety s nimi se nesměrují, „platné“ pouze v LAN, tzv. **privátní**

Úvod

- pro (tzv. koncovou, přímou) komunikaci v IP síti, např. Internetu, potřebuje zařízení **IP adresu** – unikátní v celé síti
  - IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP), vyčerpaný omezený celkový adresní prostor
  - částečné řešení: dynamické adresy jen pro aktuálně připojená odpojovaná zařízení – např. v mobilních sítích, v LAN DHCP
  - (trvalé?) řešení: IPv6 – „neomezený“ adresní prostor, ale pomalý přechod z IPv4
  - „trvalé“ „řešení“?!: **Network Address Translation (NAT)**

= **překlad IP adres** = přepisování v IP paketech libovolných adres v LAN na přidělené adresy v síti ISP a opačně – **basic (one-to-one) NAT**, mnoho RFC

- původně pro odstranění potřeby změny adres při změně (sítě) ISP
- téměř výhradně pro IPv4 (ale pro IPv6 experimentální Network Prefix Translation, NPTv6)

- pro LAN vyhrazené **rozsahy IPv4 adres pro privátní sítě** (RFC 1918): 10./8, 172.16./12, 192.168./16 – pakety s nimi se nesměrují, „platné“ pouze v LAN, tzv. **privátní**
- **carrier-grade/large-scale NAT (CGN/LSN)**: privátní adresy i v síti ISP, NAT mezi LAN a ní i mezi ní a sítí jeho ISP2, vyhrazený rozsah pro ISP (RFC 6598): 100.64./10

Překlad adres

- obvykle provádí (hraniční, přístupový) směrovač mezi LAN a sítí ISP – pro ni LAN $\sim$ koncový uzel v ní, „skrytí“ LAN za adresu (příp. více)
- adresa v LAN se při překladu neukládá např. do (záhlaví) paketu
- přidělených, tzv. **veřejných**, adres v síti ISP pro LAN je typicky méně než (privátních, současně „komunikujících“) v LAN

Překlad adres

- obvykle provádí (hraniční, přístupový) směrovač mezi LAN a sítí ISP – pro ni LAN ∼ koncový uzel v ní, „skrytí“ LAN za adresu (příp. více)
- adresa v LAN se při překladu neukládá např. do (záhlaví) paketu
- přidělených, tzv. **veřejných**, adres v síti ISP pro LAN je typicky méně než (privátních, současně „komunikujících“) v LAN

→ přepis **adresy a portu** – TCP/UDP (NAPT, PAT), z TCP spojení nebo výměny UDP datagramů (adresa socketu), **one-to-many NAT**

1. při přeposlání (úvodního) paketu jedním směrem uložení překládané adresy a porty v LAN a v síti ISP do **NAT translation table**
2. využití záznamu u dalších paketů v rámci spojení/výměny (pro stejný překlad) a u paketů opačným směrem (pro opačný překlad)!

Překlad adres

Obrázek z knihy
zdroj: KR 4.25

Source NAT (SNAT)

= překlad (privátní) zdrojové adresy a portu u paketů z LAN do sítě ISP a (veřejné) cílové u paketů zpět

- dynamický: dynamicky náhodná nová adresa (z více) a port v síti ISP (port volný)
- **maškaráda** („NAT“) = jediná (veřejná) adresa v síti ISP
- ne plně standardizované metody překladu ⇒ různé (nedokumentované) implementace se specifickým chováním:
  - **full/address+port restricted-cone (in/dependent filtering)**: pakety zpět jen ze (zdrojové) adresy a portu jakýchkoliv / takových, na které (cílové) šel úvodní paket (jen adresu nebo obojí)
  - **symetrický (dependent mapping)**: pro různé cílové adresy a porty různý překlad, jen u restricted cone
  - ponechat při překladu stejný (zdrojový) port?, kdy a jak (dynamicky) změnit překlad? aj.

Destination NAT (DNAT)

= překlad (veřejné) cílové adresy a portu u paketů ze sítě ISP do LAN a (privátní) zdrojové u paketů zpět

- **přesměrování portu (port forwarding)** = stejný (cílový) port
- pro pakety z LAN (na veřejnou adresu) potřeba i SNAT! = **NAT loopback/reflection/hairpinning**
- rozložení zátěže (load distribution): dynamicky vybraná nová adresa v LAN z více

Problémy/kontroverze

- narušení **koncové (end-to-end) komunikace** – přenos dat jedním směrem není možný dokud není zahájený druhým, do té doby neznámé (veřejné) adresy
  - problém pro některé služby, např. A/V telefonie, P2P sítě, navíc pokud protokol používá přepisovanou (privátní) IP adresu a/nebo TCP/UDP port → náročný **protocol tracking** a překlad „v datech“
  - → veřejná proxy/relay (např. SOCKS), DNAT (port triggering), metody **NAT traversal** (NAT-T, RFC 5389): (TCP/UDP/ICMP) hole punching, STUN, TURN, ICE, UPnP IGDP, NAT-PMP, PCP, predikce adresy a portu v síti ISP (u symetrického SNAT) aj.

Problémy/kontroverze

- narušení **koncové (end-to-end) komunikace** – přenos dat jedním směrem není možný dokud není zahájený druhým, do té doby neznámé (veřejné) adresy
  - problém pro některé služby, např. A/V telefonie, P2P sítě, navíc pokud protokol používá přepisovanou (privátní) IP adresu a/nebo TCP/UDP port → náročný **protocol tracking** a překlad „v datech“
  - → veřejná proxy/relay (např. SOCKS), DNAT (port triggering), metody **NAT traversal** (NAT-T, RFC 5389): (TCP/UDP/ICMP) hole punching, STUN, TURN, ICE, UPnP IGDP, NAT-PMP, PCP, predikce adresy a portu v síti ISP (u symetrického SNAT) aj.
- narušení **unikátnosti identifikace zařízení** připojeného k Internetu (IP adresou) – „sdílejí“ adresu v síti ISP, v různých LAN mohou mít stejné, rozšíření na adresu a port

Problémy/kontroverze

- narušení **koncové (end-to-end) komunikace** – přenos dat jedním směrem není možný dokud není zahájený druhým, do té doby neznámé (veřejné) adresy
  - problém pro některé služby, např. A/V telefonie, P2P sítě, navíc pokud protokol používá přepisovanou (privátní) IP adresu a/nebo TCP/UDP port → náročný **protocol tracking** a překlad „v datech“
  - → veřejná proxy/relay (např. SOCKS), DNAT (port triggering), metody **NAT traversal** (NAT-T, RFC 5389): (TCP/UDP/ICMP) hole punching, STUN, TURN, ICE, UPnP IGDP, NAT-PMP, PCP, predikce adresy a portu v síti ISP (u symetrického SNAT) aj.
- narušení **unikátnosti identifikace zařízení** připojeného k Internetu (IP adresou) – „sdílejí“ adresu v síti ISP, v různých LAN mohou mít stejné, rozšíření na adresu a port
- proměna Internetu z **nespojované (IP) sítě** na „jakousi“ spojovanou – udržování překladů (tj. stavů) pro TCP spojení nebo výměny UDP datagramů, jejich závislost na existenci překladů

Problémy/kontroverze

- narušení **koncové (end-to-end) komunikace** – přenos dat jedním směrem není možný dokud není zahájený druhým, do té doby neznámé (veřejné) adresy
  - problém pro některé služby, např. A/V telefonie, P2P sítě, navíc pokud protokol používá přepisovanou (privátní) IP adresu a/nebo TCP/UDP port → náročný **protocol tracking** a překlad „v datech“
  - → veřejná proxy/relay (např. SOCKS), DNAT (port triggering), metody **NAT traversal** (NAT-T, RFC 5389): (TCP/UDP/ICMP) hole punching, STUN, TURN, ICE, UPnP IGDP, NAT-PMP, PCP, predikce adresy a portu v síti ISP (u symetrického SNAT) aj.
- narušení **unikátnosti identifikace zařízení** připojeného k Internetu (IP adresou) – „sdílejí“ adresu v síti ISP, v různých LAN mohou mít stejné, rozšíření na adresu a port
- proměna Internetu z **nespojované (IP) sítě** na „jakousi“ spojovanou – udržování překladů (tj. stavů) pro TCP spojení nebo výměny UDP datagramů, jejich závislost na existenci překladů
- narušení **nezávislosti na vyšší vrstvě** (datech) – využití TCP/UDP portů pro přeposílání IP paketů, pro ICMP pakety využito místo portu ID (echo) nebo (část) záhlaví IP paketu v datech (jiné zprávy)

Problémy/kontroverze

- omezení počtu aktivních TCP spojení / UDP výměn mezi LAN a sítí ISP – $\approx$ 60 tis. (volných TCP/UDP portů) $\times$ přidělených adres v síti ISP

Problémy/kontroverze

- omezení počtu aktivních TCP spojení / UDP výměn mezi LAN a sítí ISP – $\approx$ 60 tis. (volných TCP/UDP portů) $\times$ přidělených adres v síti ISP
- pro pakety mezi LAN a sítí ISP manipulace s tabulkou překladů, přepočítání kontrolních součtů v IP a TCP/UDP záhlaví aj. – nutné výpočetní zdroje (výkon, paměť)
- ...

Problémy/kontroverze

- omezení počtu aktivních TCP spojení / UDP výměn mezi LAN a sítí ISP – $\approx$ 60 tis. (volných TCP/UDP portů) $\times$ přidělených adres v síti ISP
- pro pakety mezi LAN a sítí ISP manipulace s tabulkou překladů, přepočítání kontrolních součtů v IP a TCP/UDP záhlaví aj. – nutné výpočetní zdroje (výkon, paměť)
- ...

! u SNAT **„bezpečnost“ LAN, „skrytí“** před (ne-bezpečným) Internetem – typicky součást firewallu, ale pak port forwarding/triggering (DNAT), NAT traversal (zejm. UPnP) atd.!