**(1.) Význam služby NAT v IPv4 a její varianty**

* NAT — Network Address Translation
* Překládá IPv4 na IPv4 — Zejména privátní IPv4 na veřejné IPv4
* Vznikla kvůli nedostatku IPv4 adres
  + IPv4 bloky adres se rozdávali “velkým” hráčům
  + Hodně se jimi plýtvalo
  + V dnešní době již není žádný volný blok IPv4 adres: poslední se rozdal v roce 2020
* Umožňuje síti, která je adresována pomocí privátními rozsahy, aby komunikovala v internetu pomocí jedné (či více) veřejných IP adres
  + Privátní rozsahy:
  + 10.0.0.0/8
  + 172.16.0.0/12
  + 192.168.0.0/16
  + NATce lze přidělit jedna veřejná IP (**PAT**) či bazén veřejných IP (**PAT**, **Dynamic NAT**) či přidělat jednu veřejnou IP na jednu privátní IP (**Static NAT**)
* Tím, jak NAT funguje, tak z toho vyplývá i bezpečností výhoda: zařízení na internetu nebudou mít přístup k naší privátní síti, jelikož komunikujeme prostřednictvím specifikovaných veřejných IP adres
  + Každopádně by se toto nemělo brát jako definitivní zabezpečení oproti firewallům, atd.
* NAT konfigurujeme na hraničních routerech sítě

**Nevýhoda**

* Ztrácíme end-to-end adresování
* Pakety přeložené NATem se obtížně trasují
  + Proto ISPs a další musí uchovávat logy přeložení pro státní osoby
* Mohou zde také nastat problémy s tunelovacími protokoly, zejména IPsec VPN, které pracuje na 3. vrstvě — NAT mění hlavičky paketů a tím naruší integritu
  + Také narušuje funkčnost IP telefonie, kvůli tomu, že z vnějška není možné se připojit do vnitřka (vysvětlo níže, co je vnějšek a vnitřek)

**Terminologie**

V NAT se používají 4 typy adres

* **Inside Local** — jak IP adresa vnitřního zařízení vypadá v naší síti (e.g., 192.168.0.7)
* **Inside Global** — jak IP adresa vnitřního zařízení vypadá ve vnější síti (e.g., veřejná IP v Internetu)
* **Outside Local** — jak IP adresa vnějšího zařízení vypadá v naší síti (veřejná IP → privátní IP)
* **Outside Global** — jak IP adresa vnějšího zařízení vypadá ve vnější síti (veřejná IP)

**Inside**

* Označuje fyzické rozhraní, které je směrem do naší sítě (privátní)

**Outside**

* Označuje fyzické rozhraní, které je směrem z naší sítě (do internetu)

**Varianty NATu**

1. Statický NAT
2. Dynamický NAT
3. PAT — Port Address Translation

**1. Statický NAT**

* Překládá jednu privátní adresu na veřejnou adresu
* Nešetří IP adresy
* Je nutné privátní adrese přiřadit ručně jednu veřejnou
* Využívá se např. když chceme aby se zařízení chovalo jako internetově dostupné

**2. Dynamický NAT**

* Využívá pool veřejných adres, které přiděluje na vyžádání jednotlivým uzlům v privátní síti
* Každopádně, v jednom okamžiku může komunikovat pomocí veřejné adresy jen takový počet zařízení, kolik je veřejných adres v poolu
  + Zařízení, na které nezbude veřejný adresa, musí čekat

**3. PAT — Port Address Translation**

* Taky označována jako NAT overload
* PAT mapuje vícero privátních adres na jednu či pool veřejných adres
* Dělá to tak pomocí dvojici portů — **Source IP:Port** → **Public IP:Port**
  + Source IP bude logicky jiná, pri jiné zařízení
  + Ale public IP může být stejná v případě jedné veřejní IP
  + Komunikace se překládá pomocí portů
    - Zdali máme např. 192.168.0.7:4638 → 88.99.15.52:1234, tak pokud přijde odpověď na 88.99.15.52:1234, NAT nám to přeloží na 192.168.0.7:4638
    - Těchto překladů zde může být stovky
* PAT také ověřuje, že byl příchozí paket klientem vyžádán – tím plní i takovou ochrannou funkci

**(2.) Konfigurace služby NAT a PAT**

**Statický NAT**

1. Namapujeme vnitřní lokální adresu na vnější lokální adresu
2. Po té nakonfigurujeme, jaké interfaces jsou inside a outside

# Vnitřní zdrojová statická <PRIVATE IP> na <PUBLIC IP>

ip nat inside source static <PRIVATE\_IP> <PUBLIC\_IP>

int g0/0 # Např. inside interface

ip nat inside

int g0/1 # Např. outside interface

ip nat outside

​

**Dynamický NAT**

1. Vytvoříme pool veřejných adres, které se budou používat k překladu
2. Vytvoříme ACL, ve které budou definované privátní IP, které chceme, aby mohli využívat dynamickou NAT
3. Povolíme překlad NAT z poolu a ACL
4. Po té nakonfigurujeme, jaké interfaces jsou inside a outside

# 1.

## NAT pool s názvem <POOL\_NAME>,

## který začíná na <FIRST\_IP> a končí na <LAST\_IP>

## a má síťovou masku <MASK>

ip nat <POOL\_NAME> <FIRST\_IP> <LAST\_IP> netmask <MASK>

## Např. ip nat BAZEN 192.168.0.1 192.168.0.64 netmask 255.255.255.0

# 2.

## ACL s <ID> povolující <PRIVATE\_NETWORK\_IP> s filtrací <WILDCARD\_MASKOU>

access-list <ID> permit <PRIVATE\_NETWORK\_IP> <WILDCARD\_MASK>

## Např. access-list 1 permit 192.168.0.0 0.0.0.63

# 3.

ip nat inside source list <ID> pool <POOL\_NAME>

## Např. ip nat isnide source list 1 pool BAZEN

# 4.

int g0/0 # Např. inside interface

ip nat inside

int g0/1 # Např. outside interface

ip nat outside

​

**PAT**

1. Optional — Vytvoříme pool veřejných adres, které se budou používat k překladu
2. Vytvoříme ACL, ve které budou definované privátní IP, které chceme, aby mohli využívat PAT
3. Nastavíme PAT na interface s overload (v případě poolu tam dáme pool)
4. Po té nakonfigurujeme, jaké interfaces jsou inside a outside

# OPTIONAL: 1.

## NAT pool s názvem <POOL\_NAME>,

## který začíná na <FIRST\_IP> a končí na <LAST\_IP>

## a má síťovou masku <MASK>

ip nat <POOL\_NAME> <FIRST\_IP> <LAST\_IP> netmask <MASK>

## Např. ip nat BAZEN 192.168.0.1 192.168.0.64 netmask 255.255.255.0

# 2.

## ACL s <ID> povolující <PRIVATE\_NETWORK\_IP> s filtrací <WILDCARD\_MASKOU>

access-list <ID> permit <PRIVATE\_NETWORK\_IP> <WILDCARD\_MASK>

## Např. access-list 1 permit 192.168.0.0 0.0.0.63

# 3.

ip nat inside source list <ID> interface <INTERFACE> overload

## Např. ip nat isnide source list 1 pool BAZEN

### V případě poolu:

### ip nat inside source list <ID> pool <POOL\_NAME> overload

# 4.

int g0/0 # Např. inside interface

ip nat inside

int g0/1 # Např. outside interface

ip nat outside

​

**(3.) Port-forwarding – charakteristika a konfigurace**

**Charakteristika**

* Umožní předání paketů, směrující z veřejné části sítě, na určitý aplikační port na počítač v privátní části sítě
* Vhodná např. u serverových služeb, běžících na počítači s privátní IP adresou
  + Např. port-forward MC serveru na portu 25565 na privátní ip 192.168.0.2:25565

**Konfigurace**

1. Vytvoříme port-forward na privátní IP s portem z veřejné IP s portem
2. Po té nakonfigurujeme, jaké interfaces jsou inside a outside

# 1.

ip nat inside source static tcp <PRIVATE\_IP> <PRIVATE\_PORT> <PUBLIC\_IP> <PUBLIC\_PORT>

# Private IP + private port -> např. 192.168.0.2 + 25565

# Public IP + public port -> např. 88.99.15.52 + 20088

## Umožní komunikaci z internetu na 88.99.15.52:20088 s privátním

## uzlem a aplikací na 192.168.0.2:25565

# 2.

int g0/0 # Např. inside interface

ip nat inside

int g0/1 # Např. outside interface

ip nat outside