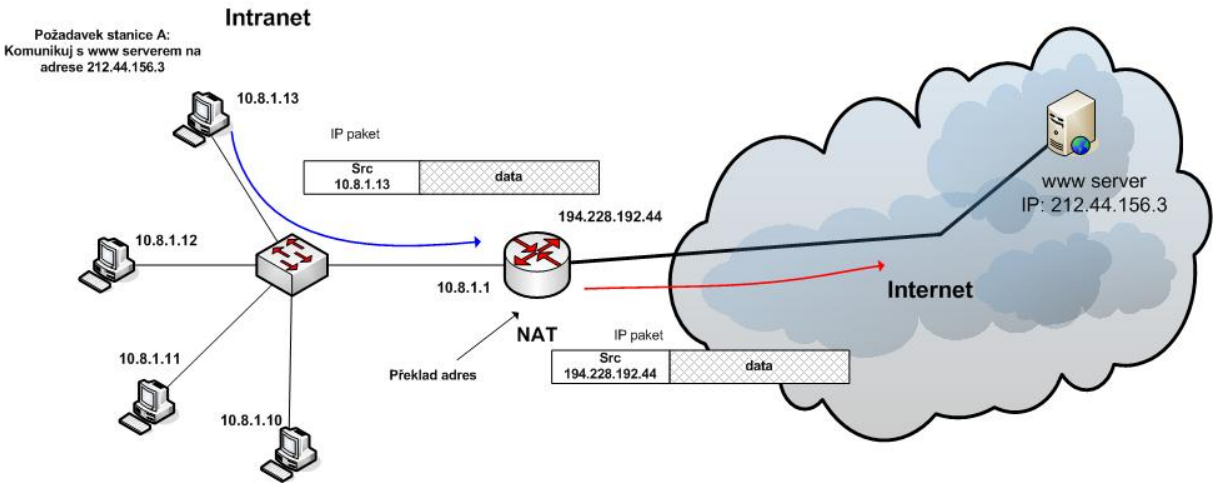
Překlad adres – Network Address Translation

Překlad adres je důležitou vlastností směrovačů. Používá se zejména ze dvou důvodů:

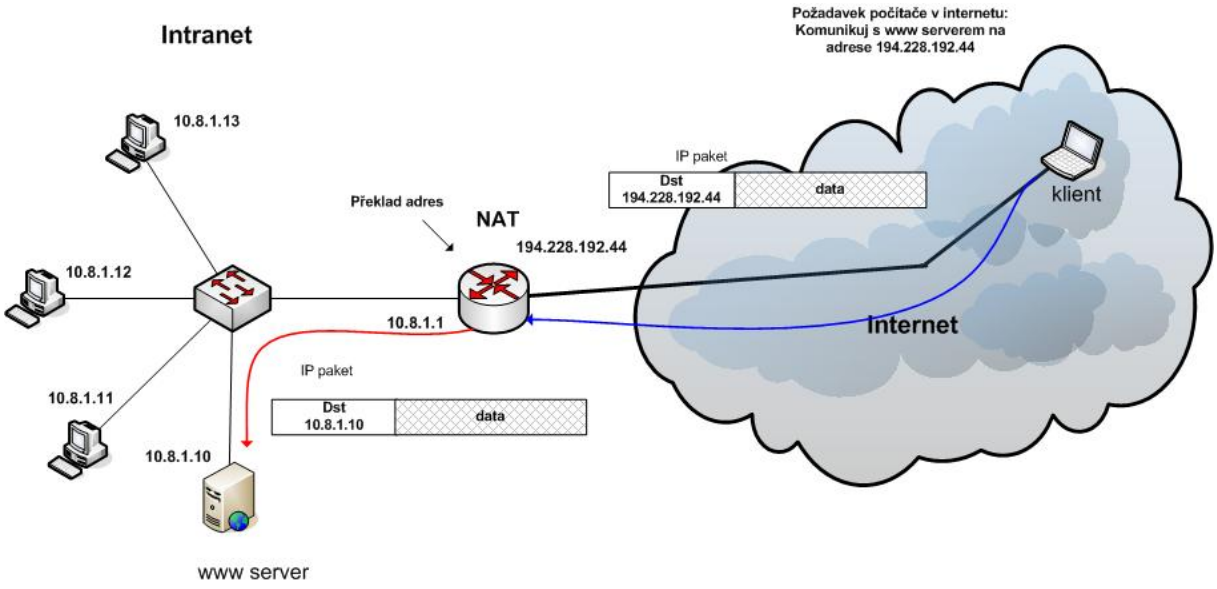
- omezit potřebný počet veřejných IP adres
- zajistit bezpečnost komunikace mezi vnitřní a veřejnou sítí

Připojení vnitřní sítě LAN k internetu pak zajišťuje pouze jediná veřejná IP adresa. Ta je přidělena na venkovní rozhraní směrovače,který zajišťuje spojení se sítí internet. NAT může fungovat jak pro příchozí tak pro odchozí spojení.

U odchozího spojení dochází k nahrazení zdrojové adresy z privátního rozsahu veřejnou IP adresou směrovače. Při příchozích spojeních zase dochází ke změně cílové adresy z veřejné na privátní.



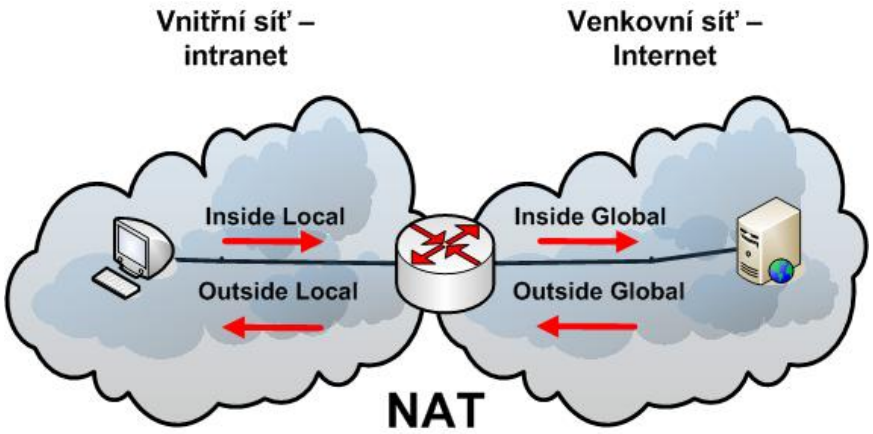
NAT pro odchozí spojení



NAT pro příchozí spojení

Při používání NAT definujeme tyto druhy IP adres:

- **Inside local** – adresa zařízení ve vnitřní síti (počítač), privátní IP adresa
- **Inside global** – veřejná IP adresa, která je viditelná v Internetu jako adresa počítače
- **Outside local** – IP adresa z vnitřní sítě, pod kterou je viditelný venkovní počítač
- **Outside global** – veřejná IP adresa vzdáleného serveru v Internetu



IP adresy používané při NAT

Technologie NAT pracuje v několika režimech:

- **statický NAT** – mapuje vnitřní IP adresu na vnější IP adresu. Statický NAT je používán pokud je zapotřebí přistupovat z vnější sítě do vnitřní
- **dynamický NAT** – mapuje vnitřní IP adresu na vnější IP adresu z nějaké skupiny IP adres (address pool)
- **overloading** – přetěžování mapuje vnitřní IP adresy na jednu vnější IP adresu; bývá označován jako PAT; jedná se o formu dynamického NATu

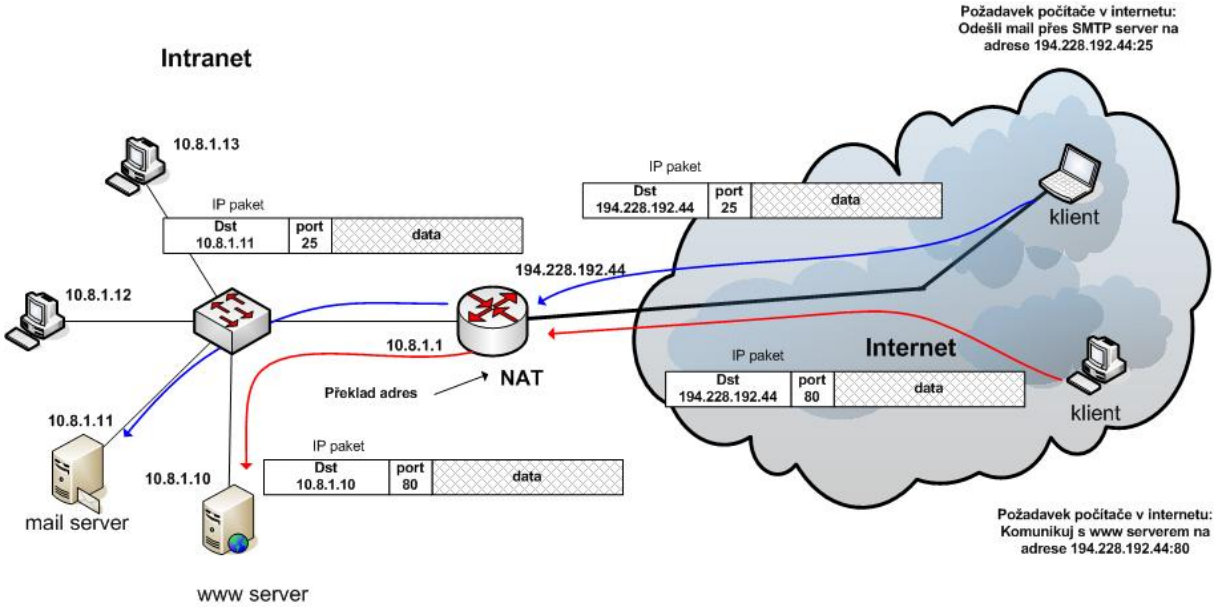
NAT může pro překlad používat jedinou veřejnou IP adresu nebo i více adres. Záleží na množství počítačů ve vnitřní síti a druhu provozu. V případě, že používáme jedinou veřejnou IP adresu mluvíme o přetěžování (overload).

- **NAT pracuje na 3. (síťové) vrstvě OSI modelu.**

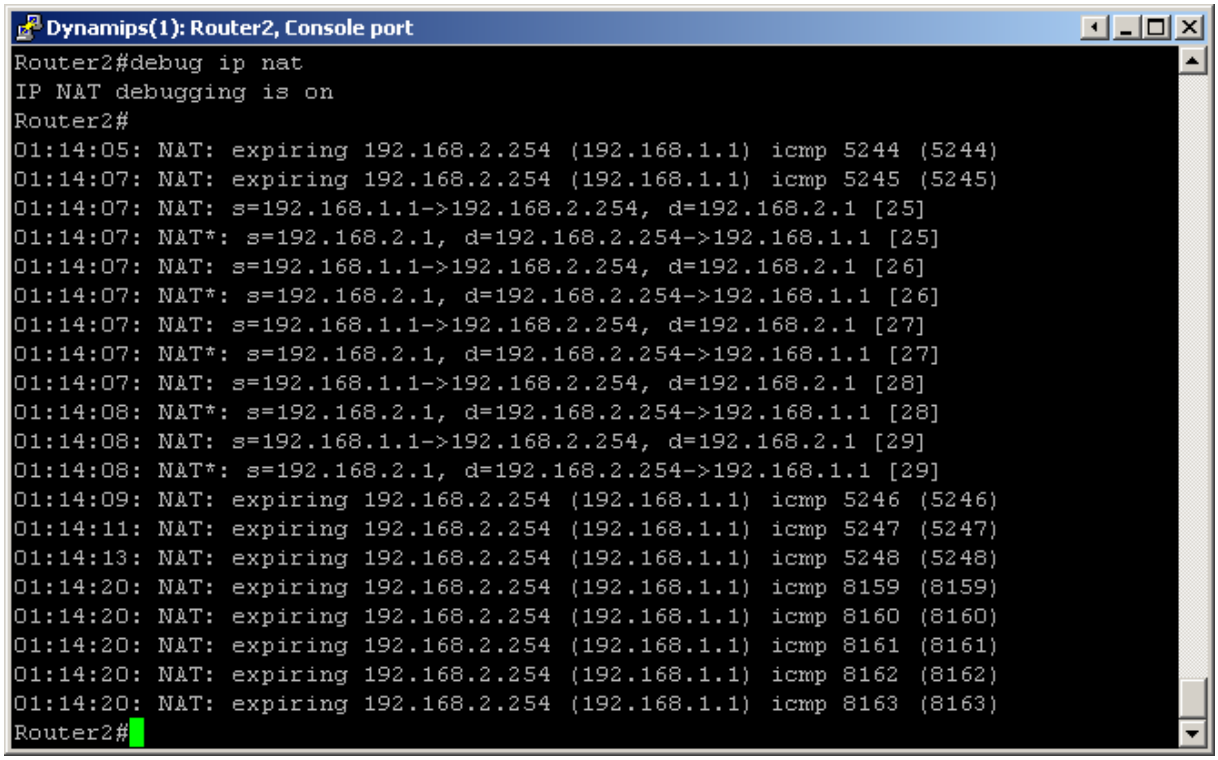
Při používání technologie NAT se setkáváme s různými problémy. Některé aplikace nemusí fungovat správně. To je jedním z důvodů proč ISP (zejména velcí jako UPC, O_2, …) přidělují klientům přímo veřejné IP adresy. Typickým příkladem je protokol IPSec. Jelikož IPSec navazuje komunikaci mezi dvěma koncovými body, je zde zásadním problémem záměna adres v hlavičce paketu.

Port Address Translation - PAT

V případě PAT dochází k překladu jak adres tak i příslušných portů v IP komunikaci. Výhodou zde je, že za jednu venkovní IP adresu můžeme maskovat celou řadu služeb, které jsou hostovány na různých serverech. Typickým příkladem jsou FTP a www servery umístěné v DMZ.



PAT – maskování dvou serverů za jedinou veřejnou IP adresu



Funkce NAT na směrovači

192.168.1.0/24 … vnitřní síť
192.168.2.0/24 … venkovní síť (Internet)
Počítač s IP adresou 192.168.1.1 komunikuje s počítačem v Internetu 192.168.2.1:

1. Paket se dostane na výchozí bránu 192.168.1.254.
2. Funkce NAT zamění zdrojovou adresu 192.168.1.1 venkovní adresou směrovače 192.168.2.254 (záznamy označené *NAT:*)
3. Paket dorazí k cíli
4. Na směrovač přijde odpověď je zaměněna cílová adresa 192.168.2.254 adresou 192.168.1.1 (záznamy označené *NAT*:*)
5. Odpověď dorazí zpět na počítač 192.168.1.1

Dynamické záznamy v tabulce NAT mají omezenou životnost – záznamy *NAT: expiring*.