A2B32DAT
Datové sítě

Ing. Pavel Bezpalec, Ph.D.

Katedra telekomunikační techniky
FEL ČVUT v Praze

Pavel.Bezpalec@fel.cvut.cz

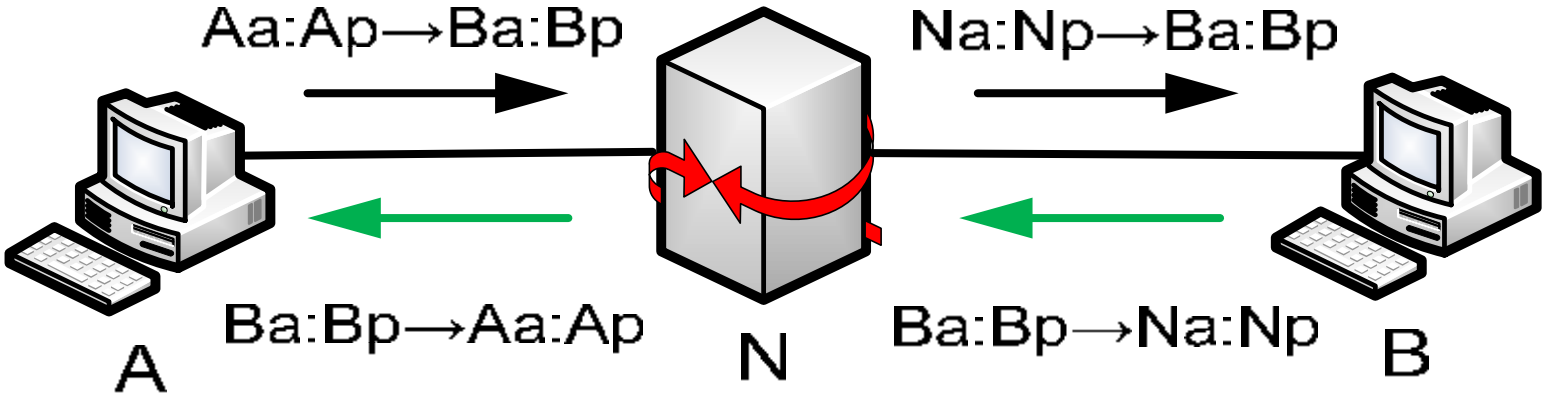
NAT – *Network Address Translation*

- RFC 1631
- proces modifikace IP záhlaví výměnou jedné adresy za jinou
- realizován (obvykle) na hraničním směrovači
- odděluje vnitřní a vnější síť
- zajišťuje schopnost stanicím s neveřejnými adresami přístup na Internet
- vnitřní síť adresována neveřejnými/privátními adresami
  - RFC 1918 (10.0.0.0/8 , 172.16.0.0/12 , 192.168.0.0/16)
- vnější síť (obvykle) adresována veřejnými adresami
  - lze dělat i překlady typu
    - neveřejná-neveřejná adresa
    - veřejná-veřejná adresa

NAT – základní pojmy

- ü směrovač si udržuje překladovou tabulku
- ü snaha zachovat číslo portu při překladu
  - pokud nelze je zvoleno náhodně

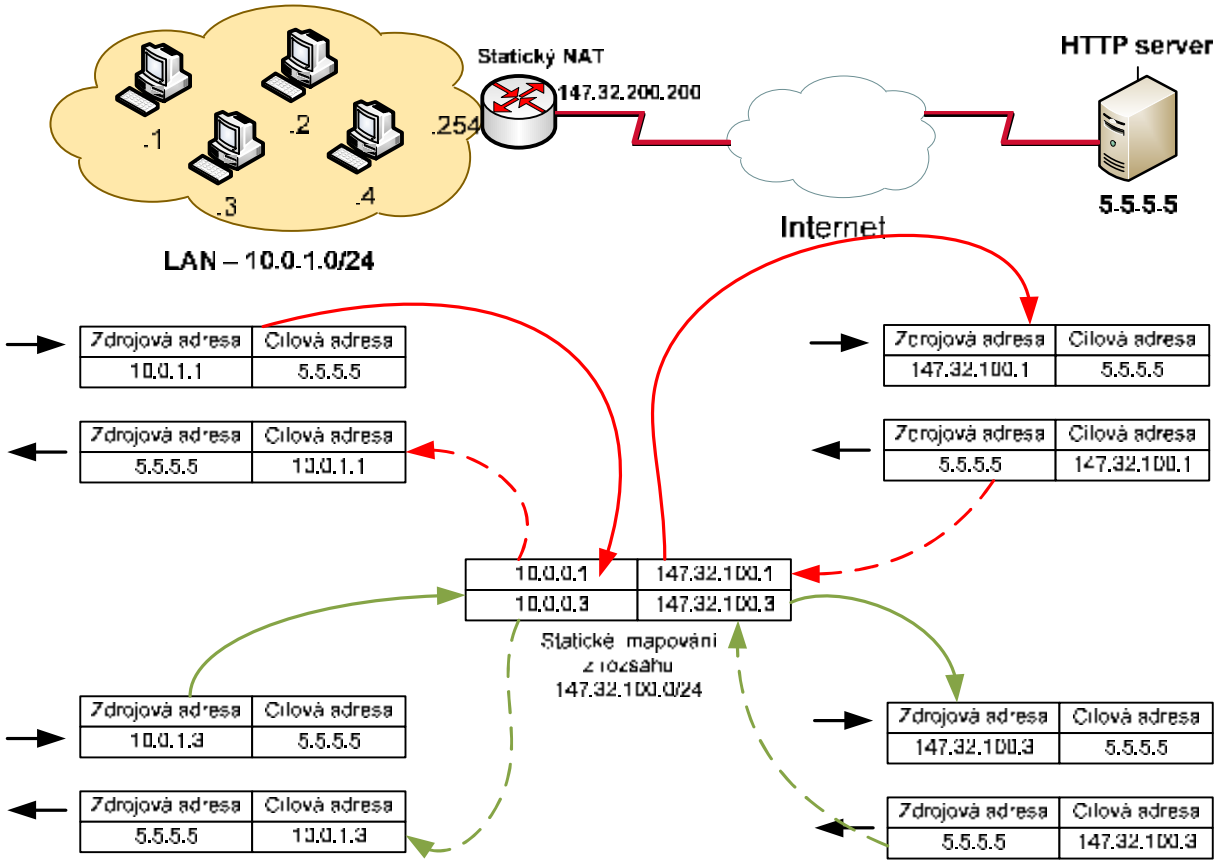
Překládej odchozí provoz Aa:Ap na Na:Np
Mapuj příchozí provoz Na:Np na Aa:Ap



Aa:Ap → Ba:Bp	Zdrojová adresa:Zdrojový port→Cílová adresa:Cílový port
Aa	adresa *a* stanice *A*
Ap	port *p* stanice *A*
N	bod, ve které se realizuje překlad adres

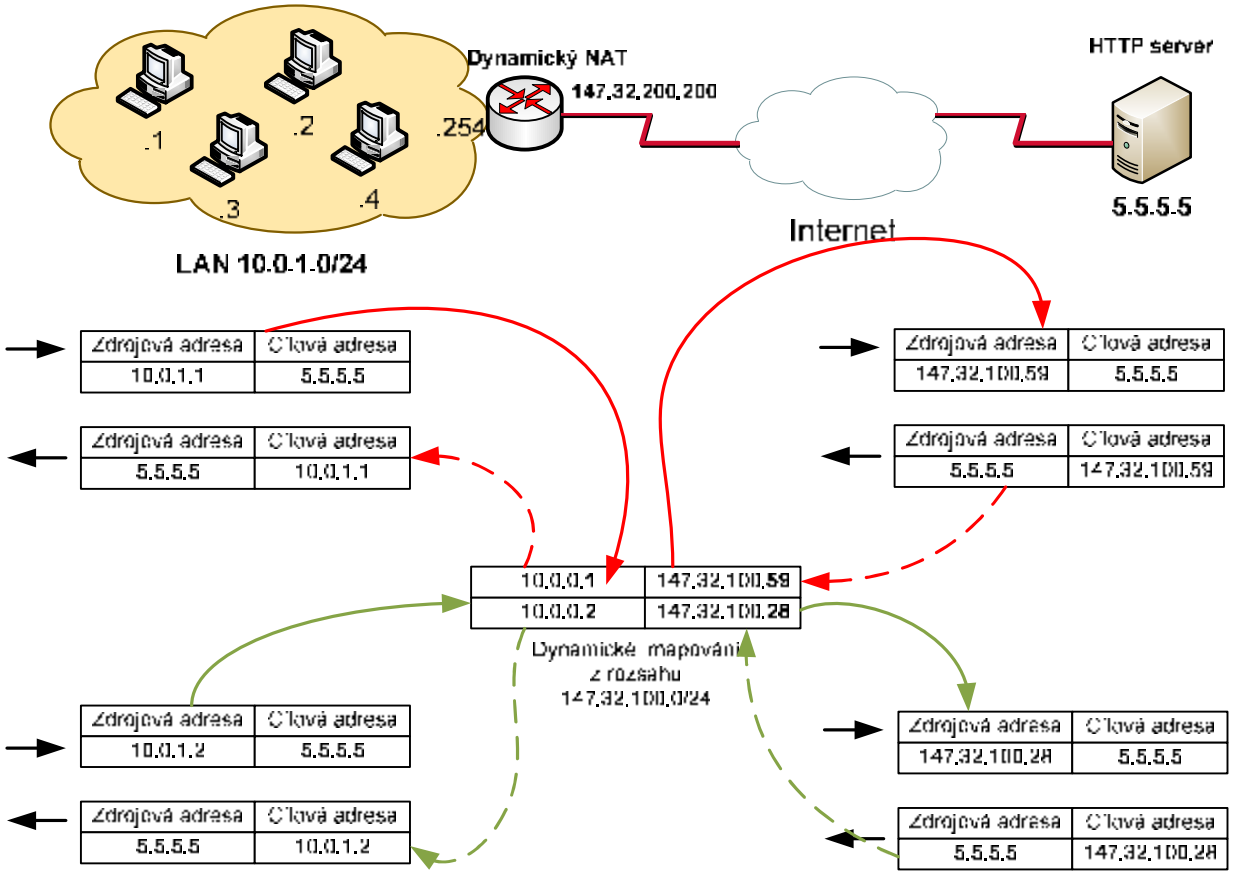
Statický NAT

- pevné mapování 1:1 vnitřní IP adresy na konkrétní vnější IP adresu
- zachovává čísla portů
- pro každou vnitřní adresu musí být přidělena veřejná adresa (pokud má mít stanice přístup „ven“)

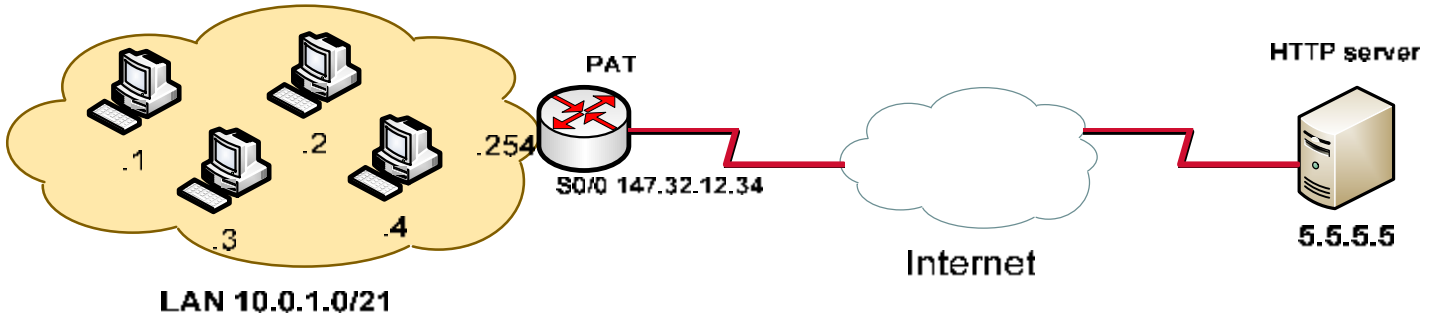


Dynamický NAT

- dynamické mapování vnitřní IP adresy na konkrétní vnější IP adresu
- zachovává čísla portů
- počet současných spojení je omezen počtem veřejných IP adres



PAT – *Port Address Translation*



Zdrojová adresa	Cílová adresa	Zdrojový port	Cílový port
10.0.1.1	5.5.5.5	1234	80

Zdrojová adresa	Cílová adresa	Zdrojový port	Cílový port
5.5.5.5	10.0.1.1	80	1234

Zdrojová adresa	Cílová adresa	Zdrojový port	Cílový port
147.32.12.34	5.5.5.5	1234	80

Zdrojová adresa	Cílová adresa	Zdrojový port	Cílový port
5.5.5.5	147.32.12.34	80	1234

10.0.0.1	1234	S0/0	1234
10.0.0.2	1234	S0/0	1235

Překladová tabulka

Zdrojová adresa	Cílová adresa	Zdrojový port	Cílový port
10.0.1.2	5.5.5.5	1234	80

Zdrojová adresa	Cílová adresa	Zdrojový port	Cílový port
5.5.5.5	10.0.1.2	80	1234

Zdrojová adresa	Cílová adresa	Zdrojový port	Cílový port
147.32.12.34	5.5.5.5	1235	80

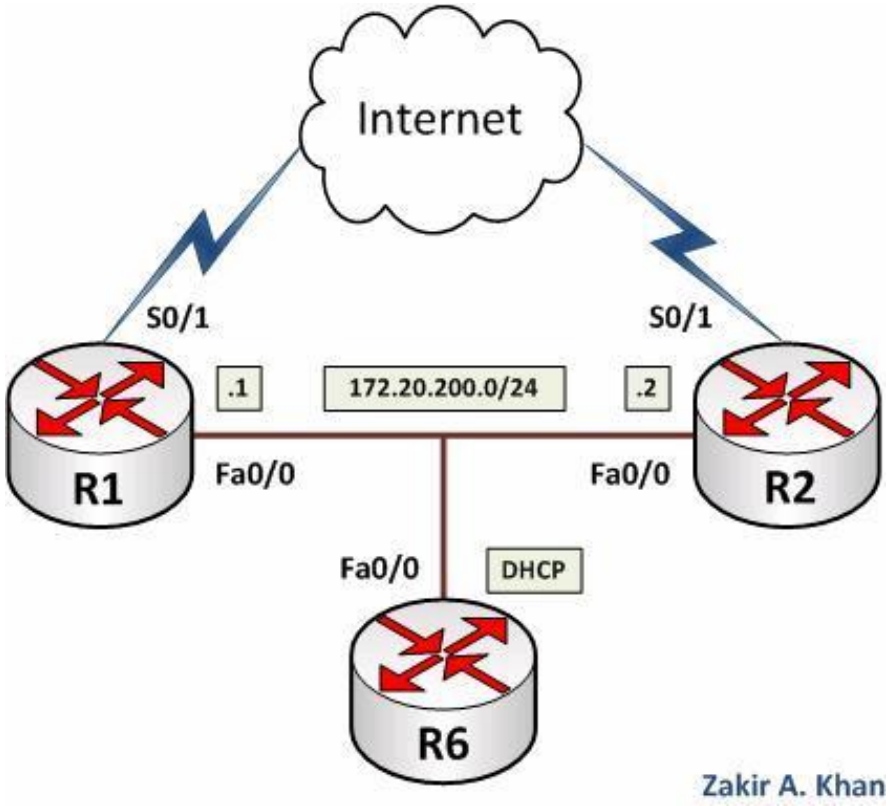
Zdrojová adresa	Cílová adresa	Zdrojový port	Cílový port
5.5.5.5	147.32.12.34	80	1235

PAT

- Ekvivalentní s označením:
  - NAPT – *Network Address and Port Translation*
  - Masquerade NAT
  - IP Masquerade
- jako veřejná IP adresa je použita adresa vnějšího rozhraní (obvykle) přidělená od ISP
- nejčastější případ pro „domácí“ sítě
- jednotlivá spojení jsou rozlišena porty
- komunikace musí být iniciována z vnitřní sítě
- příchozí datagramy bez záznamu v tabulce jsou zahozeny

NAT podle směru

- SNAT – Source NAT
  - překlad zdrojové adresy/portu
  - obvyklý typ NATu
- DNAT – Destination NAT
  - překlad cílové adresy/portu
  - přístup ke službám ve vnitřní síti
  - port-forwading
- Cisco SNAT – Statefull NAT
  - HSRP
  - vysoká dostupnost (HA) + NAT
  - výměna překladových tabulek mezi R1 a R2



Výchozí doby životnosti záznamů v NAT tabulce

Mikrotik

- ICMP, UDP 10s
- UDP-stream 180s
  - počítá se od poslední přijaté odpovědi
  - pro VoIP
- TCP SYN 60s
- TCP established 24h
- TCP FIN,CLOSE 10s
- jiné (GRE, ESP…) 600s

Cisco

- UDP 300s
- DNS 10s
- TCP 24h
- TCP SYN,FIN, RES 60s
- ICMP 60s
- PPTP 24h

Nevýhody NATu

- ü Neexistuje end-to-end dostupnost stanic (obecně)
- ü Komunikace musí být vždy iniciována z vnitřní sítě
- ü Existují problematické aplikace
  - FTP
    - aktivní režim – nelze s NAT
    - pasivní režim
  - SIP a jiné aplikační protokoly nesoucí IP adresy i v aplikační vrstvě
    - řešení ALG – Application Layer Gateway
  - multicast
  - směrovací protokoly

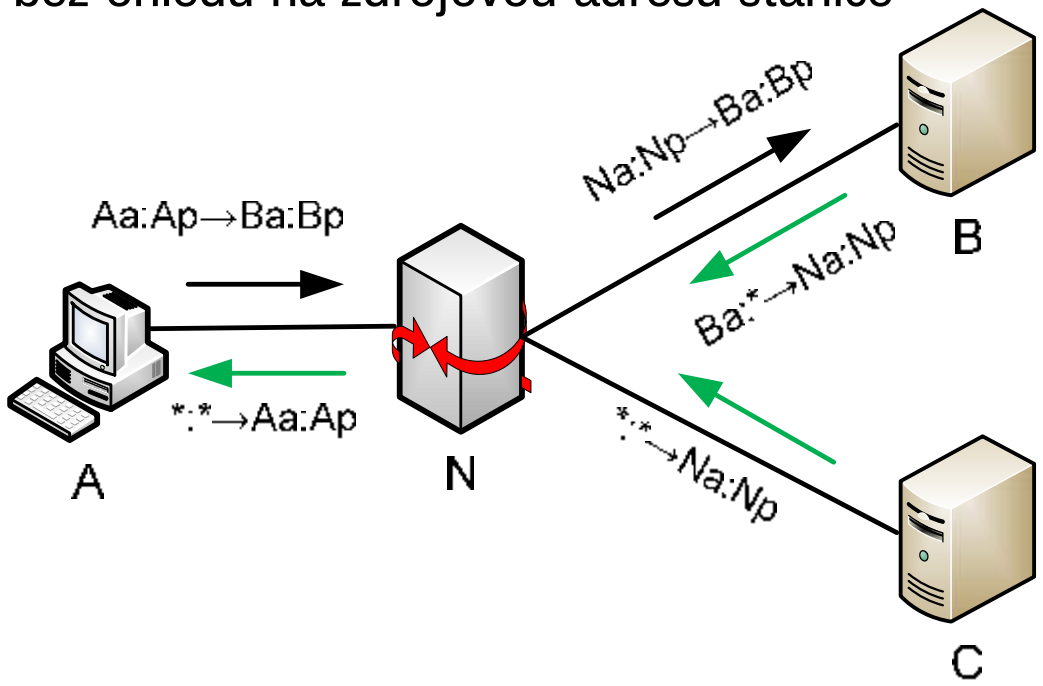
Varianty NATu

- Full Cone NAT
- IP Restricted NAT
- Port Restricted NAT
- Symmetric NAT

- zavedeno protokolem STUN
- v praxi se často vyskytují implementace kombinující různé přístupy

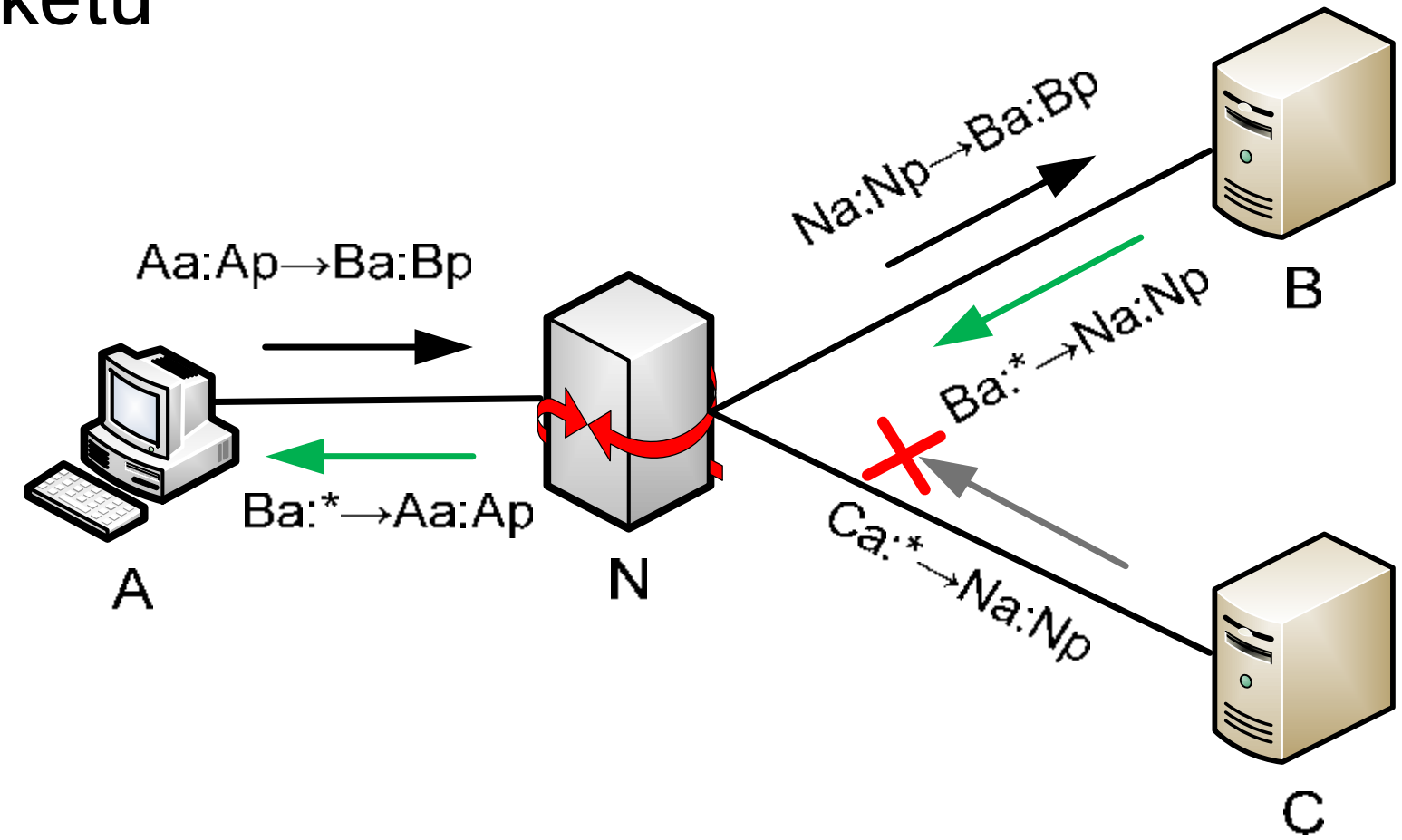
Full-cone NAT

- 1:1 NAT
- Nejméně omezující
- První spojení z A na B vytvoří překlad z vnitřní adresy (IntAdd:IntPort) na externí adresu (ExtAdd:ExtPort).
- Jakákoliv další data z A na B budou využívat tyto adresy/porty.
- Paket odeslaný na (ExtAdd:ExtPort) bude doručen na stanici ve vnitřní síti (IntAdd:IntPort) bez ohledu na zdrojovou adresu stanice



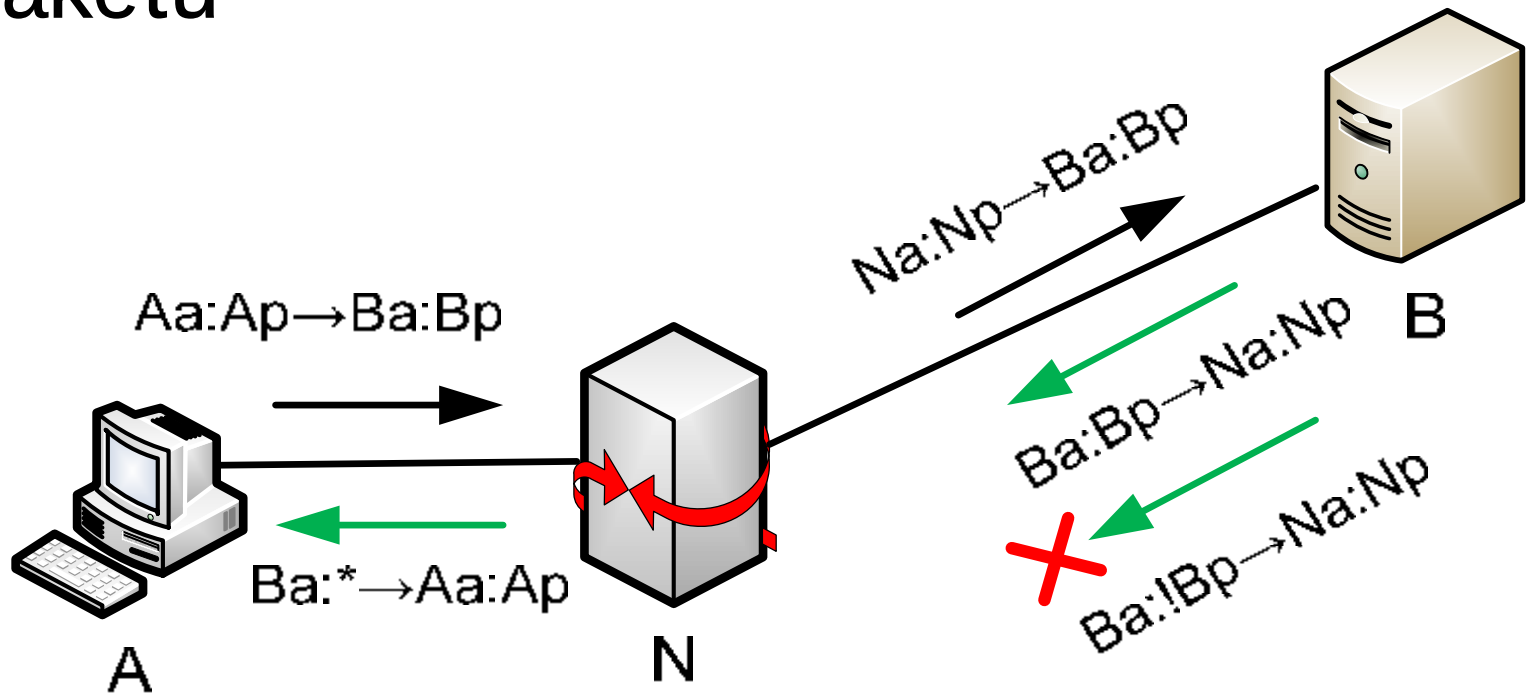
IP address restricted NAT

- kontroluje zdrojovou adresu příchozího IP paketu



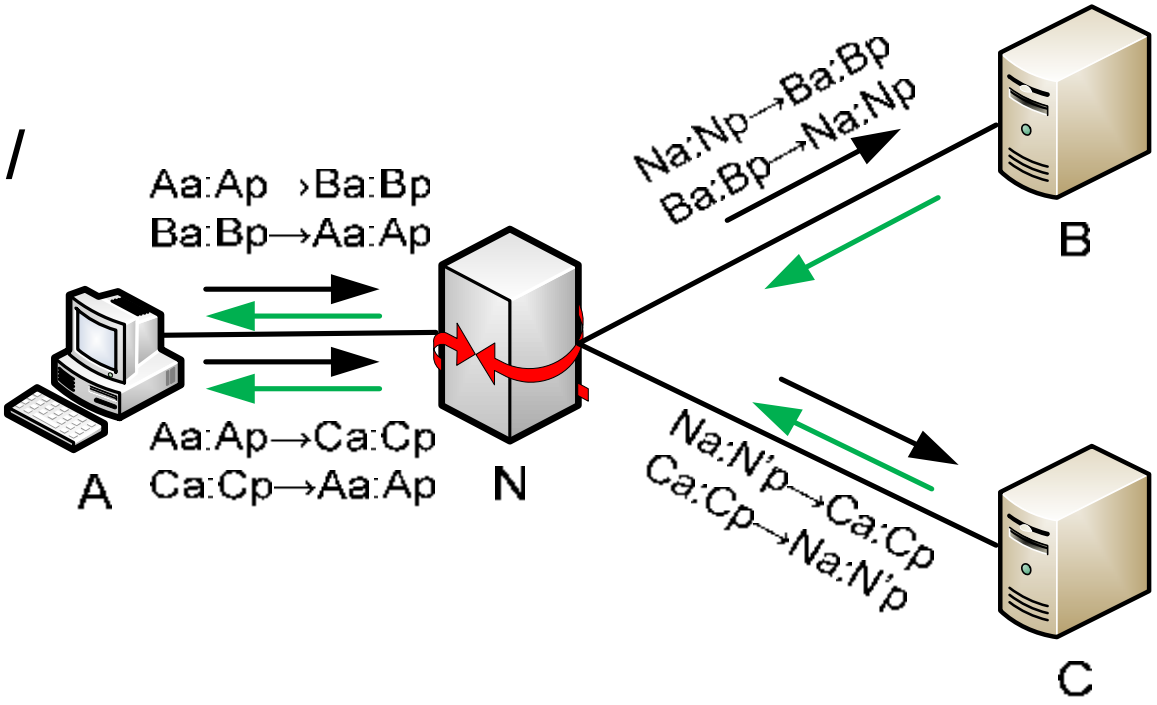
Port restricted NAT

- kontroluje zdrojovou adresu a port příchozího IP paketu



Symetrický NAT

- nejrestriktivnější varianta NATu
- každé spojení ze stejné lokální adresy/portu má unikátní záznam (adresa/port) v překladové tabulce
- Pokud se odešle paket s stejnou lokální adresou/ portem ale jinou cílovou adresou použije se jiné mapování!



Překonávání NATu

- NAT traversal
  - obecný pojem označující techniky k překonání NATu

- STUN – Session Traversal Utilities for NAT
  - dříve Simple Traversal UDP through NAT
  - RFC 5389
  - C-S aplikace
  - C pošle požadavek na S
  - S vrátí adresu/port
  - z odpovědi C zjistí typ použitého NATu
  - nefunguje se symetrickým NATem
  - STUN server musí mít dvě veřejné IP adresy

Překonávání NATu

ü TURN – Traversal Using Relay NAT

- RFC 5766
- protokol pro přeposílání TCP/UDP zpráv stanicím, které jsou za NATem
- dosažitelnost stanice za NATem je zajištěna přesměrováním provozu přes TURN server
- funguje i se symetrickým NATem
- doporučuje se použít ho jako poslední možný způsob
- SPF
- vyžaduje vysoký výkon

Překonávání NATu

- ICE – Interactive Connectivity Establishment
  - RFC 5245
  - zjišťuje s pomocí kterých metod je stanice za NATem dosažitelná
  - využívá STUN a TURN

Překonávání NATu

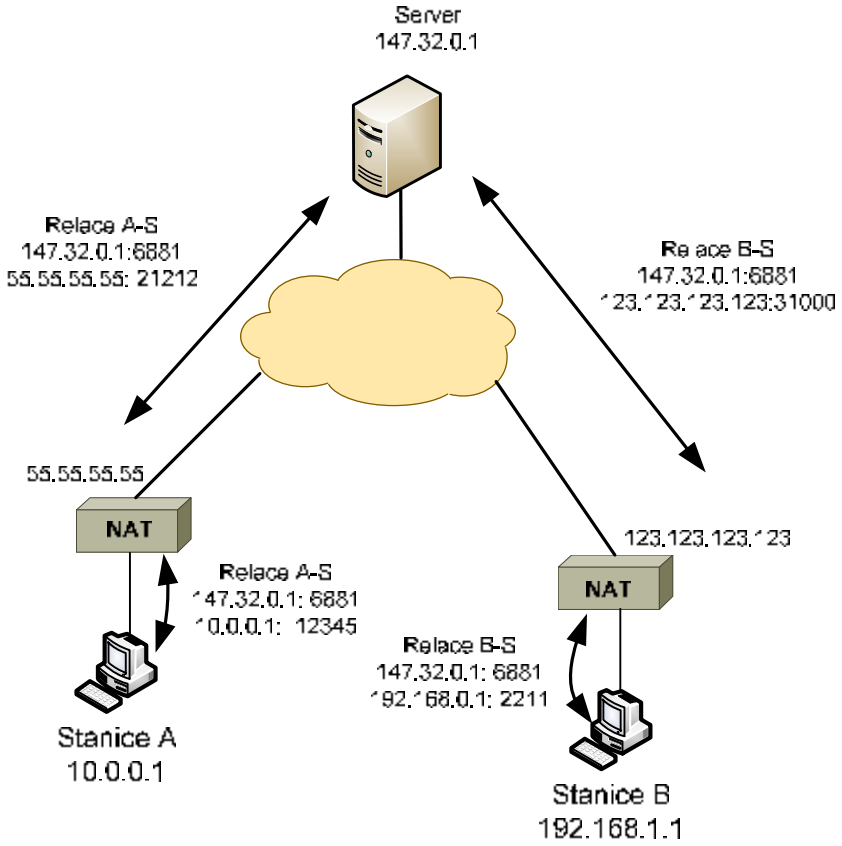
- ALG – Application Layer Gateway
  - RFC2663 sec. 2.9
  - aplikace (plugin) spolupracující s NATem, která umožňuje vzájemnou komunikaci klientů zapojených za NATem pomocí specifických překladů adres pro daný aplikační protokol
  - typicky SIP, přenos souborů přes IM, FTP
  - velmi podobné proxy serveru
    - ale nepotřebuje konfiguraci na straně klienta
    - pro klientskou aplikaci je transparentní

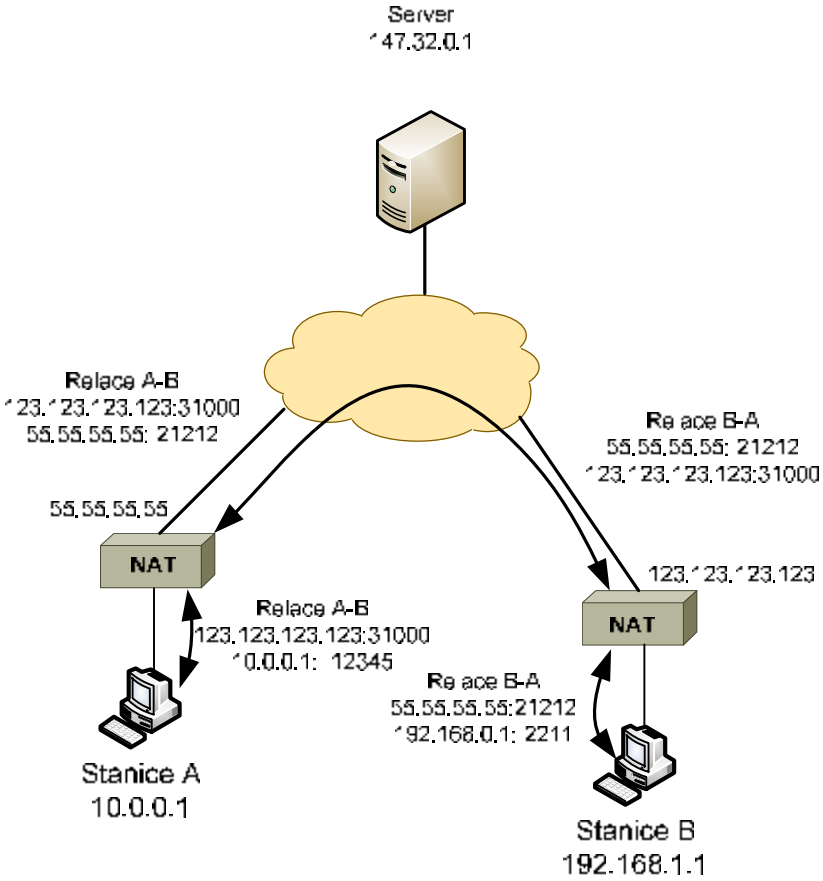
Překonávání NATu

ü Hole punching

- technika pro navázání komunikace, pokud jsou obě stanice za NATem
- dohodnutí čísla portu, na kterém se bude komunikovat
- „prošťouchnutí“ cesty z obou stran
- udržování „tunelu“ periodickými keepalive zprávami
- existují metody pro UDP i TCP
- nefunguje se symetrickým NATem
- používá se v P2P aplikacích, VoIP

UDP hole punching





NAT × Firewall

- Firewall
  - filtrování paketů na základě pravidel
  - L3 – paketový filtr
  - L4 – stavový paketový filtr
  - L7 – proxy server
- NAT
  - mechanismus sloužící ke zpomalení úbytku IPv4 adres
  - překlad zdrojové/cílové adresy/portu
  - aktualizace vybraných částí IP záhlaví
    - kontrolní součet záhlaví …

NAT a Firewall se dnes často používají společně

Dotazy